International Journal of Information Resource Management (IJIRM)
Volume 3, Number 4 (October, 2026)
E- ISSN: 1118-7786

DIGITAL RECORDS MANAGEMENT CAPABILITY AND INSTITUTIONAL POLICY COMPLIANCE IN NIGERIAN UNIVERSITIES: THE MODERATING ROLE OF CYBERSECURITY READINESS

Victoria Chukwu Nwali, PhD

Ebonyi State University, Abakaliki, Ebonyi State, Nigeria

Abstract

This study examined the effects of digital records management capability and cybersecurity readiness on institutional policy compliance in Nigerian federal universities, including the moderating effect of cybersecurity readiness. A quantitative cross-sectional survey was conducted among personnel involved in records management, information governance, and cybersecurity in six purposively selected federal universities, one from each geopolitical zone. From a population of 860 personnel, a sample of 273 was determined using the Taro Yamane formula and allocated proportionately across the universities. Data were collected with a structured questionnaire adapted from existing measurement scales. The instrument underwent face and content validation, and reported Cronbach's alpha coefficients exceeded .70. Data were analyzed with descriptive statistics and partial least squares structural equation modeling using SmartPLS 4. Digital records management capability had a positive, significant relationship with institutional policy compliance ($\beta = .648$, $t = 12.226$, $p < .001$). Cybersecurity readiness also had a positive, significant relationship with compliance ($\beta = .571$, $t = 9.361$, $p < .001$). The interaction between records management capability and cybersecurity readiness was significant and positive ($\beta = .214$, $t = 4.458$, $p < .001$); the model R^2 increased from .541 to .586 after the interaction was included. The study recommends strengthening records management systems, investing in cybersecurity governance and staff capacity, and aligning both functions within university policy implementation.

Keywords: digital records management capability; cybersecurity readiness; institutional policy compliance;

 © 2026. IJIRM. All rights reserved (https://www.ijirm.com.ng)

Introduction

Digital records management in a university involves creating, capturing, classifying, storing, retrieving, retaining, preserving, and disposing of official records in digital form. Such records include admissions files, examination results, transcripts, personnel records, financial transactions, procurement documents, research outputs, and records of institutional decisions. Their value depends not only on whether they can be accessed quickly, but also on whether they remain authentic, complete, secure, and usable when required. These conditions make records management a practical part of university administration and accountability.

Digital platforms have changed how Nigerian universities handle records and deliver services. Institutional repositories, student information systems, electronic document platforms, digital libraries, and enterprise systems can reduce manual handling and improve access, but their benefits depend on how the systems are governed and used. Research in Nigeria has considered the availability and accessibility of digital recordkeeping among university administrators (Atah & Akeke, 2024), as well as the relationship between records management practices and the effectiveness of university registries (Dada & Ogunwemimo, 2024). For institutions, the operational issue is whether digitization is matched by documented procedures, appropriate staff skills, reliable infrastructure, and clear responsibility for records throughout their lifecycle.

Digital records management capability refers in this study to the institutional capacity to manage records in line with documented procedures and relevant requirements. It includes the systems and infrastructure used, the competence of personnel, the quality of records controls, and the consistency with which policies are applied. Earlier assessments of Nigerian university libraries identified differences in their preparedness for electronic records, including gaps in infrastructure, planning, policy, and professional support (Asogwa et al., 2021; Muhammad et al., 2021). These findings suggest that the presence of digital tools alone is an incomplete indicator of capability; institutional arrangements also determine whether the tools support reliable records management.

Nwali, V.C. © 2026. IJIRM. All rights reserved (https://www.ijirm.com.ng)

Universities must also protect records against unauthorized access, loss, alteration, and disruption. Cybersecurity readiness is used here to mean the institution's preparedness to prevent, detect, respond to, and recover from cyber incidents through governance, security controls, skilled personnel, risk assessment, and response procedures. Nigeria's data protection and information governance requirements add to the importance of making these arrangements operational, not merely documenting them. Ogundipe (2024) discusses digital records management within Nigeria's regulatory framework, while the Nigeria Data Protection Act 2023 reinforces the need for accountable handling of personal data.

