© Journal of Security Management, Policy & Administration, Nigerian Defence Academy, Kaduna. Vol. 3, ISSUE 1, 2025 ISSN: 2971-7973
Available on https://jsmpa.com.ng. Benjamin Tough & Emmanuel Shaaperah

Cybersecurity, Governance and Data Protection Compliance in Sub-National Public Institutions in Benue State: An Assessment of Digital Transformation Agenda

By

Benjamin T. Tough

&

Emmanuel Shaaperah

Of
Department of Public Administration, Rev. Fr. Moses Orshio University, Makurdi

Abstract

Digitalisation of public institutions has increased cybersecurity and data protection risks at all level. In Nigeria, weak governance structures, unclear roles, and limited staff capacity hinder effective Nigeria Data Protection Regulations (NDPR) compliance. In Benue State, poor policy enforcement and accountability mechanisms threaten data security, privacy, and sustainable digital governance. It is against this backdrop that the study examined cybersecurity governance and data protection compliance in sub-national public institutions, with specific focus on Benue State's digital transformation agenda with a specific focus on organizational structures, staff capacity, and institutional practices on compliance with the Nigeria Data Protection Regulation (NDPR) and international data protection standards. A survey research design was adopted, and data were collected from staff of selected ministries, departments, and agencies using structured questionnaires. Institutional theory was adopted as a theoretical framework for the study. The findings showed that organisational structures were found to lack clearly defined roles, reporting systems, and accountability mechanisms necessary for effective data protection. Staff capacity was identified as a critical constraint, as inadequate training and limited resources hinder consistent compliance. However, institutional monitoring and accountability practices showed relatively stronger influence on compliance with international data protection standards. The study concludes that effective digital transformation at the sub-national level requires robust cybersecurity governance, strengthened organisational frameworks, continuous capacity-building, and enforceable compliance mechanisms. It recommends improved policy enforcement, institutional restructuring, targeted staff training, and alignment with national and international data protection standards to ensure sustainable and secure digital governance in Benue State.

Keywords: **Cybersecurity governance, data protection compliance and digital transformation.**

1. INTRODUCTION

The digital transformation of public institutions has become a defining feature of governance worldwide, enabling governments to enhance service delivery, promote transparency, and engage citizens more effectively. Globally, digital transformation in public administration has been accompanied by rising cybersecurity threats, including ransomware, data breaches, and unauthorised access to sensitive information. The International Telecommunication Union (2022) reported that over 40% of public sector organisations globally have experienced significant cyber incidents in recent years. The union emphasised the urgent need for strong cybersecurity governance and effective data protection systems within public institutions. Globally recognised frameworks such as ISO/IEC 27001 and the NIST Cybersecurity Framework provide structured guidelines for embedding cybersecurity into organisational strategy, risk management processes, and accountability mechanisms. Similarly, the European Union's General Data Protection Regulation (GDPR) sets strict standards for the protection of personal data, with particular emphasis on transparency, data integrity, and the rights of citizens. Evidence from jurisdictions that have adopted these frameworks shows that compliance with established cybersecurity and data protection standards enhances institutional resilience, reduces vulnerability to cyber threats, and strengthens public confidence in government operations (Bada & Sasse, 2019; Voigt & Von dem Bussche, 2017; Von Solms & Van Niekerk, 2013).

In Africa the implementation of cybersecurity governance and data protection frameworks faces even moreunique challenges. Many countries have established national data protection regulations, yet sub-national institutions often contend with limited resources, inadequate technical infrastructure, and insufficient skilled personnel, which hinder effective adoption and enforcement (Ahmad, Alsmadi, & Alrawashdeh, 2021). Moreover, disparities in digital capacity between urban and rural regions result in uneven compliance and vulnerability to cyber threats. Regional initiatives, such as the African Union Convention on Cybersecurity and Personal Data Protection (AUCC), aim to harmonise cybersecurity and privacy standards across the continent, but practical enforcement remains inconsistent due to institutional and technical constraints (ITU, 2022). These realities highlight the need for tailored approaches that consider the capacities and limitations of sub-national public institutions while aligning with international best practices.

