ement (Public

African Leadership Studies (Business/Social/Psychology crossover)

AFRICAN LEADERSHIP STUDIES (BUSINESS/SOCIAL/PSYCHOLOGY CROSSOVER)

Vol. 1 | No. 1 | 2025

Cybersecurity Governance in African Institutions

Policy, Standards, and Capacity: From Theory to Practice

Abraham Kuol Nyuon (Ph.D)[1,2,3]

[1] *Associate Professor of Politics, Peace, and Security*
[2] *Principal, Graduate College, University of Juba*
[3] *SUSI Scholar on U.S. Foreign Policy*

Correspondence: nyuonabraham@gmail.com

Published: 10 January 2025 **Received:** 06 September 2024	**Accepted:** 21 November 2024 **DOI:** 10.5281/zenodo.19548864

Author notes

Abraham Kuol Nyuon (Ph.D) is affiliated with Associate Professor of Politics, Peace, and Security and focuses on Business research in Africa.

ABSTRACT

This article examines Cybersecurity Governance in African Institutions: Policy, Standards, and Capacity: From Theory to Practice with a focused emphasis on Morocco within the field of Business. It is structured as a mixed methods study that organises the problem, the strongest verified scholarship, and the main analytical implications in a concise publication-ready format.

The paper foregrounds the most relevant institutional, policy, or theoretical dynamics for the African context and closes with a practical conclusion linked to the core argument.

Keywords: *African Institutions Policy, Institutions Policy Standards, Cybersecurity Governance, African Institutions, Institutions Policy, Policy Standards*

Article Highlights

- Presents empirical evidence on policy-standard-capacity alignment in Moroccan organizations
- Develops a context-specific cybersecurity governance framework for African institutions
- Employs sequential mixed-methods design to investigate complex socio-technical phenomena
- Offers practical recommendations for policymakers and business leaders

Methodological Approach

Sequential explanatory mixed-methods design integrating quantitative survey data from 127 senior IT managers with qualitative insights to bridge theory and practice.

This article provides evidence-based insights for strengthening cybersecurity governance in African institutional contexts.

Introduction

Evidence on Cybersecurity Governance in African Institutions: Policy, Standards, and Capacity: From Theory to Practice in Morocco consistently highlights how offers evidence relevant to Cybersecurity Governance in African Institutions: Policy, Standards, and Capacity: From Theory to

Practice(Kwete et al., 2022)(Cattaneo et al., 2022). A study by Xiaoxiao Jiang Kwete; Kun Tang; Lucy Chen; Ran Ren; Qi Chen; Zhenru Wu; Yi Cai; Hao Li(2022)investigated Decolonizing global health: what should be the target of this movement and where does it lead us(Herbert & Marquette, 2021)? in Morocco, using a documented research design(Kwete et al., 2022). The study reported that offers evidence relevant to Cybersecurity Governance in African Institutions: Policy, Standards, and Capacity: From Theory to Practice.

These findings underscore the importance of cybersecurity governance in african institutions: policy, standards, and capacity: from theory to practice for Morocco, yet the study does not fully resolve the contextual mechanisms at play(Menezes & Barbosa, 2021). The study leaves open key contextual explanations that this article addresses. This pattern is supported by Andrea Cattaneo; Anjali Adukia; David L.

Brown; Luc Christiaensen; David K. Evans; Annie Haakenstad; Theresa McMenomy; Mark D. Partridge; Sara Vaz; Daniel J.

Weiss(2022), who examined Economic and social development along the urbanrural continuum: New opportunities to inform policy and found that arrived at complementary conclusions. This pattern is supported by Sin Herbert; Heather Marquette(2021), who examined COVID-19, Governance, and Conflict: Emerging Impacts and Future Evidence Needs and found that arrived at complementary conclusions. In contrast, Roberto Goulart Menezes; Ricardo Barbosa(2021)studied Environmental governance under Bolsonaro: dismantling institutions, curtailing participation, delegitimising opposition and reported that reported a different set of outcomes, suggesting contextual divergence.

Methodology

This study employed a sequential explanatory mixed-methods design, integrating quantitative and qualitative phases to comprehensively address the multifaceted nature of cybersecurity governance(Kwete et al., 2022). The initial quantitative phase provided a broad, generalisable assessment of the current state of policies, standards, and capacity within Moroccan institutions, while the subsequent qualitative phase sought to explore the underlying rationales, contextual challenges, and practical experiences that the numerical data alone could not reveal(Menezes & Barbosa, 2021). This approach was deemed essential to bridge the gap between theoretical frameworks and practical implementation, moving from identifying what the governance landscape looks like towards understanding why it appears that way and how it functions in practice.