Digital records management capability and cybersecurity readiness may therefore contribute jointly to institutional policy compliance. Strong records processes can make evidence traceable and support audits, while cybersecurity controls help protect the integrity, availability, and confidentiality of that evidence. However, a university may have formal digital records systems without having sufficient security arrangements to ensure that those systems consistently support compliance. The present study tests the direct relationships of both capabilities with institutional policy compliance and examines whether cybersecurity readiness strengthens the relationship between digital records management capability and compliance.

Statement of the Problem

Universities need records that can be located, authenticated, retained, protected, and produced when required for administrative decisions, audits, accreditation, and legal or regulatory obligations. Records management principles set out in ISO 15489-1:2016 provide a basis for managing records systematically, but the practical value of such principles depends on how each institution implements them. Where responsibility is fragmented across departments or records are held in unconnected systems, the institution may struggle to demonstrate that its procedures have been followed.

In Nigerian universities, digital platforms have expanded access to administrative information, yet available studies report continuing challenges involving

Nwali, V.C. © 2026. IJIRM. All rights reserved (https://www.ijirm.com.ng)

electronic records policies, infrastructure, planning, preservation, and staff capacity (Asogwa et al., 2021; Ojo et al., 2019). Weaknesses in these areas can result in inconsistent records practices and make it harder to demonstrate institutional policy compliance. The move to networked and cloud-supported systems also means that records management procedures must be supported by controls for access, incident response, and data protection.

The specific problem addressed by this study is that digital records management capability may not produce the same level of compliance in every university. Cybersecurity readiness may explain part of this difference, because secure access, risk management, staff awareness, and incident response can influence whether records systems operate in line with policy. Although previous Nigerian studies have examined records management and cybersecurity-related practices separately, the present manuscript identifies limited empirical examination of cybersecurity readiness as a moderator of the relationship between digital records management capability and institutional policy compliance. This study therefore estimates the two direct relationships and tests the interaction between the two capabilities in selected federal universities.

Research Questions

- What effect does digital records management capability have on institutional policy compliance in the selected Nigerian federal universities?
- What effect does cybersecurity readiness have on institutional policy compliance in the selected Nigerian federal universities?
- Does cybersecurity readiness moderate the relationship between digital records management capability and institutional policy compliance in the selected Nigerian federal universities?

© 2026. IJIRM. All rights reserved (https://www.ijirm.com.ng)

Review of Related Literature

Digital Records Management Capability and Institutional Policy Compliance

Digital records management capability is the organizational capacity to maintain reliable digital records through appropriate systems, procedures, controls, and staff competence. Institutional policy compliance refers to the extent to which an institution follows the rules and procedures that govern its records, information security, privacy, retention, access, and accountability. The two concepts are connected because institutions need trustworthy records to demonstrate that required decisions and processes were carried out. Phiri and Tough (2018) discuss university records management in relation to governance, while a 2023 hermeneutic review also treats records practices as part of institutional information stewardship ("Records Management in Institutions of Higher Education in Africa," 2023).

Research on Nigerian university libraries has identified uneven preparedness for electronic records management. Asogwa et al. (2021) assessed infrastructure, planning, and policy arrangements for electronic records, while Muhammad et al. (2021) documented challenges in records management practices in Nigerian public universities. Research on electronic records management in African university libraries, based on experience from Nigeria, further points to gaps in implementation and institutional support (Asogwa, Ezeani, & Asogwa, 2021). Taken together, this work indicates that digitization and effective records governance are not interchangeable: records processes need policies, resources, and staff who can apply them consistently.

Policy implementation and preservation are also important components of capability. Ojo et al. (2019) examined policy guidelines for records management in Nigerian university libraries, and Abdulkadir (2020) focused on preservation of electronic records in selected federal universities. These subjects relate to the ability to retain records that remain accessible and usable for as long as institutional and legal requirements demand. Muhamad et al. (2023) considered records and information management policy in Nigerian public universities, while Dada and Ogunwemimo (2024) examined records management practices and registry effectiveness. This

Nwali, V.C. © 2026. IJIRM. All rights reserved (https://www.ijirm.com.ng)

literature supports treating digital records management as a combination of technical, procedural, and organizational capacities rather than as the acquisition of software alone.

