Identifying Cybersecurity Elements for a Cybersecurity Framework in Higher Education

Mafika Nkambule[1], Joey Jansen van Vuuren[1] and Louise Leenen[2]
[1]Tshwane University of Technology, Pretoria, South Africa
[2]University of the Western Cape and CAIR, Cape Town, South Africa

nkambulemw@tut.ac.za
Jansenvanvuurena1@tut.ac.za
lleenen@uwc.ac.za

Abstract: The increasing cybersecurity threats to higher education institutions in Africa necessitate risk management frameworks that are resilient and sensitive to regional needs. This paper applies Modified General Morphological Analysis (MGMA) to identify essential elements for an adaptable cybersecurity framework, focusing on the African higher education context. African institutions face many challenges, like limited funding, underdeveloped digital infrastructures, and rising cyberattacks. Our proposed MGMA is a structured methodology to examine key cybersecurity dimensions: governance, policy, technical controls, capacity building, and resource allocation. This approach allows for assessing complex interrelations among these elements, aimed at practical solutions suitable for African institutions. This study focuses on risk management approaches to address the specific vulnerabilities of African higher education institutions (HEIs), such as restricted budgets, inadequate cybersecurity teams, and increasing reliance on digital systems. The study promotes collaborative efforts by creating institutional networks, sharing resources, and enhancing cybersecurity expertise across Africa. The findings will guide decision-makers in aligning cybersecurity investments with strategic institutional goals, providing a framework for protecting critical educational assets, strengthening resilience, and advancing digital infrastructure development across African higher education.

Keywords: Cybersecurity risk management, Cybersecurity frameworks, Modified general morphological analysis, Cybersecurity strategies, Higher education in Africa

1. Introduction

Traditional cybersecurity frameworks, often crafted for more resourced sectors, struggle to meet the specific demands of educational environments, especially within the African context. This paper introduces an MGMA tailored for African HEIs to bridge these gaps. MGMA provides a structured, systems-based approach to assessing interconnected cybersecurity elements. Through focused analysis of governance, policy, technical controls, resource allocation, and capacity building, MGMA addresses the unique risks that African HEIs face. This method allows for a flexible, context-sensitive framework more suited to Africa's complex cybersecurity landscape of higher education.

This study aims to develop a comprehensive, adaptable cybersecurity framework for African HEIs by applying MGMA. Given Africa's specific challenges—from constrained resources to rising cyber incidents—this framework seeks to guide institutions in fortifying their cybersecurity practices in a sustainable, scalable manner. The study's relevance is rooted in its focus on Africa, a region often sidelined in broader cybersecurity discourse. By addressing both technical and organisational aspects of cybersecurity, this research contributes practical insights for African HEIs to protect their digital assets, maintain operational continuity, and navigate risks in an increasingly digital world.

2. Literature Review

Cybercriminals increasingly target higher education institutions due to the sensitive data they hold: student records, intellectual property, and valuable research outputs (Ulven & Wangen, 2021). While cyber threats are a global issue, African HEIs face distinct challenges, such as limited cybersecurity budgets, underdeveloped digital infrastructures, and a shortage of skilled personnel (Chigada, 2023). The rapid shift to digital platforms for academic and administrative purposes has intensified these vulnerabilities, making African universities susceptible to cyber threats. Most African HEIs still adopt reactive cybersecurity measures, responding to breaches rather than anticipating them (Mogoane & Kabanda, 2019). This approach, expected due to resource constraints, leaves critical gaps that cybercriminals exploit.

Cybersecurity threats in higher education have steadily risen, with African institutions particularly vulnerable due to limited funding, outdated infrastructure, and inadequate security measures (Chigada, 2023). These universities store sensitive data, making them prime targets for cybercriminals. Despite adopting basic

cybersecurity practices, the fast-paced digitisation of educational platforms has exposed new weaknesses, highlighting the need for more comprehensive and context-sensitive frameworks (Ulven & Wangen, 2021).

Existing cybersecurity frameworks, such as NIST's Cybersecurity Framework (CSF), ISO/IEC 27001, and CIS Critical Security Controls, provide valuable guidance but often lack the flexibility required for African HEIs. For instance, the NIST CSF focuses on risk management but does not account for the resource limitations typical of African universities (White & Sjelin, 2022). Similarly, while ISO/IEC 27001 emphasises risk-based controls, it lacks adaptability for institutions with limited cybersecurity expertise (Humphreys, 2016). CIS Controls are highly prescriptive, which can challenge institutions needing a more customised approach (Groš, 2021).

3. Methodology

3.1 Modified General Morphological Analysis

General Morphological Analysis (GMA) is a structured, systems-based approach designed to solve complex, multi-dimensional problems (Ritchey, 2022). Initially developed for complex problem-solving, GMA has been adapted for cybersecurity, providing a flexible method for identifying key risk factors and vulnerabilities among subject experts (Roodt, Leenen, Jansen van Vuuren, & Khan, 2020). It is particularly well-suited to dynamic environments like higher education, where multiple variables, such as technology, policy, governance, and user behaviour—must be considered together to create an effective cybersecurity strategy. Lantada, Carreño, and Jaramillo (2020) used the GMA methodology to support decision-making on disaster risk management. The methodology systematically structures and analyses the total set of relationships in this multi-dimensional, non-quantifiable problem. Traditionally applied in complex problem-solving across various fields, GMA is particularly relevant to cybersecurity, where numerous interdependent factors—ranging from technology and policy to user behaviour and governance—must be examined collectively to design effective strategies (Roodt et al., 2020)

The MGMA follows the same steps as the GMA, but in the MGMA process, facilitators or project owners with subject knowledge are allowed to contribute their knowledge during the preparation phase (J. Jansen van Vuuren, Leenen, Grobler, Chan, & Khan, 2016). The MGMA facilitation process starts by presenting subject experts with predetermined variables and values to facilitate a shortened variable brainstorming phase. Using the MGMA methodology in this study, information is initially gathered from a literature review and then evaluated for correctness by a group of subject experts in a facilitated manner.