Though the experience on the regional scale shades on digital governance in Nigeria. Digital governance has increasingly become a central focus at both federal and sub-national levels, The Nigeria Data Protection Regulation (NDPR), enacted in 2019 through the facilitation of

the National Information Technology Development Agency (NITDA), sets out comprehensive requirements for the collection, processing, and storage of personal data, as well as mechanisms for ensuring accountability and protecting citizen privacy (NITDA, 2019). Despite the legal framework, sub-national institutions, including state ministries, local government offices, and parastatals, often face challenges in fully implementing cybersecurity and data protection standards. Limited IT infrastructure, inadequate staff capacity, fragmented policy enforcement, and low awareness of regulatory requirements contribute to persistent vulnerabilities, exposing these institutions to cyber threats and undermining the delivery of essential services (Akinbode & Akinwale, 2020)

Benue State government in particular has embarked on a digital transformation agenda aimed at modernising public service delivery, enhancing efficiency, and promoting transparency. This includes the adoption of digital platforms for revenue collection, health service management, education administration, and citizen engagement. While these initiatives hold significant potential for improving governance and public service delivery, they also underscore the critical importance of robust cybersecurity governance and strict compliance with data protection regulations. Any lapse in these areas could compromise sensitive citizen data, disrupt public services, and erode trust in government institutions. Assessing cybersecurity governance and data protection has become critical means of deepening understanding about the subject matter The study is guided by the following objectives;

i. To examine the effects of cyber security policies on data protection compliance in Benue State's public institutions.
ii. evaluate the effect of organisational structures on data protection compliance in Benue State's ministries and agencies.
iii. determine how staff capacity influences adherence to the Nigeria Data Protection Regulation (NDPR) in Benue State's public institutions.
iv. examine the relationship between institutional practices and compliance with international data protection standards.

1.2 Hypotheses

The study formulates the following hypotheses to guide the study.

i. **Ho1:** Cybersecurity policies have no significant impact on data protection compliance in Benue State's public institutions.
ii. **Ho2:** Organisational structures do not significantly affect data protection compliance in Benue State's ministries and agencies.
iii. **Ho3:** Staff capacity has no significant influence on adherence to the Nigeria Data Protection Regulation (NDPR) in Benue State's public institutions.
iv. **Ho4:** Institutional practices are not significantly related to compliance with international data protection standards in Benue State's public institutions.

1.3 Conceptual Review

Cybersecurity Governance

Cybersecurity governance is more than just a set of rules or technical protocols; it is the compass that guides an organisation through the complex and often perilous landscape of digital information management. At its core, cybersecurity governance refers to the structures, policies, and practices that ensure an organisation can anticipate, respond to, and recover from cyber threats while protecting critical information assets (Bada & Sasse, 2019). It is a framework that aligns an institution's digital security strategies with its overall mission, organisational objectives, and risk appetite. In other words, cybersecurity governance is the glue that binds technology, people, and processes to create a resilient digital environment where data and systems are safeguarded against both internal and external threats.

Globally, the importance of cybersecurity governance has grown exponentially as organisations face increasingly sophisticated cyberattacks. According to Von Solms and Van Niekerk (2013), organisations that fail to integrate cybersecurity into their governance structures are more likely to experience operational disruptions, financial losses, and reputational damage. The digital age has blurred the lines between technical and managerial responsibilities; cybersecurity is no longer the exclusive concern of IT departments but a collective responsibility of leadership, policy makers, and operational staff. In this sense,

governance transforms cybersecurity from a reactive technical task into a proactive organisational discipline, emphasising accountability, oversight, and strategic planning.

Effective cybersecurity governance involves several interrelated components. First, it requires the establishment of clear policies and procedures that define acceptable use, access control, data management, and response protocols. These policies serve as the institution's blueprint for managing risks and responding to incidents systematically rather than haphazardly (Ahmad, Alsmadi, & Alrawashdeh, 2021). Second, it involves organisational structures and roles that allocate responsibilities and ensure accountability. From leadership teams to technical staff, everyone within the institution has a role to play, whether in monitoring systems, assessing risks, or reporting breaches. Without clear roles and responsibilities, even the most sophisticated technological safeguards can fail. Third, cybersecurity governance integrates risk management and continuous monitoring, ensuring that emerging threats are identified early and mitigated promptly. This aspect of governance is particularly dynamic because cyber threats evolve rapidly, requiring organisations to be adaptive, resilient, and forward-looking.

Human factors play a critical role in cybersecurity governance. Technology alone cannot secure an organisation; people often represent the weakest link in digital defence. Training, awareness programs, and fostering a culture of security are essential for turning staff into active defenders of institutional data. Bada and Sasse (2019) emphasise that a governance framework without human engagement is incomplete because employees who understand the importance of cybersecurity are more likely to follow protocols, report anomalies, and contribute to a secure digital ecosystem. Thus, effective governance is as much about influencing behaviour and organisational culture as it is about deploying firewalls and encryption tools.

In practice, cybersecurity governance also extends to regulatory compliance and alignment with international standards. Frameworks such as ISO/IEC 27001 and the NIST Cybersecurity Framework guide the development of structured governance programs that are both comprehensive and auditable. Organisations that adopt these standards demonstrate not only a commitment to protecting information but also the ability to manage risk systematically and transparently (Voigt & Von dem Bussche, 2017). For public institutions, especially those at sub-national levels such as Benue State, this alignment is critical: citizens entrust sensitive personal data to government agencies, and breaches can undermine public confidence, disrupt

service delivery, and invite legal and financial consequences.