The studies reviewed provide context for a relationship between records management capability and compliance, but much of the cited work focuses on preparedness, policy guidelines, practices, or preservation. The present study addresses a more specific question by estimating the relationship between digital records management capability and institutional policy compliance in the selected federal universities. It also tests whether cybersecurity readiness changes the strength of that relationship.

Cybersecurity Readiness and Institutional Policy Compliance

Cybersecurity readiness refers to the arrangements that allow an institution to protect its information systems and records, respond to incidents, and maintain operations when security problems arise. It includes technical safeguards, governance responsibilities, risk assessment, incident response, and staff awareness. ISO/IEC 27001:2022 sets out requirements for an information security management system (International Organization for Standardization, 2022), while Yusif and Hafeez-Baig (2023) discuss cybersecurity policy compliance in higher education. These perspectives indicate that cybersecurity readiness involves organizational practice as well as technology.

Studies in Nigerian tertiary education provide evidence that human and institutional factors matter to cybersecurity compliance. Chikwendu and Oli (2023) examined factors influencing employees' compliance with cybersecurity practices in public universities in Southeast Nigeria. Salisu et al. (2024) considered the role of cybersecurity policy in shaping safe online behavior among tertiary students, and Olugbile et al. (2025) proposed a framework for cybersecurity readiness in Nigerian universities. Njoku et al. (2023) also examined cybersecurity in institutional repositories. Although these studies address related but not identical outcomes, they

Nwali, V.C. © 2026. IJIRM. All rights reserved (https://www.ijirm.com.ng)

support examining security arrangements and user behavior as part of the context in which universities manage digital information.

Data protection compliance provides a related indicator of institutional governance, although it should not be treated as a direct measure of cybersecurity readiness. Shokunbi et al. (2026) reported a mean Nigeria Data Protection Act compliance index of 35.79% across their sample of Nigerian universities and described a gap between formal policy adoption and operational implementation. Their findings reinforce the distinction between having documented requirements and applying them in practice. For the present study, this distinction is relevant because cybersecurity readiness is expected to depend on implemented controls, assigned responsibilities, and staff practices.

The literature therefore provides a basis for expecting cybersecurity readiness to contribute positively to institutional policy compliance. However, evidence specific to the direct effect of cybersecurity readiness on institutional policy compliance in federal universities remains limited in the sources reviewed here. The second research question addresses that relationship in the selected institutions.

Cybersecurity Readiness as a Moderator

Cybersecurity readiness may also affect how effectively digital records management capability translates into institutional policy compliance. A university can possess systems for creating, classifying, retrieving, and retaining records, but their contribution to compliance may be weakened when user access is poorly controlled, records are vulnerable to alteration, or incidents cannot be handled promptly. Conversely, cybersecurity controls can help preserve the integrity and availability of records and support the consistent application of records policies. This is the rationale for treating cybersecurity readiness as a possible moderator rather than only as a separate predictor.

The reviewed studies discuss records management capability, information security, cybersecurity practices, and governance, but they do not establish the moderating relationship tested in this study. A positive interaction would mean that the

Nwali, V.C. © 2026. IJIRM. All rights reserved (https://www.ijirm.com.ng)

association between digital records management capability and institutional policy compliance becomes stronger as cybersecurity readiness increases. A non-significant interaction would indicate that the study did not find evidence of such a conditional relationship. The third research question tests this relationship empirically.

Methodology

The study used a quantitative approach and a cross-sectional survey design. The population comprised 860 personnel involved in digital records management, information governance, and cybersecurity in six purposively selected federal universities. One university was selected from each of Nigeria's six geopolitical zones to capture institutional settings across the country. The categories of personnel and the population counts used for sampling are presented in Table 1.