This study uses Modified General Morphological Analysis (MGMA) rather than the more classical approach followed by Ritchey. MGMA provides a systems-based methodology that allows institutions to evaluate complex cybersecurity problems by identifying key factors and their interrelations (J. C. Jansen van Vuuren, Leenen, Grobler, Chan, & Khan, 2015). In African HEIs, cybersecurity threats intersect with unique resource and infrastructural constraints. MGMA allows African higher education institutions to systematically assess their cybersecurity challenges, focusing on governance, technology, and policy to build a more resilient cybersecurity posture. MGMA's structured approach enables institutions to prioritise their cybersecurity efforts effectively, even with resource constraints.

MGMA was utilised in a study to analyse complex cybersecurity elements, enabling universities to understand their risk landscapes better and identify critical elements for effective risk management.

3.2 MGMA-Based Approach Compared to Traditional Frameworks

MGMA distinguishes itself from traditional cybersecurity frameworks by offering a more flexible, adaptable solution. While frameworks like ISO/IEC 27001 and CIS Controls provide fixed guidelines (Hamdani et al., 2021), MGMA allows for the customisation of cybersecurity strategies tailored to the specific needs of African HEIs (Lakhno et al., 2024). The MGMA-based approach holistically integrates governance, policy, and technical solutions, creating a dynamic cybersecurity framework that can evolve as threats emerge, making it particularly effective in resource-limited environments (Ngounou Ngounou, Matanga, Essomba Mbondjo, Basile Kabiena, & Gamom Ngounou Ewo, 2024).

Table 1 compares existing cybersecurity frameworks with the proposed MGMA-based approach, highlighting how the latter addresses the specific needs of African higher education institutions.

Table 1: Literature Review

#	SOURCE	EXISTING FRAMEWORK/INSIGHT	COMPARING EXISTING FRAMEWORKS WITH THE PROPOSED MGMA-BASED APPROACH
1	(Chigada, 2023)	**South African National Cybersecurity Policy Framework**	This framework focuses on aligning national-level cybersecurity policies. The MGMA-based approach, while incorporating national policies, emphasises institutional alignment with specific cybersecurity risks and interdependencies at the university level.
2	(Eltahir & Ahmed, 2023)	**Cybersecurity Awareness in African HEIs**	The focus on awareness-raising is critical, but the MGMA approach goes further by integrating governance, policy, and technical solutions tailored to address the specific vulnerabilities of African HEIs.
3	(Gujar, Thiyagarajan, Sakpal, & Pandey, 2024)	**Advanced Cybersecurity Frameworks for Academic Libraries**	Focuses on protecting sensitive data in academic libraries using innovative technical controls.
4	(Hesham et al., 2024)	**Machine Learning for Threat Detection**	This study emphasises predictive models for threat detection using MGMA.
5	(Kibuku, Ochieng, & Wausi, 2020).	**Challenges in e-Learning**	Identifies cybersecurity challenges in e-learning environments, focusing on technology gaps. The MGMA framework addresses these gaps by linking technical solutions to governance and policy improvements, ensuring a holistic approach to e-learning security.
6	(Kure, 2021)	**Integrated Cybersecurity Risk Management (I-CSRM) Framework**	The MGMA approach similarly emphasises integrated risk management but adapts it to the educational sector, ensuring alignment with institutional objectives and constraints.
7	(Lakhno et al., 2024)	**Analysis of Digital Footprints in University Systems**	This study focuses on behaviour patterns within university systems. The MGMA-based framework would include such behavioural analyses but expand to evaluate the interrelation of digital behaviours with governance, policy, and resource allocation.
8	(Lantada et al., 2020)	**Disaster Risk Reduction Using Morphological Analysis**	This MGMA approach similarly applies this method to cybersecurity, enabling a detailed exploration of interdependencies in university systems to create a tailored risk management framework.
9	(Mtakati & Sengati, 2024).	**Cybersecurity Posture of Higher Education Institutions in Tanzania**	This MGMA framework adds to this by offering strategic solutions for improving cybersecurity maturity through governance and resource allocation.
10	(Ngounou Ngounou et al., 2024).	**National Cybersecurity Capability Maturity Model for Cameroon**	This MGMA-based approach would similarly evaluate institutional maturity but emphasise institutional collaboration and resource-sharing across African HEIs to build resilience.
11	(Ritchey, 2022)	**General Morphological Analysis Overview**	This MGMA-based approach applies these principles to cybersecurity, enabling African HEIs to address their cybersecurity challenges systematically through structured problem-solving.
12	(Roodt et al., 2020)	**Complex Societal Problem Modelling**	The MGMA approach in this paper applies GMA to complex cybersecurity challenges in HEIs, mapping out interdependencies between governance, technology, and resources.
13	(Ulven & Wangen, 2021)	**Systematic Review of Cybersecurity Risks in HEIs**	This MGMA-based approach reviews risks in higher education but does not offer specific frameworks.
14	(Vassilakos & Martin, 2023)	**Cybersecurity in the Southern African Development Community (SADC)**	This MGMA-based framework aligns with this holistic view but focuses on institutional solutions for HEIs, emphasising adaptability and collaboration to address regional challenges.
15	(Hamdani et al., 2021)	**Cybersecurity standards in the context of operating system: Practical aspects, analysis, and comparisons**	This paper analyses cybersecurity standards around operating systems, looking at their practical implementation. However, it does not look into the broader, multidimensional challenges specific to higher education. Our proposed framework extends beyond technical standards to provide a holistic framework focused on the unique needs of HEIs.