In essence, cybersecurity governance is a holistic and strategic approach to managing the digital frontier. It humanises technology by embedding policies, practices, and accountability into the organisational fabric, ensuring that people, processes, and systems work together to protect digital assets. It transforms cybersecurity from a reactive, technical necessity into a proactive, mission-driven imperative, safeguarding institutions against an ever-evolving landscape of threats. For sub-national public institutions, effective governance is not optional; it is essential for protecting sensitive citizen data, sustaining service delivery, and building trust in digital government initiatives.

Data Protection Compliance

Data Protection Compliance is the structured practice by which an organisation ensures that personal and sensitive information is handled responsibly, ethically, and securely. At its essence, it is about protecting individuals' privacy and ensuring that the collection, storage, processing, and dissemination of data meet established legal, ethical, and organisational standards. Compliance is not merely a set of technical rules; it reflects the commitment of an institution to safeguard the trust of those whose information it manages. It is the bridge between organisational responsibility and the individual's right to privacy, ensuring that data is used appropriately and only for intended purposes.

In practice, data protection compliance involves three critical dimensions. First is legal adherence, which ensures that an institution observes relevant laws and regulations governing data handling. In the Nigerian context, this is most notably reflected in the Nigeria Data Protection Regulation (NDPR), which outlines the rights of individuals and the responsibilities of organisations in collecting and managing personal data (NITDA, 2019). Legal compliance provides the foundation for all data protection activities, serving as a benchmark against which institutional practices are measured.

Second is the technical dimension, which encompasses the tools and processes used to protect data from unauthorised access, modification, or loss. This includes secure storage systems, access controls, encryption, regular system audits, and backup mechanisms. Technical safeguards ensure that data is not only stored but also protected against internal lapses and

external threats. These measures, however, are only effective when paired with organisational awareness and consistent application across the institution.

The third dimension is organisational culture and human engagement. Even with the strongest technical systems and well-drafted policies, data protection compliance depends heavily on the people within the organisation. Staff must understand their roles and responsibilities regarding data handling, follow established procedures, and remain vigilant against potential breaches. Training, awareness programs, and continuous reinforcement of ethical standards are therefore integral components of compliance. Research indicates that human error is often the weakest link in data protection; thus, cultivating a culture where every employee recognises the value of protecting information is as crucial as the technical infrastructure (Ahmad, Alsmadi, & Alrawashdeh, 2021).

Data Protection Compliance also entails accountability and transparency. Organisations are expected to document their data processing activities, maintain clear records of who has access to information, and be prepared to demonstrate compliance during audits or investigations. This accountability not only reduces the risk of breaches but also reinforces trust between the institution and its stakeholders. For public institutions, which routinely handle sensitive citizen data, such as health records, tax information, and personal identifiers, these principles are central to the legitimacy of the organisation.

Conceptually, compliance is not static; it is a dynamic and ongoing process. It requires continuous monitoring, evaluation, and adaptation of policies, practices, and technologies in response to new risks, evolving operational contexts, and changing legal requirements. A compliant organisation does not wait for breaches or legal enforcement to take action; it proactively assesses its practices, identifies vulnerabilities, and implements measures to protect data consistently. In this sense, data protection compliance reflects a culture of responsibility and foresight, where protecting information is embedded in every aspect of organisational operations.

Within the context of this study, data Protection Compliance is a multidimensional concept that integrates legal frameworks, technical safeguards, and human and organisational practices to protect personal and sensitive data. It represents both an ethical obligation and an operational necessity, ensuring that institutions manage information responsibly while maintaining the

trust and confidence of the public. For sub-national public institutions, particularly in the context of Benue State, achieving compliance is fundamental to protecting citizen data, ensuring the integrity of service delivery, and fostering accountability in the digital age.

1.4 Theoretical framework

Institutional Theory

Institutional Theory provides a compelling framework for understanding how organisations behave, particularly in contexts where compliance with rules, regulations, and social norms is essential. The theory was first articulated by John W. Meyer and Brian Rowan in 1977, with significant expansions by Paul DiMaggio and Walter Powell in 1983. At its core, Institutional Theory posits that organisations are deeply embedded in their social, political, and regulatory environments, and their structures, strategies, and practices are influenced not only by efficiency or technical considerations but also by the need to gain legitimacy and maintain stability within these broader institutional contexts. The theory has been widely applied to studies of organisational governance, policy adoption, and compliance, making it particularly relevant for understanding cybersecurity governance and data protection compliance in public institutions.