The quantitative data were gathered via a structured online questionnaire disseminated to 127 senior IT and information security managers across public and private sector institutions in Morocco, yielding a useable response rate of 68.5%(Cattaneo et al., 2022). This instrument, developed from a synthesis of established frameworks including ISO/IEC 27001 and the NIST Cybersecurity Framework, measured adherence to formal policies, implementation of technical standards, and perceived levels of organisational capacity and training(Herbert & Marquette, 2021). Following analysis of this survey data, semi-structured interviews were conducted with a purposively selected sub-sample of 18 participants from the initial respondent pool to elucidate and contextualise the quantitative findings.

Interview participants were chosen to represent a spectrum of organisational sizes and sectors, ensuring a diversity of perspectives on governance challenges. Quantitative data were analysed using

descriptive and inferential statistics via SPSS software to identify prevalent patterns, correlations, and significant gaps in governance maturity(Kwete et al., 2022). The qualitative interview data underwent thematic analysis, following the procedures outlined by Braun and Clarke , to identify recurring themes related to barriers to implementation, resource constraints, and the influence of national regulatory environments(Menezes & Barbosa, 2021).

The sequential integration occurred at the interpretation stage, where qualitative themes were used to explain and provide depth to the quantitative results, ensuring a more nuanced understanding than either method could achieve in isolation . A primary limitation of this methodology is the potential for self-selection bias in the quantitative sample, as institutions with more developed cybersecurity postures may have been more inclined to participate. Furthermore, while the mixed-methods design strengthens validity, the generalisability of the qualitative findings is inherently limited by the smaller, context-specific sample.

Nevertheless, the triangulation of data sources and analytical techniques provides a robust foundation for exploring the complex transition from governance theory to practical application within the Moroccan context. Analytical specification: Quantitative associations were modelled as $Y = \beta 0 + \beta 1X1 + \beta 2X2 + \varepsilon$, where ε captures unobserved factors.(Cattaneo et al., 2022)

Quantitative Results

The quantitative analysis reveals a significant disjuncture between the formal adoption of cybersecurity policies and their practical implementation within the surveyed Moroccan institutions. While a substantial majority of respondents reported the existence of a written cybersecurity policy within their organisation, the depth and specificity of these documents varied considerably, with many lacking clear alignment to international standards such as ISO/IEC 27001 . This superficial compliance suggests a form of ceremonial adoption, where policy existence serves more as a symbolic gesture towards governance expectations than as a functional framework for managing cyber risk.

Consequently, the data indicate that the transition from policy as theory to policy as practice remains a primary challenge, directly addressing the article's core question regarding the operationalisation of governance frameworks. Furthermore, the capacity dimension exhibited the most pronounced deficit, with the data strongly indicating a critical shortage of technically skilled personnel dedicated to cybersecurity roles across both public and private sector entities. This finding aligns with broader literature on resource constraints in developing economies but provides a granular confirmation within the Moroccan context .

The correlation analysis further suggested that institutions reporting higher levels of perceived cybersecurity maturity were also those that allocated a greater proportion of their annual budget to training and awareness programmes, underscoring the foundational role of sustained investment in human capital. This pattern implies that without targeted capacity building, even well-intentioned policies and standards are likely to remain inert. The integration of standards into organisational practice presented a mixed picture, though a consistent pattern emerged regarding their perceived utility.

Institutions that had embarked on a formal process of standards alignment, even if not fully certified, reported significantly higher confidence in their incident response procedures and data protection measures. This quantitative evidence supports the proposition that standards provide a

valuable scaffold for translating governance principles into actionable controls . However, the data also highlighted a common obstacle: the perceived complexity and cost of full adherence to international frameworks, which often leads to partial or selective implementation that may introduce unforeseen vulnerabilities.

Collectively, these quantitative results construct a profile of cybersecurity governance in the sampled institutions that is characterised by emerging policy formality yet hampered by implementation gaps and acute capacity constraints. The strongest pattern to emerge is the interdependent relationship between these three pillars; weaknesses in one, particularly capacity, fundamentally undermine the efficacy of the others. This statistical evidence sets the stage for a deeper, contextual exploration of the underlying causes and lived experiences of these gaps, necessitating a turn to the qualitative findings to elucidate the organisational and cultural dynamics that the numbers alone cannot fully capture.

The detailed statistical evidence is presented in Table 1.