4. The Cybersecurity Threat Landscape in African Higher Education Institutions

4.1 Current Cybersecurity Threat Landscape

The digital transformation of African higher education institutions has brought numerous benefits and exposed them to many cyber threats (Kibuku et al., 2020). As universities increasingly rely on digital platforms for teaching, administration, and research, they become more vulnerable to cyberattacks. Phishing, malware, ransomware, and denial-of-service (DoS) attacks are just some of the many threats institutions must now defend against daily. The sensitive nature of the data stored by these institutions—from personal student information to confidential research data—makes them prime targets for cybercriminals seeking financial gain or access to valuable intellectual property (Gujar et al., 2024).

Unlike in other parts of the world where universities may have more robust, more developed cybersecurity measures, African HEIs often face significant resource constraints. Many institutions lack the funding, personnel, and expertise to mount effective defences against these increasingly sophisticated cyber threats. As a result, African universities are often left playing catch-up, scrambling to respond to cyber incidents after they have already occurred rather than preventing them proactively.

4.2 Unique Challenges Faced by African Institutions

The challenges faced by African higher education institutions are unique and multifaceted. Financial limitations are one of the most significant barriers to implementing strong cybersecurity measures (Mtakati & Sengati, 2024). Many institutions operate on tight budgets, and cybersecurity is often viewed as a secondary priority compared to other pressing needs, such as expanding access to education or improving basic infrastructure. The costs associated with purchasing advanced cybersecurity tools, training staff, and maintaining secure IT systems are often prohibitive for African HEIs, further compounding their vulnerability.

Moreover, the lack of cybersecurity expertise on the continent poses another critical challenge (Kaibiru, Karume, Kibas, & Onga'nyo, 2023). While some institutions have begun developing cybersecurity programs and training specialists, there is still a significant shortage of skilled professionals who can effectively manage and defend against cyber threats. This skills gap leaves many universities relying on outdated or inadequate security practices, making them even more susceptible to attacks. Additionally, the diverse and often decentralised nature of academic environments complicates the implementation of unified cybersecurity policies across institutions (Yusif & Hafeez-Baig, 2023). Ensuring comprehensive protection becomes an enormous task with multiple campuses, varied administrative systems, and numerous users—ranging from students and faculty to third-party contractors.

4.3 Cybersecurity Readiness and Maturity in Africa

African HEIs also tend to lag in terms of cybersecurity readiness and maturity (Ngounou Ngounou et al., 2024). While many institutions in other regions have invested in sophisticated cybersecurity frameworks and integrated risk management processes, African universities often operate without comprehensive cybersecurity strategies. Many institutions lack dedicated cybersecurity teams, and the absence of structured protocols for responding to cyber incidents leaves them vulnerable to even the most basic forms of attack (Vassilakos & Martin, 2023). This reactive approach to cybersecurity risks critical data and threatens the institutions' reputations and financial stability in the event of a severe breach (Kure, 2021).

In addition, the absence of a cohesive legal framework for cybersecurity in many African countries further complicates efforts to secure higher education institutions (Chigada, 2023). Without national cybersecurity standards or regulations, universities are left to develop their security practices in isolation, often leading to fragmented and inconsistent approaches across the sector. Despite these challenges, there is growing recognition of the need to address these issues, with efforts underway to improve cybersecurity awareness, capacity building, and collaboration across the continent.

5. Methodology: Modified General Morphological Analysis

5.1 MGMA Model

The MGMA approach allows African HEIs to systematically deconstruct their cybersecurity landscape, identifying key vulnerabilities and critical security elements. MGMA can zero in on the particular requirements of resource-limited environments, providing a structured pathway to explore viable cybersecurity strategies tailored to African institutions' needs (Lantada et al., 2020).

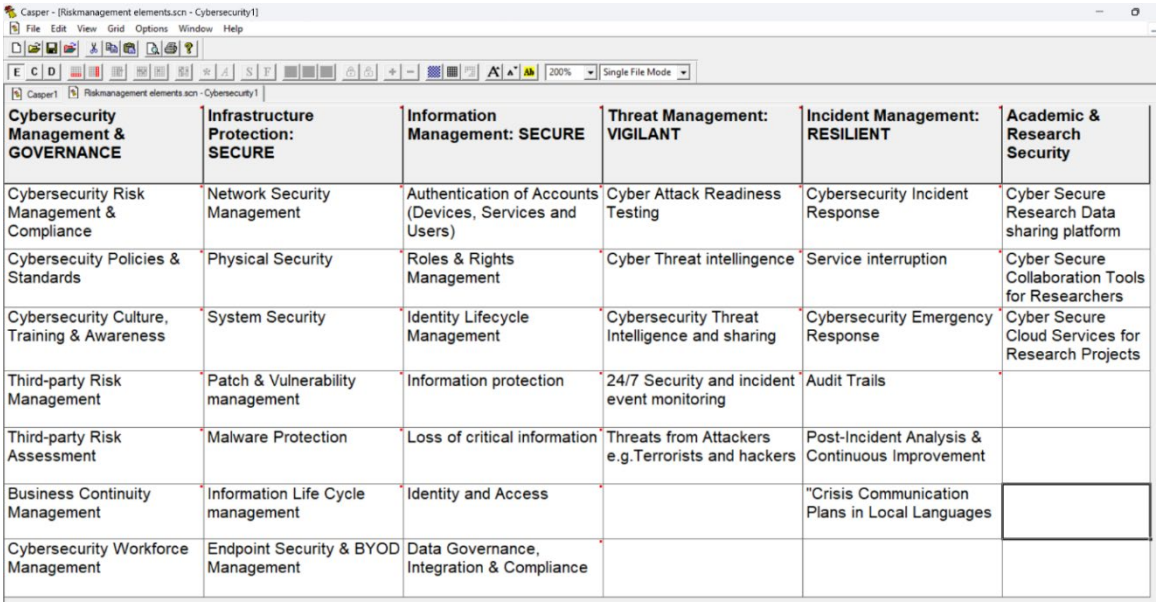
This study used MGMA to construct a morphological matrix that categorises and analyses essential cybersecurity components across governance, technical controls, policy, resource allocation, and capacity development. Each of these dimensions is dissected into specific variables, with possible states or configurations mapped out along the matrix axes, allowing for a thorough examination of how these elements interact to strengthen or undermine cybersecurity. Figure 1 provides a matrix of the MGMA model used for this study, illustrating the key dimensions and elements critical to enhancing cybersecurity resilience within African higher education institutions. This matrix allows for systematically examining all possible combinations of these factors, providing a holistic view of how they interact (Hesham et al., 2024).