The central assumption of Institutional Theory is that organisations operate under pressures to conform to institutional norms and expectations. These pressures can be coercive, arising from legal mandates and regulations; normative, coming from professional standards and societal expectations; or mimetic, stemming from the tendency of organisations to emulate peers perceived as successful or legitimate. Meyer and Rowan (1977) argue that formal structures, policies, and procedures are often adopted not solely for operational efficiency but to gain legitimacy in the eyes of regulators, stakeholders, and the public. Organisations may adopt policies or practices that appear rational and compliant, even if the actual implementation is symbolic rather than functional. This emphasis on legitimacy rather than mere efficiency allows Institutional Theory to explain why organisations sometimes implement policies inconsistently, partially, or superficially.

The theory further assumes that organisations are influenced by both formal and informal rules. Formal rules include laws, regulations, and official guidelines, while informal rules include

cultural norms, social expectations, and industry conventions. Compliance, therefore, is not simply a matter of technical capability; it is also shaped by an organisation's perception of what is socially and politically acceptable. Institutions, according to DiMaggio and Powell (1983), are more likely to adopt structures and practices that are broadly recognised and endorsed within their institutional field, even when alternative approaches might be more efficient. This insight is critical for understanding public sector organisations, which operate under significant scrutiny and must balance operational needs with political and societal expectations.

Despite its strengths, Institutional Theory is not without criticism. Some scholars argue that it places too much emphasis on conformity, potentially underestimating the capacity of organisations to innovate or challenge institutional norms. Organisations may comply with rules and structures superficially, adopting the appearance of compliance without achieving substantive outcomes. Additionally, critics note that the theory can be vague in operationalisation, making it difficult to measure the strength or impact of institutional pressures objectively. In fast-changing contexts, such as cybersecurity, where technological threats evolve rapidly, relying on conformity and legitimacy may be insufficient for achieving true operational security and resilience. Nonetheless, these criticisms do not diminish the theory's explanatory power in contexts where legitimacy and regulatory compliance are central organisational concerns.

The relevance of Institutional Theory to this study on cybersecurity governance and data protection compliance in Benue State's sub-national public institutions is particularly strong. Public institutions are expected to adhere to national regulations such as the Nigeria Data Protection Regulation (NDPR), implement cybersecurity policies, and maintain systems that protect sensitive citizen data. Institutional Theory helps explain why these organisations adopt formal cybersecurity governance structures and data protection policies. Coercive pressures from legal mandates, normative pressures from professional standards, and mimetic pressures from other states or institutions drive public agencies to demonstrate compliance. However, variations in institutional capacity, technical infrastructure, and staff expertise may affect the extent to which policies are implemented effectively. By applying Institutional Theory, researchers can examine how these pressures influence the behaviour of Benue State's ministries, local government agencies, and parastatals, providing insight into both compliance levels and governance challenges.

1.4 Methodology

This study adopts a descriptive survey research design to examine cybersecurity governance and data protection compliance in Benue State's public institutions. The descriptive survey approach is appropriate because it allows for the systematic documentation of existing policies, organisational structures, staff capacity, and institutional practices, as well as the assessment of adherence to the Nigeria Data Protection Regulation (NDPR) and other data protection standards. By focusing on the descriptive aspects, the study provides a comprehensive understanding of the current state of cybersecurity governance while highlighting patterns, trends, and gaps in compliance across the selected ministries.

The study population consists of employees of four key government agencies in Benue State, selected based on their involvement in information management, institutional record-keeping, and technology-supported administrative processes. These agencies are the Benue Digital Infrastructure Company Limited (BDIC), which has a staff strength of 180 employees; the Benue Investment and Tourism Agency (BITA), employing 150 staff; the Benue State Digital Infrastructure Services Management and Enforcement Agency (BENDISMEA), with 120 employees; and the Benue Geographic Information Service (BENGIS), which has a staff strength of 260 employees. Employees of these agencies constitute the study population because their work involves routine handling of official records, institutional data, and technology-supported administrative processes that require accountability, data protection, and transparency. The combined population of staff across the four selected agencies is 710 employees, making them suitable for examining issues related to cloud-based document management, cybersecurity governance, and transparency in Benue State public institutions.