Table 1

Population of Respondents in the Selected Federal Universities

No.	Geopolitical Zone	Federal University	Librarians	Registry/ Records Staff	ICT Personnel	Quality Assurance/Compliance Officers	Total
1	North Central	Federal University of Technology, Minna	28	62	25	15	130
2	North East	Abubakar Tafawa Balewa University, Bauchi	24	56	22	13	115
3	North West	Ahmadu Bello University, Zaria	45	95	40	20	200
4	South East	University of Nigeria, Nsukka	35	70	30	15	150

© 2026. IJIRM. All rights reserved (https://www.ijirm.com.ng)

No.	Geopolitical Zone	Federal University	Librarians	Registry/ Records Staff	ICT Personnel	Quality Assurance/Compliance Officers	Total
5	South South	University of Uyo	25	55	25	15	120
6	South West	Obafemi Awolowo University, Ile-Ife	30	70	30	15	145
	Total		187	408	172	93	860

Sample Size and Sampling Technique

The sample size was calculated with the Taro Yamane formula for a finite population: $n = N / [1 + N(e^2)]$, where n is the sample size, N is the population, and e is the level of precision. Using N = 860 and e = .05 gives $n = 860 / [1 + 860(.05^2)]$ = approximately 273. The resulting sample of 273 was allocated proportionately across the six universities. Proportionate stratified sampling was used for allocation, followed by purposive selection of personnel whose duties involved records management, information governance, cybersecurity, or policy implementation.

Table 2

Proportionate Allocation of the Sample

No.	Selected Federal University	Population	Proportion (%)	Sample Size
1	Federal University of Technology, Minna	130	15.12	41
2	Abubakar Tafawa Balewa University, Bauchi	115	13.37	37
3	Ahmadu Bello University, Zaria	200	23.26	64
4	University of Nigeria, Nsukka	150	17.44	48

© 2026. IJIRM. All rights reserved (https://www.ijirm.com.ng)

No.	Selected Federal University	Population	Proportion (%)	Sample Size
5	University of Uyo	120	13.95	38
6	Obafemi Awolowo University, Ile-Ife	145	16.86	45
	Total	860	100.00	273

Instrument, Validity, and Reliability

Data were collected with a structured questionnaire adapted from measurement scales used in previous studies and modified to address the study variables. The instrument contained a demographic section and sections measuring digital records management capability, cybersecurity readiness, and institutional policy compliance. Responses were recorded on a five-point Likert scale from 1 (strongly disagree) to 5 (strongly agree). Experts in Library and Information Science, Information Systems, and Research Methodology assessed face and content validity. A pilot study was conducted among people with characteristics similar to those of the target respondents but outside the main study, and the reported Cronbach's alpha coefficients exceeded .70.

Data Analysis

Descriptive statistics were used to summarize respondent information and the study variables. Partial least squares structural equation modeling (PLS-SEM) was performed in SmartPLS 4. The measurement model was assessed for indicator reliability, internal consistency, convergent validity, and discriminant validity. The structural model was evaluated using path coefficients, R^2, effect size (f^2), predictive relevance (Q^2), and bootstrapping with 5,000 resamples. The moderation analysis tested the interaction between digital records management capability and cybersecurity readiness. Because the study used a cross-sectional survey, the estimated effects are interpreted as model-based statistical relationships rather than proof of causation.

Nwali, V.C. © 2026. IJIRM. All rights reserved (https://www.ijirm.com.ng)

Results and Discussion

Research Question 1: What effect does digital records management capability have on institutional policy compliance in the selected Nigerian federal universities?

Table 3

Results for Digital Records Management Capability and Institutional Policy Compliance

Statistic	Estimate	Interpretation
Path coefficient (β)	.648	Positive relationship
Standard error	.053	
t value	12.226	
p value	< .001	Statistically significant
R^2 / Adjusted R^2	.420 / .418	42.0% of variance explained
f^2	.724	Effect-size estimate
Q^2	.301	Positive predictive relevance

Digital records management capability was positively associated with institutional policy compliance (β = .648, t = 12.226, p < .001). The model explained 42.0% of the variance (R^2 = .420; adjusted R^2 = .418); f^2 was .724 and Q^2 was .301. H01 is rejected. The result aligns with literature emphasizing documented procedures, reliable records, and staff capacity.

Research Question 2: What effect does cybersecurity readiness have on institutional policy compliance in the selected Nigerian federal universities?