5.2 Framework for Evaluating Cybersecurity Elements

The strength of MGMA lies in its capacity to explore a problem from multiple dimensions, uncovering interdependencies and identifying optimal solutions (Lakhno et al., 2024). Figure 2 illustrates the MGMA framework's morphological matrix, providing a structured layout to evaluate the relationships among crucial cybersecurity elements, where each connection is denoted as vital (-), uncertain (K), or non-existent (X). For instance, governance may encompass executive involvement, adherence to national regulations, or internal policy frameworks. Factors such as network segmentation, encryption protocols, and endpoint security are considered to be on the technical side. By systematically examining these combinations, the MGMA model reveals which configurations are most effective for enhancing cybersecurity posture in a higher education setting. This matrix approach allows insights beyond isolated technical fixes, encouraging a more nuanced and comprehensive view of cybersecurity risks and responses.

5.3 Identifying Critical Cybersecurity Dimensions Using MGMA

The MGMA process continues by identifying the critical cybersecurity dimensions that should be prioritised within African HEIs. By evaluating different combinations of governance structures, technology applications, policy enforcement, and resource distributions, MGMA helps uncover which elements hold the most significant impact on institutional cybersecurity.



Cybersecurity Management & GOVERNANCE	Infrastructure Protection: SECURE	Information Management: SECURE	Threat Management: VIGILANT	Incident Management: RESILIENT	Academic & Research Security
Cybersecurity Risk Management & Compliance	Network Security Management	Authentication of Accounts (Devices, Services and Users)	Cyber Attack Readiness Testing	Cybersecurity Incident Response	Cyber Secure Research Data sharing platform
Cybersecuity Policies & Standards	Physical Security	Roles & Rights Management	Cyber Threat intellingence	Service interruption	Cyber Secure Collaboration Tools for Researchers
Cybersecurity Culture, Training & Awareness	System Security	Identity Lifecycle Management	Cybersecurity Threat Intelligence and sharing	Cybersecurity Emergency Response	Cyber Secure Cloud Services for Research Projects
Third-party Risk Management	Patch & Vulnerability management	Information protection	24/7 Security and incident event monitoring	Audit Trails	
Third-party Risk Assessment	Malware Protection	Loss of critical information	Threats from Attackers e.g.Terrorists and hackers	Post-Incident Analysis & Continuous Improvement	
Business Continuity Management	Information Life Cycle management	Identity and Access		"Crisis Communication Plans in Local Languages	
Cybersecurity Workforce Management	Endpoint Security & BYOD Management	Data Governance, Integration & Compliance			