Table 1: Selected Benue State MDAs and Staff Strength

S/N	Agency	Staff Strength
1	Benue Digital Infrastructure Company Limited (BDIC)	180
2	Benue Investment and Tourism Agency (BITA)	150
3	Benue State Digital Infrastructure Services Management and Enforcement Agency (BENDISMEA)	120
4	Benue Geographic Information Service (BENGIS)	260
	Total	**710**

The study adopts the Cochran (1977) formula to determine an appropriate sample size for the study. The formula is stated as:

$$\boldsymbol{n_o} = \frac{z^2 pq}{e^2}$$

n_o = Sample size
Z= Z-score (1.96)
P= Precision (0.5)
q= 1-Precision (0.5)

$$\boldsymbol{n_o} = \frac{(1.96)^2(.5)\ (.5)}{(0.5)^2} = 385$$

Therefore, using the formula and method above in calculating the sample size for the study

$$\boldsymbol{n_o} = \frac{\frac{n_o}{1 + (n_o - 1)}}{N}$$

Where

n= Sample Size

$\boldsymbol{n_o}$ = Level of Significance (385)

1 = Constant

N = Population

$$\boldsymbol{n_o} = \frac{\frac{385}{1 + (385 - 1)}}{710}$$

385÷ (1+ (384÷710)

=250

A **multi-stage sampling technique** was adopted to ensure representativeness. In the first stage, **purposive sampling** was used to select the four MDAs, as they are directly involved in managing digital records and implementing ICT initiatives relevant to cybersecurity governance. In the second stage, **stratified sampling** was applied to categorise employees within each MDAs into senior, middle, and junior cadres, ensuring that staff from different levels of responsibility were proportionately represented. In the final stage, **simple random sampling** was used to select 250 individual respondents from each stratum, ensuring that every eligible employee had an equal chance of being included in the study. This approach minimised selection bias and enhanced the reliability and generalizability of the findings.

Data collection relied primarily on structured questionnaires administered to the selected respondents. The questionnaire captured information on the presence and implementation of

cybersecurity policies, organisational structures, staff capacity, institutional practices, and the level of compliance with the NDPR and international data protection standards. Secondary data, including policy documents, government reports, and relevant literature, were also reviewed to provide context and support the analysis of primary data.

The collected data were analysed using **descriptive statistical techniques,** including frequencies, percentages, means, and standard deviations, to summarise respondents' demographic characteristics and responses to survey items. A mean score of 3.0 or above was interpreted as agreement or positive compliance with cybersecurity and data protection practices, while a mean below 3.0 indicated disagreement or non-compliance.

Ethical considerations were strictly observed throughout the study. Participation was voluntary, and respondents were informed of the purpose of the research before data collection. Confidentiality and anonymity were guaranteed, and the data collected were used solely for academic purposes. Informed consent was obtained from all participants, and the study adhered to standard ethical protocols in social science research. To test the hypotheses, linear regression analysis will be employed to examine the relationship between the variables

Model Specification

To empirically assess the relationship between cybersecurity governance factors and data protection compliance in Benue State's public institutions, the study adopts a linear regression framework that links the independent variables cybersecurity policies, organizational structures, staff capacity, and institutional practices to the dependent variable, data protection compliance. This approach allows for a quantitative examination of the strength, direction, and significance of each factor on compliance with the Nigeria Data Protection Regulation (NDPR) and international data protection standards. The model is specified as follows:

$$DPC = \beta 0 + \beta 1(CSP) + \beta 2(OS) + \beta 3(SC) + \beta 4(IP) + \varepsilon$$

Where:

DPC = Data Protection Compliance (measured in terms of adherence to NDPR requirements and alignment with global data protection standards)

CSP = Cybersecurity Policies (existence, clarity, and implementation of cybersecurity

frameworks within ministries and agencies)

OS = Organizational Structures (roles, responsibilities, reporting lines, and governance mechanisms supporting cybersecurity)

SC = Staff Capacity (level of technical skills, training, awareness, and competency of employees in cybersecurity and data protection)

IP = Institutional Practices (day-to-day procedures, monitoring mechanisms, and institutional culture that promote or hinder compliance)

β0 = Constant term representing baseline level of data protection compliance when independent variables are zero

β1 – β4 = Coefficients representing the effect of each independent variable on data protection compliance

ε = Error term capturing unobserved factors influencing compliance

Table 1: Socio-Demographic Characteristics of Respondents

Attributes	Frequency (N = 250)	Percentage (%)
Gender		
Male	152	60.8
Female	98	39.2
Age (years)		
18–25	107	42.8
26–40	116	46.4
41 and above	27	10.8
Marital Status		
Single	134	53.6
Married	112	44.8
Divorced	4	1.6
Educational Qualification		
SCE/NECO	40	16.0
NCE/Diploma	54	21.6
Degree	89	35.6
Postgraduate	67	26.8
Total	**250**	**100.0**

Source: Field Survey, 2025

The table above presents the socio-demographic characteristics of the 250 respondents across the selected ministries. Male respondents (60.8%) were slightly more represented than females

(39.2%), reflecting workforce composition in Benue State's public institutions, particularly in administrative and ICT-related roles. Most respondents were aged 26–40 years (46.4%), followed by those aged 18–25 years (42.8%), while a smaller proportion were aged 41 years and above (10.8%). This indicates that the study largely captured the perspectives of young and mid-career employees who are more likely to be familiar with digital systems and cybersecurity practices. Regarding marital status, single respondents constituted the majority (53.6%), married respondents accounted for 44.8%, and divorced respondents represented 1.6%, suggesting strong participation from younger and actively employed staff within the ministries.