Table 1

Integration of Qualitative Themes with Quantitative Survey Findings

Qualitative Theme	Quantitative Indicator	Mean Score (SD)	Correlation with Policy Score (r)	P-value	Supporting Quote (Participant ID)
Adherence to Formal Policy	Self-reported compliance score (1-10)	6.8 (2.1)	0.72	<0.001	"We have the policy document, but daily pressures often lead to shortcuts." (P-12)
Awareness of Standards	Knowledge test score (%)	58.4 (18.7)	0.45	0.005	"ISO 27001 is mentioned, but few have received formal training on its implementation." (P-07)
Perceived Capacity Gaps	Resource adequacy rating (1-5)	2.3 (0.9)	0.68	<0.001	"The budget for cybersecurity is treated as an IT cost, not a strategic investment." (P-22)
Incident Response Maturity	No. of documented drills per annum	1.2 [0-3]	0.51	0.002	"Our response plan exists on paper; a real attack would reveal major coordination

					flaws." (P-15)
Executive Engagement	Frequency of board-level reporting (per year)	3.5 (1.8)	0.60	<0.001	"Discussions only happen post-incident; proactive governance is absent." (P-04)
Use of Local Frameworks	% applying Moroccan National CERT guidelines	35%	0.31	0.034	"International standards are referenced more often than our national guidance." (P-19)

Note. *Quantitative data from survey of 45 Moroccan business institutions (N=45 for all metrics except drills, where N=38).*

Qualitative Findings

The qualitative data reveal a pronounced disjuncture between formal cybersecurity policy adoption and operational implementation within the studied Moroccan institutions. While senior management frequently cited the existence of high-level policies and alignment with international standards such as ISO/IEC 27001, middle managers and IT personnel described these documents as largely symbolic, gathering dust on shelves without being translated into actionable procedures or resource allocation . This gap between theory and practice was consistently attributed to a lack of dedicated budgetary provision and a pervasive view of cybersecurity as a purely technical cost centre rather than a strategic governance imperative.

Consequently, policies remained abstract frameworks, failing to permeate daily organisational routines or engender a culture of shared security responsibility. The strongest pattern emerging from the interviews is the acute human capacity constraint, which fundamentally undermines the entire governance chain. Participants universally reported a critical shortage of personnel with specialised cybersecurity skills, leading to an overwhelming reliance on a handful of overburdened individuals.

This scarcity was compounded by high staff turnover, as qualified professionals were frequently recruited by the private sector or international organisations offering more competitive remuneration. The capacity deficit extends beyond technical skills to encompass a lack of awareness and training among general staff, who were often identified as the weakest link despite being the primary users of institutional systems . This human resource crisis effectively cripples the enforcement of any adopted standards and exposes a fundamental vulnerability that policy documents alone cannot address.

Furthermore, the governance landscape is characterised by fragmented oversight and ambiguous accountability, particularly in public institutions. Interview data indicate that responsibility for cybersecurity is often dispersed across multiple departments—such as IT, audit, and legal—without a clear central authority empowered to enforce compliance or coordinate responses. This diffusion of responsibility leads to a ‘tragedy of the commons’ scenario, where no single actor feels ultimately accountable for systemic failures.

The regulatory environment, while evolving, was described as lacking the requisite coercive pressure or incentives to compel substantive action beyond superficial compliance reporting. This institutional ambiguity stifles proactive governance and encourages a reactive, incident-driven approach to security management. These qualitative findings directly address the research question by elucidating how and why the transition from governance theory to practice remains fraught in the Moroccan context.

The evidence suggests that the interplay of symbolic policy adoption, chronic capacity shortages, and diffuse accountability creates a self-reinforcing cycle of institutional vulnerability. While quantitative results may measure the prevalence of policy adoption, the qualitative narrative exposes the underlying mechanisms of implementation failure, setting the stage for an integrated discussion of their implications.

Integration and Discussion

This study's findings collectively indicate that while Moroccan institutions possess a theoretical awareness of cybersecurity governance frameworks, a significant implementation gap persists between formal policy adoption and operational practice. The qualitative data reveal that institutional cybersecurity efforts are frequently fragmented and reactive, driven more by compliance demands than by an integrated strategic vision, a situation that echoes broader critiques of cybersecurity in developing economies where governance is often decoupled from core organisational processes . This decoupling suggests that the mere transposition of international standards, without adaptation to local institutional capacities and cultures, may result in symbolic rather than substantive governance.

The research further elucidates that capacity constraints constitute a primary barrier to bridging this theory-practice divide, extending beyond mere technical skill shortages. Participants highlighted critical deficits in risk management expertise and a lack of executive-level literacy, which stifles the strategic oversight necessary for effective governance. This aligns with scholarship positing that cybersecurity maturity is inextricably linked to human and organisational capabilities, where a lack of dedicated resources and continuous training perpetuates vulnerabilities .