Figure 1: Cybersecurity Risk Management Elements

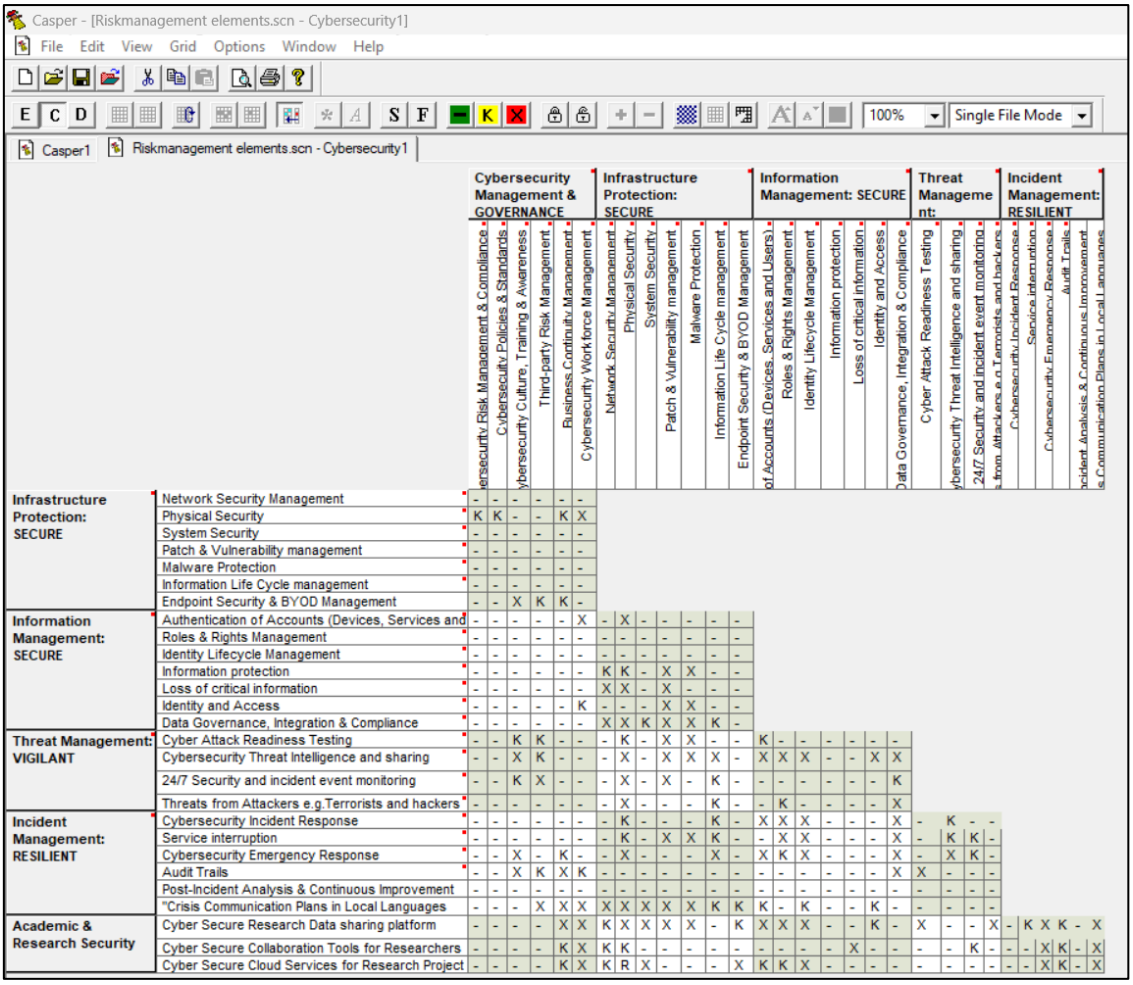


Figure 2: Relationships among elements

The following dimensions are pivotal to this analysis:

- **Governance and Policy**: Strong leadership commitment and well-defined, enforceable policies are essential. These policies must be adaptable and routinely updated to reflect the shifting threat landscape.
- **Technical Controls**: Core technical defences—such as firewalls, intrusion detection, and encryption—must be effective, but MGMA also considers the potential integration of emerging technologies tailored to institutional needs.
- **Capacity Building**: Training and awareness programs for staff and students are indispensable. MGMA evaluates current competency levels and identifies areas for targeted skill development to build a knowledgeable cybersecurity workforce.
- **Resource Allocation**: With limited budgets, African HEIs must allocate financial, technical, and human resources strategically. MGMA allows for a comparative assessment to determine where resources will yield the highest impact, helping institutions focus on priorities with the most significant security returns.

By identifying these interconnected factors, MGMA provides African HEIs with a roadmap for allocating their resources in ways that maximise security resilience.

5.4 Benefits of MGMA for African Higher Education Institutions

MGMA offers a holistic cybersecurity approach for African Higher Education Institutions (HEIs), integrating institutional, policy, and human elements. It helps institutions balance technical and organisational measures, highlighting the importance of robust governance and policy structures. MGMA's adaptability allows for regular updates, ensuring the framework remains responsive to emerging threats and evolving institutional needs, allowing institutions to focus on critical areas and achieve meaningful security improvements.

6. Key Findings: Cybersecurity Elements for Higher Education Institutions

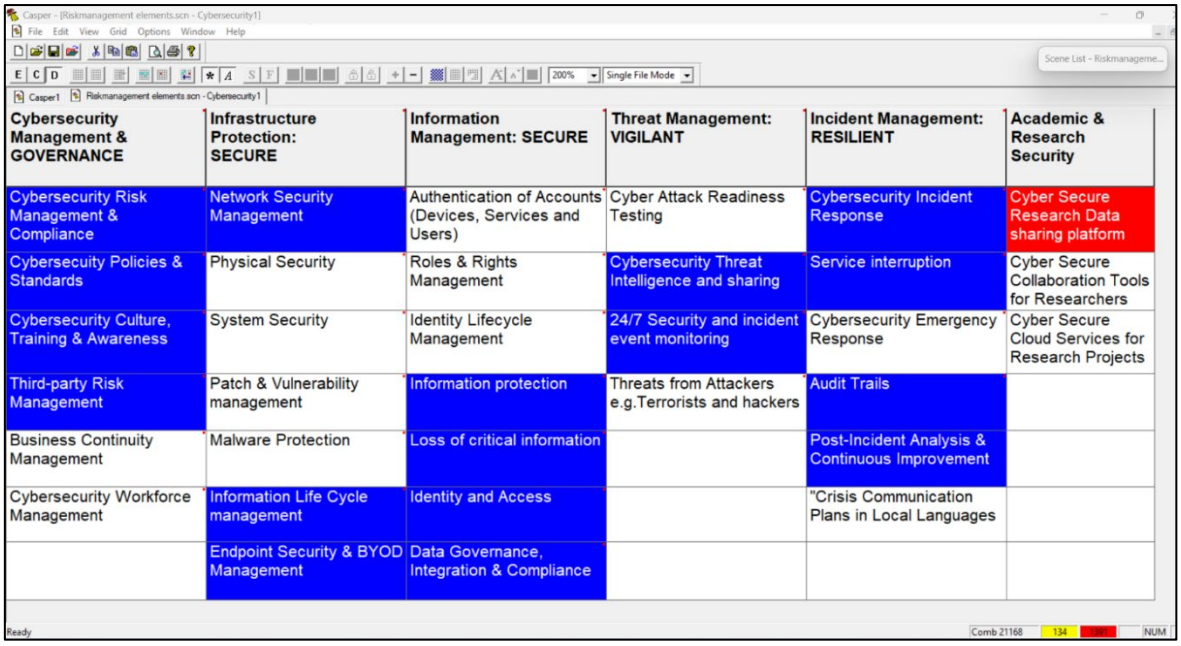
The application of MGMA in this study has highlighted several critical elements necessary for developing a robust cybersecurity framework tailored to the specific needs of African HEIs. These elements, summarised in Table 2, address African HEIs' distinct challenges, including resource limitations, a diverse user population, and the constant evolution of cyber threats. Through a systematic evaluation of governance structures, technical controls, capacity-building initiatives, and institutional collaboration, MGMA provides a roadmap for enhancing cybersecurity resilience.

The key findings in Table 2 focus on four main dimensions: Governance and Policy Development, Technical Controls and Resource Allocation, Capacity Building and Institutional Collaboration, and Academic and Research Security.