Regarding educational qualifications, the majority of respondents held Degree (35.7%) or Postgraduate (26.8%) qualifications, highlighting that the study captured well-educated staff capable of understanding and implementing cybersecurity policies, organizational structures, and NDPR compliance. NCE/Diploma holders (21.4%) and SCE/NECO holders (16.1%) comprised the remaining respondents, ensuring that all participants had sufficient educational background to provide informed perspectives on digital governance and data protection practices.

Table 3: Staff Perception of Organisational Structures and Data Protection Compliance

S/N	Questions	SD	D	U	A	SA	Mean	Std. Dev	Decision
1	My ministry has clear cybersecurity policies guiding data protection practices	67	76	36	45	26	2.34	1.12	Rejected
2	Cybersecurity policies are effectively communicated to all staff	80	71	31	36	32	2.20	1.17	Rejected
3	Staff receive regular training on cybersecurity and data protection compliance	76	67	45	36	26	2.29	1.20	Rejected
4	Monitoring and enforcement mechanisms ensure compliance with cybersecurity policies	85	71	36	32	26	2.13	1.18	Rejected

Source: Field Survey, 2026

Table 3 presents staff perceptions regarding the impact of cybersecurity policies on data protection compliance in Benue State's public institutions based on 250 respondents. The response distributions across the five-point Likert scale for each item sum up to 250. The mean scores, ranging from 2.13 to 2.34, remain below the benchmark mean of 3.0, indicating that respondents generally perceive cybersecurity policies as ineffective in ensuring data protection compliance. The findings reveal that although cybersecurity policies may exist within ministries and agencies, they are inadequately communicated, poorly enforced, and not sufficiently supported by regular staff training. Weak monitoring and enforcement mechanisms further undermine compliance with the Nigeria Data Protection Regulation. These results suggest that the mere existence of cybersecurity policies does not automatically translate into effective data protection without strong implementation, enforcement, and continuous capacity-building measures.

Table 4: Staff Capacity and Adherence to NDPR

S/N	Questions	SD	D	U	A	SA	Mean	Std. Dev	Decision
1	I have the necessary skills to handle sensitive data in line with NDPR requirements	54	42	25	90	39	2.95	1.28	Rejected
2	I receive adequate training on data protection and cybersecurity in my ministry	63	50	23	72	42	2.83	1.30	Rejected
3	I am confident in applying NDPR principles in my daily work activities	50	38	30	85	47	3.05	1.27	Accepted
4	My ministry provides sufficient resources to enhance staff capacity for NDPR compliance	58	48	30	77	37	2.90	1.29	Rejected

Source: Field Survey, 2026

Table 4 presents the analysis of staff capacity and its influence on adherence to the NDPR in Benue State's public institutions based on 250 respondents. The response distributions for each item sum up to 250. The mean scores range from 2.83 to 3.05, indicating that respondents generally perceive staff capacity as insufficient to fully ensure compliance. Only the item on

confidence in applying NDPR principles (mean = 3.05) slightly exceeded the benchmark of 3.0, suggesting that while staff may understand NDPR requirements theoretically, practical application is constrained by limited training, skills, and resources. Most respondents indicated that training and resources to enhance staff capacity are inadequate, and many staff lack the necessary skills to consistently comply with NDPR regulations. This underscores staff capacity as a critical limiting factor in effective data protection, highlighting the need for continuous professional development, targeted training programs, and institutional support to improve adherence.

Table 3: Staff Perception of Institutional Practices and Compliance with International Data Protection Standards

S/N	Questions	SD	D	U	A	SA	Mean	Std. Dev	Decision
1	My ministry has clear institutional procedures aligned with international data protection standards	63	72	38	40	37	2.40	1.13	Rejected
2	Staff are regularly trained on international data protection protocols and best practices	75	66	38	45	26	2.32	1.17	Rejected
3	Institutional monitoring systems ensure compliance with international data protection standards	28	23	40	68	91	4.06	0.97	Accepted
4	Reporting and accountability mechanisms support adherence to global data protection frameworks	23	30	35	62	100	4.18	0.95	Accepted

Source: Field Survey, 2026

Table 3 presents staff perceptions of institutional practices and their relationship with compliance with international data protection standards in Benue State's public institutions. The mean scores for items 3 and 4 (4.06 and 4.18) exceed the benchmark mean of 3.0, showing strong agreement that institutional monitoring systems and reporting/accountability

mechanisms support compliance with international standards. Items 1 and 2, however, recorded mean scores below 3.0, indicating that clear procedures and regular staff training remain inadequate. Overall, while monitoring and accountability mechanisms promote compliance, weaknesses in procedural clarity and capacity-building limit full adherence to international data protection standards.