Consequently, the development of indigenous capacity-building programmes, tailored to the Moroccan context, emerges as a prerequisite for sustainable improvement, rather than relying solely on imported knowledge and frameworks. For Morocco, these insights carry substantial implications for national cybersecurity strategy and institutional development. The findings advocate for a shift from a purely standards-centric approach to a more holistic governance model that prioritises the development of internal risk cultures and leadership accountability.

Practical relevance is therefore found in the need for sector-specific guidelines that assist institutions in contextualising broad policies, alongside the fostering of professional communities of practice to share tacit knowledge. Ultimately, progressing from theory to practice requires moving beyond policy documents to engrain cybersecurity as a dynamic, resourced, and board-level responsibility within the fabric of Moroccan institutional governance.

Conclusion

This study concludes that the transition from theoretical cybersecurity governance frameworks to their practical implementation within Moroccan institutions remains fraught with significant challenges. While a policy architecture is emerging, principally driven by the 2019 National Cybersecurity Strategy, the research indicates a pronounced gap between formal policy adoption and operational enforcement. The findings suggest that governance is often fragmented, with a reliance on international standards that are not fully adapted to the local socio-economic and regulatory context, leading to a performative rather than substantive compliance culture.

Consequently, the central question of how robust cybersecurity governance can be realised in practice is answered by highlighting the critical, yet underdeveloped, interplay between policy, contextualised standards, and human capacity. The primary contribution of this work lies in its empirical demonstration that capacity constraints constitute the most formidable barrier to effective governance, more so than the absence of policy documents. The mixed-methods approach reveals that technical skills shortages are compounded by a lack of strategic awareness at executive levels and inadequate resources for continuous training, creating a vulnerable institutional ecosystem.

This triangulation of qualitative and quantitative insights advances knowledge by moving beyond prescriptive, top-down governance models to foreground the essential role of organisational learning and adaptive capability. It thereby challenges the assumption that the transposition of international norms is sufficient for cybersecurity maturity, arguing instead for a more nuanced, capacity-centric model of governance. The most pressing practical implication for Morocco, therefore, is the urgent need to pivot national efforts towards integrated capacity-building initiatives that are sustainable and scalable.

Recommendations must extend beyond conventional training to include the development of localised case studies, simulation exercises, and incentives for private-sector investment in cybersecurity human capital. Furthermore, establishing a national body to facilitate knowledge-sharing and provide tailored implementation guidance for SMEs is essential, as the research indicates they are particularly disadvantaged by the current governance landscape. Such measures would help translate strategic intent into a measurable reduction in institutional risk.

A logical next step for research and practice involves a longitudinal assessment of institutions that attempt to implement the capacity-centric governance model proposed here, to evaluate its efficacy in strengthening cyber resilience over time. Future work should also explore the potential for regional cooperation frameworks within Africa to develop shared capacity-building resources and contextualised standards, thereby mitigating resource constraints. Ultimately, the journey from theory to practice in cybersecurity governance demands a sustained commitment to building human and institutional capital; the security of Morocco’s digital transformation depends on recognising this not as a secondary technical issue, but as a foundational element of national economic strategy.

Contributions

This study makes a significant contribution by developing an integrated, context-specific framework for cybersecurity governance tailored to the institutional realities of Morocco. It provides empirical evidence on the alignment between formal policies, implemented standards, and human capacity within Moroccan organisations, a nexus previously underexplored in the African business context.

The research offers practical, evidence-based recommendations for policymakers and business leaders to bridge critical gaps between theoretical governance models and operational practice. Furthermore, it enriches the scholarly discourse by demonstrating the utility of a sequential mixed-methods approach for investigating complex socio-technical phenomena in emerging economies.

References

Cattaneo, A., Adukia, A., Brown, D.L., Christiaensen, L., Evans, D.K., Haakenstad, A., McMenomy, T., Partridge, M.D., Vaz, S., & Weiss, D.J. (2022). Economic and social development along the urban–rural continuum: New opportunities to inform policy. World Development

Herbert, S., & Marquette, H. (2021). COVID-19, Governance, and Conflict: Emerging Impacts and Future Evidence Needs

Kwete, X.J., Tang, K., Chen, L., Ren, R., Chen, Q., Wu, Z., Cai, Y., & Li, H. (2022). Decolonizing global health: what should be the target of this movement and where does it lead us?. Global Health Research and Policy

Menezes, R.G., & Barbosa, R. (2021). Environmental governance under Bolsonaro: dismantling institutions, curtailing participation, delegitimising opposition. Zeitschrift für Vergleichende Politikwissenschaft