Figure 3 presents the resulting relationship analysis, highlighting specific interactions between elements such as the Cyber Secure Research Data Sharing Platform and other core components within the cybersecurity framework. These dimensions collectively shape the cybersecurity approach of African HEIs and determine the strength of their overall security posture. Each dimension is interdependent, and understanding these connections is essential for developing a cybersecurity strategy that is both resilient and adaptable.

Table 2: Key Cybersecurity Elements Identified Using MGMA

Dimension	Key Element	Description
Governance and Policy Development	**Leadership Engagement**	Active participation of institutional leadership in shaping and enforcing cybersecurity priorities and policies.
	Policy Adaptation and Alignment	Develop and regularly update cybersecurity policies to ensure alignment with national and international standards.
	Risk Assessment Procedures	Systematic evaluations to identify vulnerabilities, assess risks, and prioritise cybersecurity actions.
Technical Controls and Resource Allocation	**Firewalls and Intrusion Detection**	Implementation of essential technical defences to monitor and prevent unauthorised access.
	Encryption Standards	Application of encryption protocols to secure sensitive data, including research outputs and student information.
	Regular System Updates and Patching	Continuous updates of systems to mitigate known vulnerabilities and safeguard against emerging threats.
	Targeted Resource Allocation	Strategic financial, technical, and human resource distribution to maintain and enhance cybersecurity measures.
Capacity Building and Institutional Collaboration	**Cybersecurity Training Programs**	Comprehensive training initiatives for staff, students, and faculty to foster cybersecurity awareness and skills.
	Cross-Institutional Collaboration	Partnerships with other institutions for resource sharing, knowledge exchange, and coordinated threat response.
	Skilled Cybersecurity Workforce	Investment in recruiting and training professionals equipped to manage and protect institutional cybersecurity assets.
Academic and Research Security	**Secure Research Data Sharing**	Develop secure platforms for exchanging research data in compliance with regional regulations.
	Collaborative Research Tools	Implementation of secure tools for collaboration on research projects across different institutions.
	Secure Cloud Services	Use of protected cloud services to support research activities, ensuring data integrity and compliance.



Cybersecurity Management & GOVERNANCE	Infrastructure Protection: SECURE	Information Management: SECURE	Threat Management: VIGILANT	Incident Management: RESILIENT	Academic & Research Security
Cybersecurity Risk Management & Compliance	Network Security Management	Authentication of Accounts (Devices, Services and Users)	Cyber Attack Readiness Testing	Cybersecurity Incident Response	Cyber Secure Research Data sharing platform
Cybersecuity Policies & Standards	Physical Security	Roles & Rights Management	Cybersecurity Threat Intelligence and sharing	Service interruption	Cyber Secure Collaboration Tools for Researchers
Cybersecurity Culture, Training & Awareness	System Security	Identity Lifecycle Management	24/7 Security and incident event monitoring	Cybersecurity Emergency Response	Cyber Secure Cloud Services for Research Projects
Third-party Risk Management	Patch & Vulnerability management	Information protection	Threats from Attackers e.g.Terrorists and hackers	Audit Trails	
Business Continuity Management	Malware Protection	Loss of critical information		Post-Incident Analysis & Continuous Improvement	
Cybersecurity Workforce Management	Information Life Cycle management	Identity and Access		"Crisis Communication Plans in Local Languages	
	Endpoint Security & BYOD Management	Data Governance, Integration & Compliance			

Figure 3: MGMA Relationship Analysis

6.1 Governance and Policy Development

Effective governance and adaptive policies are the foundation of any robust cybersecurity strategy. HEIs must establish well-defined cybersecurity policies, align them with national and international standards, and ensure regular updates to address new vulnerabilities. Active engagement from institutional leadership is vital to enforce these policies prioritising cybersecurity within the broader institutional agenda and allocating resources effectively.

6.2 Technical Controls and Resource Allocation

Technical controls—firewalls, encryption, and intrusion detection systems—are fundamental in safeguarding digital infrastructure. However, the efficacy of these tools hinges on adequate resources for their deployment and upkeep. African HEIs often face budgetary and technical constraints, so allocating resources for cybersecurity must be prioritised. This involves acquiring the necessary tools and ensuring proper configuration, regular updates, and continuous monitoring to counter evolving threats.

6.3 Capacity Building and Institutional Collaboration

One of the prominent challenges identified is the lack of skilled cybersecurity professionals within African HEIs. Through structured training and continuous professional development, capacity building is essential to close this gap. Additionally, collaboration among institutions—both within and across national boundaries—presents opportunities for sharing resources, expertise, and best practices, strengthening the cybersecurity resilience of the higher education sector.

6.4 Academic and Research Security

Protecting research data and intellectual property is a growing concern in research-oriented African universities. Academic and Research Security focuses on creating secure data-sharing platforms, implementing secure collaboration tools, and leveraging cloud services that comply with regional data protection regulations. This dimension underscores the importance of tailored security measures for research activities, ensuring that valuable data remains protected throughout its lifecycle.

7. Discussion and Implications

The findings derived from applying MGMA highlight a comprehensive set of cybersecurity elements essential for strengthening African HEIs against cyber threats. These elements—governance, policy, technical controls, resource allocation, capacity building, institutional collaboration, and research-specific security—are interconnected factors that together form a resilient cybersecurity posture. Addressing these areas, particularly in resource-limited contexts, gives African HEIs a structured framework for proactive cyber risk management.

7.1 Addressing Institutional Vulnerabilities

A significant insight from this study is the need for institutions to shift from reactive cybersecurity measures to a proactive, integrated approach. Weak governance structures and outdated policies often leave African HEIs vulnerable to cyber incidents. Embedding cybersecurity within institutional governance helps prioritise cybersecurity efforts, ensuring they align with broader institutional goals and receive adequate resources. Leadership engagement is pivotal, as it secures strategic direction and fosters a culture that values cybersecurity.