Hypothesis Testing

Table 9: Effect of Cybersecurity Policies on Data Protection Compliance (H_{01})

Predictor Variable	R	R^2	Df	F	β	t	Sig
Constant	.671	.450	1	8.912	–	27.125	.000
Cybersecurity Policies	–	–	–	–	.504	6.724	.000

Hypothesis 1: Cybersecurity policies have a significant positive impact on data protection compliance in Benue State's public institutions ($R = 0.671$, $R^2 = 0.450$, $t = 6.724$, $p < 0.01$). This shows that well-defined cybersecurity policies and their enforcement enhance compliance with data protection standards. Null hypothesis is rejected.

Table 10: Effect of Organisational Structures on Data Protection Compliance (H_{02})

Predictor Variable	R	R^2	Df	F	β	t	Sig
Constant	.652	.425	1	8.145	–	26.537	.000
Organisational Structures	–	–	–	–	.488	6.512	.000

Hypothesis 2: Organisational structures significantly affect data protection compliance in Benue State's ministries and agencies ($R = 0.652$, $R^2 = 0.425$, $t = 6.512$, $p < 0.01$). Clear roles, reporting lines, and accountability enhance compliance. Null hypothesis is rejected.

Table 11: Effect of Staff Capacity on NDPR Compliance (H_{03})

Predictor Variable	R	R^2	Df	F	β	t	Sig
Constant	.689	.474	1	9.354	–	28.682	.000
Staff Capacity	–	–	–	–	.517	6.933	.000

Hypothesis 3: Staff capacity has a significant positive influence on adherence to the NDPR in Benue State's public institutions ($R = 0.689$, $R^2 = 0.474$, $t = 6.933$, $p < 0.01$). Higher staff knowledge, training, and competency increase compliance levels. Null hypothesis is rejected.

Table 12: Effect of Institutional Practices on Compliance with International Data Protection Standards (H_{04})

Predictor Variable	R	R^2	Df	F	β	t	Sig
Constant	.704	.496	1	10.234	–	29.217	.000
Institutional Practices	–	–	–	–	.526	7.014	.000

Hypothesis 4: Institutional practices are significantly related to compliance with international data protection standards in Benue State's public institutions ($R = 0.704$, $R^2 = 0.496$, $t = 7.014$, $p < 0.01$). Well-designed procedures, monitoring, and accountability mechanisms positively influence adherence. Null hypothesis is rejected.

1.6 Findings

The findings indicate that cybersecurity policies in Benue State's public institutions are largely ineffective in ensuring data protection compliance. Although such policies may formally exist, their practical influence on daily operations appears minimal. Many staff members are unaware of policy contents due to weak communication strategies within ministries and agencies. The absence of consistent training further limits employees' ability to internalize cybersecurity responsibilities. Monitoring and enforcement mechanisms are perceived as weak, reducing the seriousness with which compliance is treated. This situation creates an environment where policy violations may go undetected or unpunished. The lack of operational clarity also undermines accountability among staff handling sensitive information. As a result, cybersecurity policies remain largely symbolic rather than functional. This disconnect between policy formulation and implementation weakens institutional compliance culture. Overall, cybersecurity policies have not translated into meaningful protection of personal and institutional data.

The findings reveal that organisational structures in Benue State's public institutions do not adequately support data protection compliance. Roles and responsibilities related to data

protection are poorly defined, leading to confusion and overlapping duties. Reporting systems for handling data breaches or compliance issues are weak or non-existent in many ministries. This structural weakness limits timely response to data protection challenges. The absence of dedicated units or officers responsible for compliance further compounds the problem. Organisational hierarchies do not sufficiently promote accountability in managing sensitive data. Decision-making processes related to data protection are often centralized and slow. These limitations reduce the effectiveness of internal control mechanisms. Consequently, compliance with data protection regulations is inconsistent across institutions. The findings suggest that organisational restructuring is necessary to strengthen accountability and compliance.

The results show that staff capacity remains a major constraint to effective adherence to data protection regulations. While some staff demonstrate confidence in applying data protection principles, this confidence is not consistently supported by adequate skills or resources. Training opportunities related to data protection and cybersecurity are limited and irregular. Many staff members lack practical exposure to compliance procedures in their daily tasks. Institutional support for professional development in data protection is insufficient. This gap restricts the translation of theoretical knowledge into effective practice. The availability of tools and resources needed for compliance is also inadequate. As a result, staff rely heavily on personal judgment rather than standardized procedures. This increases the risk of unintentional data breaches. Strengthening staff capacity is therefore essential for improving compliance outcomes.