Regular policy alignment with national and international standards ensures compliance and equips institutions to counter the shifting threat landscape. Without updated and robust governance and policy frameworks, institutions are more likely to experience data breaches and security incidents that could have long-term financial and reputational consequences.

7.2 Collaborative Cybersecurity Efforts Across African Universities

The study also underscores the importance of collaboration among African HEIs, especially given many institutions' resource constraints. Institutions can bolster their cybersecurity capabilities by pooling knowledge, resources, and expertise. This collaboration can take various forms, such as joint training initiatives, shared threat intelligence platforms, and coordinated incident responses, enhancing cybersecurity resilience across the sector.

Collaboration can extend to partnerships with government agencies, private sector organisations, and international cybersecurity bodies. Such partnerships can offer African HEIs access to advanced tools, industry best practices, and additional funding, otherwise difficult to secure independently. Shared cybersecurity awareness initiatives, for instance, can raise cyber hygiene standards among students, faculty, and staff, thereby reducing vulnerability to common threats.

7.3 Implications for Policy and Leadership

Finally, the findings emphasise that cybersecurity is a strategic issue requiring institutional leaders' active involvement. HEI leaders must go beyond delegating cybersecurity to IT departments, recognising it as a critical risk that affects the institution's reputation, financial stability, and long-term success. This shift demands that cybersecurity policies align with institutional goals and are agile enough to respond to emerging threats.

8. Proposed MGMA-Based Cybersecurity Framework for African HEIs

Building upon insights from the MGMA, this study proposes a cybersecurity framework specifically designed to address the pressing needs of African HEIs. This framework responds to the challenges of limited financial resources, scarce cybersecurity expertise, and the evolving nature of cyber threats faced by African HEIs. Anchored in MGMA principles, this framework underscores governance, resource optimisation, collaboration, and adaptability, ensuring cybersecurity measures align with the strategic goals of each institution.

8.1 Framework Overview

The MGMA-based cybersecurity framework is structured around core components: governance and policy, technical controls, capacity building, institutional collaboration, and academic and research security. These interconnected components form a comprehensive approach to managing cybersecurity risks, recognising cybersecurity as a strategic priority rather than merely a technical concern. This integrated approach requires active involvement from leadership, faculty, IT staff, and the broader academic community. At its core, the framework adopts a holistic view, understanding that effective cybersecurity relies on more than technical defences. Instead, it emphasises the complex interplay among governance, policy, technical solutions, and capacity-building efforts. Designed for flexibility, this framework can adapt as new threats emerge, enabling institutions to remain resilient and responsive in the face of shifting cyber risks.

8.2 Risk Management Processes

Risk management is central to the MGMA-based framework. Given the continuous evolution of cybersecurity threats, this framework encourages proactive risk management through ongoing assessment, prioritisation, and strategic mitigation. The process begins with a comprehensive risk assessment to identify potential vulnerabilities, including outdated systems, inadequate policies, or weak governance structures. Once identified, vulnerabilities are prioritised based on their potential impact on institutional assets and operations. This allows resource-limited institutions to focus first on securing their most critical assets—such as student data, research

outputs, and intellectual property—before expanding to other areas. Additionally, the framework stresses continuous monitoring and regular updates, ensuring that emerging vulnerabilities are promptly addressed.

8.3 Institutional Linkages and Resource Sharing

A vital advantage of the MGMA-based framework is its emphasis on collaboration and resource sharing among African HEIs. Given the typical resource constraints in the region, collective efforts can enable institutions to strengthen their cybersecurity stance beyond what would be achievable independently. The framework encourages the formation of institutional linkages, fostering a network of HEIs that share cybersecurity resources, expertise, and best practices. Institutions can co-invest in cybersecurity training programs through collaborative initiatives, building a workforce equipped to address complex cyber challenges. Additionally, institutions can share cybersecurity tools—such as threat detection systems and vulnerability assessment platforms—thereby reducing the financial burden on individual universities.

The framework also promotes the establishment of a shared threat intelligence network. By pooling knowledge on emerging cyber threats, HEIs can respond more swiftly to incidents and bolster their defences against future attacks. This collaborative approach shifts cybersecurity from isolated institutional efforts to a unified, sector-wide defence strategy, reinforcing the cybersecurity resilience of African higher education.

8.4 Flexibility and Adaptability of the Framework

One of the defining strengths of the MGMA-based framework is its inherent flexibility and adaptability. Cyber threats continually evolve, and this framework provides a structure that can dynamically respond to these changes. Institutions can ensure that their cybersecurity strategies remain effective and aligned with current risks by updating the morphological matrix and reassessing the interdependencies among governance, technology, and policy. This adaptability is especially valuable in Africa, where cyber threats can be unpredictable, and resource availability is often limited. The MGMA-based framework empowers institutions to make incremental adjustments to their cybersecurity practices as new challenges emerge rather than undertaking costly overhauls. By allowing institutions to tailor their strategies to fit their specific needs and circumstances, this framework offers a practical, sustainable approach to long-term cybersecurity management.

9. Conclusion

This study demonstrates how the MGMA can effectively support the development of a tailored cybersecurity framework for African higher education institutions. By systematically exploring multiple dimensions—governance, technical controls, policy alignment, resource allocation, and capacity building—the MGMA approach offers a structured, adaptable framework to address the specific cybersecurity challenges faced by African HEIs. The findings underscore the need for an integrated approach, where interdependent elements are considered collectively rather than in isolation. This integrated perspective aligns cybersecurity efforts with broader institutional objectives, fostering a more resilient, sustainable, and effective cybersecurity posture across the higher education sector.