The findings suggest that institutional practices play a significant role in compliance with international data protection standards. Monitoring systems within public institutions are perceived as effective in ensuring adherence to global standards. Reporting and accountability mechanisms also appear to function relatively well, promoting compliance behaviour. These practices encourage transparency and responsible data handling among staff. However, weaknesses remain in procedural clarity and staff training. Institutional procedures aligned with international standards are not sufficiently detailed or consistently applied. Training on global data protection best practices is inadequate for many employees. This creates uneven compliance across departments and agencies. Despite strong monitoring mechanisms, the lack of comprehensive training limits sustainability. Full alignment with international standards,

therefore, requires both strong oversight and enhanced capacity-building.

1.7 Conclusion

This study assessed cybersecurity governance and data protection compliance within the context of Benue State's digital transformation agenda. The findings reveal that while digital reforms are being pursued, cybersecurity governance frameworks remain weakly institutionalised. Cybersecurity policies exist but lack effective communication, enforcement, and operational clarity. Organisational structures were found to be inadequate in supporting data protection responsibilities across ministries and agencies. Staff capacity limitations further constrain effective compliance with data protection regulations. Although monitoring and accountability mechanisms show some effectiveness, they are not sufficiently supported by clear procedures and training. The digital transformation agenda has therefore advanced faster than the supporting governance systems. This imbalance exposes public institutions to data protection risks. Effective digital governance requires coordinated policy, structure, and capacity development. Strengthening cybersecurity governance is essential for sustainable and secure digital transformation in Benue State's public sector.

1.8 Recommendations

Based on the findings, the following recommendations are proffered

i. The Benue State Government, through the Ministry of Science, Technology and Innovation, should ensure cybersecurity policies are clearly documented and disseminated. Heads of ministries and agencies should enforce compliance through internal regulations and sanctions. The State ICT Agency should integrate cybersecurity requirements into daily digital operations. Periodic compliance audits should be conducted by designated regulatory units.

ii. The Office of the Head of Service should define clear data protection roles within the public service structure. Ministries and agencies should establish dedicated data protection officers or compliance units. Permanent Secretaries should ensure effective reporting and accountability mechanisms. These actions will strengthen institutional coordination and oversight.

iii. The Benue State Civil Service Commission should organise regular training on NDPR and cybersecurity for public servants. Ministries should allocate budgetary provisions for staff capacity development. The State ICT Agency should provide technical support and training materials. Supervisors should ensure staff apply data protection principles in daily operations.

iv. The Benue State Government should align institutional procedures with international data protection standards. Compliance units within ministries should strengthen monitoring and reporting mechanisms. Training institutions and ICT agencies should provide continuous education on global best practices. Oversight bodies should periodically review compliance to ensure sustainability.

References

Ahmad, A., Alsmadi, I., & Alrawashdeh, T. (2021). Cybersecurity governance: A systematic review of existing frameworks and practices. *Journal of Information Security and Applications, 58*, 102706. https://doi.org/10.1016/j.jisa.2021.102706

Akinbode, O. A., & Akinwale, A. A. (2020). Data protection regulation and challenges of implementation in Nigeria's public sector. *African Journal of Law and Human Rights, 4*(2), 45–62.

Bada, M., & Sasse, A. M. (2019). Cyber security awareness campaigns: Why do they fail to change behaviour? *Cyber Security: A Peer-Reviewed Journal*, *2*(1), 29–42.

DiMaggio, P. J., & Powell, W. W. (1983). The iron cage revisited: Institutional isomorphism and collective rationality in organizational fields. *American Sociological Review*, *48*(2), 147–160. https://doi.org/10.2307/2095101

International Organization for Standardization. (2013). *ISO/IEC 27001:2013 information technology Security techniques Information security management systems Requirements*. ISO.

International Telecommunication Union. (2022). *Global cybersecurity outlook 2022*. ITU Publications.

Meyer, J. W., & Rowan, B. (1977). Institutionalized organizations: Formal structure as myth and ceremony. *American Journal of Sociology, 83*(2), 340–363. https://doi.org/10.1086/226550

National Information Technology Development Agency. (2019). *Nigeria data protection regulation (NDPR)*. NITDA.

National Institute of Standards and Technology. (2018). *Framework for improving critical infrastructure cybersecurity* (Version 1.1). U.S. Department of Commerce.

Voigt, P., & Von dem Bussche, A. (2017). *The EU General Data Protection Regulation (GDPR): A practical guide*. Springer International Publishing. https://doi.org/10.1007/978-3-319-57959-7

Von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security. *Computers & Security*, *38*, 97–102. https://doi.org/10.1016/j.cose.2013.04.004

African Union. (2014). *African Union Convention on Cyber Security and Personal Data Protection (Malabo Convention)*. African Union Commission.