Adopting an MGMA-based cybersecurity framework presents significant benefits for African HEIs, which operate under unique constraints such as limited funding, a shortage of cybersecurity expertise, and increasing reliance on digital infrastructure. By emphasising leadership involvement, adaptive policy development, and institutional collaboration, this framework provides a pragmatic path for enhancing cybersecurity resilience across African universities. Strategic resource allocation and a focus on capacity building empower even resource-constrained institutions to strengthen their defences against cyber threats. Moreover, the framework's adaptability allows institutions to remain responsive to the evolving cyber landscape, making it scalable and applicable to diverse HEIs, regardless of size or resource levels.

References

Chigada, J. (2023). Towards an aligned South African national cybersecurity policy framework.

Eltahir, M., & Ahmed, O. (2023). Cybersecurity awareness in African higher education institutions: A case study of Sudan. *Inf. Sci. Lett, 12*(1), 171-183.

Groš, S. (2021). *A critical view on CIS controls.* Paper presented at the 2021 16th International Conference on Telecommunications (ConTEL).

Gujar, S. S., Thiyagarajan, V., Sakpal, S. S., & Pandey, A. K. (2024). Advanced Cybersecurity Frameworks for Protecting Sensitive Information in Academic Libraries: Innovations and Best Practices. *Library Progress International, 44*(3), 198-209.

Hamdani, S. W. A., Abbas, H., Janjua, A. R., Shahid, W. B., Amjad, M. F., Malik, J., . . . Khan, A. W. (2021). Cybersecurity standards in the context of operating system: Practical aspects, analysis, and comparisons. *ACM Computing Surveys (CSUR), 54*(3), 1-36.

Hesham, M., Essam, M., Bahaa, M., Mohamed, A., Gomaa, M., Hany, M., & Elsersy, W. (2024). *Evaluating Predictive Models in Cybersecurity: A Comparative Analysis of Machine and Deep Learning Techniques for Threat Detection.* Paper presented at the 2024 Intelligent Methods, Systems, and Applications (IMSA).

Humphreys, E. (2016). *Implementing the ISO/IEC 27001: 2013 ISMS Standard*: Artech house.

Jansen van Vuuren, J., Leenen, L., Grobler, M. M., Chan, K. F. P., & Khan, Z. C. (2016). Morphological Ontology Design Engineering: A Methodology to Model Ill-Structured Problems. In *Mixed Methods Research for Improved Scientific Study* (pp. 262-291): IGI Global.

Jansen van Vuuren, J. C., Leenen, L., Grobler, M., Chan, K., & Khan, Z. (2015). *Modelling the cybersecurity environment using Morphological Ontology Design Engineering.* Paper presented at the 10th International Conference on Cyber Warfare & Security, Kruger National Park South Africa.

Kaibiru, R. M., Karume, S. M., Kibas, F., & Onga'nyo, M. L. B. (2023). Closing the Cybersecurity Skill Gap in Kenya: Curriculum Interventions in Higher Education. *Journal of Information Security, 14*(2), 136-151.

Kibuku, R. N., Ochieng, D. O., & Wausi, A. N. (2020). e-Learning Challenges Faced by Universities in Kenya: A Literature Review. *Electronic Journal of E-learning, 18*(2), pp150-161-pp150-161.

Kure, H. (2021). *An Integrated Cybersecurity Risk Management (I-CSRM) framework for critical infrastructure protection.* University of East London,

Lakhno, V., Kurbaiyazov, N., Lakhno, M., Kryvoruchko, O., Desiatko, A., Tsiutsiura, S., & Tsiutsiura, M. (2024). Analysis of digital footprints associated with cybersecurity behavior patterns of users of University Information and Education Systems. *International Journal of Electronics and Telecommunications*, 673-682-673-682.

Lantada, N., Carreño, M. L., & Jaramillo, N. (2020). Disaster risk reduction: a decision-making support tool based on the morphological analysis. *International journal of disaster risk reduction, 42*, 101342.

Mogoane, S. N., & Kabanda, S. (2019). *Challenges in Information and Cybersecurity program offering at Higher Education Institutions.* Paper presented at the ICICIS.

Mtakati, B., & Sengati, F. (2024). Cybersecurity posture of higher learning institutions in Tanzania. *The Journal of Informatics, 1*(1), 1-12.

Ngounou Ngounou, F., Matanga, J., Essomba Mbondjo, R., Basile Kabiena, I., & Gamom Ngounou Ewo, R. C. (2024). Design of a National Cybersecurity Capability Maturity Model for African Emerging Country: Case of Cameroon. *Jacques and Essomba Mbondjo, Richard and Basile Kabiena, Ivan and Gamom Ngounou Ewo, Roland Christian, Design of a National Cybersecurity Capability Maturity Model for African Emerging Country: Case of Cameroon*.

Ritchey, T. (2022). General morphological analysis: an overview.

Roodt, J. H., Leenen, L., Jansen van Vuuren, J. C., & Khan, Z. C. (2020). *Modelling Of The Complex Societal Problem Of Establishing A National Energy Sufficiency Competence.* Paper presented at the 2020 IEEE 23rd International Conference on Information Fusion (FUSION), Virtual Conference.

Ulven, J. B., & Wangen, G. (2021). A systematic review of cybersecurity risks in higher education. *Future Internet, 13*(2), 39.

Vassilakos, A., & Martin, R. (2023). Understanding the Challenge of Cybersecurity in Africa: A Holistic Analysis of Southern African Development Community (SADC) and Foundation for Future Research. *HOLISTICA–Journal of Business and Public Administration, 14*(1), 162-172.

White, G. B., & Sjelin, N. (2022). The NIST cybersecurity framework. In *Research Anthology on Business Aspects of Cybersecurity* (pp. 39-55): IGI Global.

Yusif, S., & Hafeez-Baig, A. (2023). Cybersecurity policy compliance in higher education: a theoretical framework. *Journal of Applied Security Research, 18*(2), 267-288.