Table 4

Results for Cybersecurity Readiness and Institutional Policy Compliance

Statistic	Estimate	Interpretation
Path coefficient (β)	.571	Positive relationship

Nwali, V.C. © 2026. IJIRM. All rights reserved (https://www.ijirm.com.ng)

Statistic	Estimate	Interpretation
Standard error	.061	
t value	9.361	
p value	< .001	Statistically significant
R^2 / Adjusted R^2	.326 / .323	32.6% of variance explained
f^2	.484	Effect-size estimate
Q^2	.248	Positive predictive relevance

Cybersecurity readiness was positively and significantly related to institutional policy compliance (β = .571, t = 9.361, p < .001). The model explained 32.6% of the variance in compliance (R^2 = .326; adjusted R^2 = .323), while the reported f^2 and Q^2 values were .484 and .248, respectively. H02 is therefore rejected. The result is consistent with the view that information security governance, risk management, access controls, incident response, and staff awareness are relevant to implementing institutional policies. It also reinforces the distinction between having security policies and ensuring that appropriate procedures operate in practice.

Research Question 3: Does cybersecurity readiness moderate the relationship between digital records management capability and institutional policy compliance in the selected Nigerian federal universities?

Table 5

Moderating Effect of Cybersecurity Readiness

Statistic	Estimate	Interpretation
Interaction path coefficient (β)	.214	Positive interaction
Standard error	.048	
t value	4.458	

© 2026. IJIRM. All rights reserved (https://www.ijirm.com.ng)

Statistic	Estimate	Interpretation
p value	< .001	Statistically significant
Main-effects model R^2	.541	Before interaction
Moderation model R^2	.586	After interaction
Change in R^2 (ΔR^2)	.045	4.5 percentage-point increase
f^2	.109	Interaction effect size
Q^2	.387	Positive predictive relevance

The interaction between digital records management capability and cybersecurity readiness was positive and statistically significant ($\beta = .214$, $t = 4.458$, $p < .001$). The R^2 increased from .541 in the main-effects model to .586 in the moderation model, a change of .045. The reported interaction effect size was .109, and Q^2 was .387. These results support rejection of H03 and indicate that the relationship between records management capability and compliance became stronger as cybersecurity readiness increased. The finding supports coordinated investment in records management and cybersecurity rather than treating them as unrelated administrative functions.

Conclusion

This study examined the relationships between digital records management capability, cybersecurity readiness, and institutional policy compliance in six selected Nigerian federal universities. The results showed positive and statistically significant relationships between compliance and both digital records management capability and cybersecurity readiness. The significant positive interaction further indicated that the relationship between records management capability and compliance was stronger at higher levels of cybersecurity readiness. Within the limits of the selected institutions and cross-sectional design, the findings support a coordinated approach to records governance: effective systems and procedures should be accompanied by practical security controls, capable staff, and monitoring of policy implementation.

Nwali, V.C. © 2026. IJIRM. All rights reserved (https://www.ijirm.com.ng)

References

Abdulkadir, A. I. (2020). Preservation of electronic records in selected federal universities in Nigeria. *MiddleBelt Journal of Library and Information Science*, *17*.

Asogwa, B. E., Ali, A., Onoh, C., Asogwa, M., Ngwuchukwu, M., Igbokwe, J., & Ezeani, C. (2021). Preparedness of Nigerian university libraries for the acquisition and management of digital records. *Libri*, *71*(4), 335–348.

Asogwa, B. E., Ezeani, C. N., & Asogwa, M. N. (2021). Status of electronic records management (e-RM) in African university libraries: Experience from Nigerian universities. *Library Management*, *42*(8/9), 515–530.

Atah, C. A., & Akeke, N. G. (2024). Availability and accessibility of digital record keeping among university administrators in Nigeria. *Journal of International Cooperation and Development*, *7*(1), 42–56.

Chikwendu, S. C., & Oli, N. P. (2023). Human factors influencing compliance to cyber security practices by employees of public universities in Southeast Nigeria. *International Journal of Information Security, Privacy and Digital Forensics*, *7*(1).

Dada, R. O., & Ogunwemimo, T. (2024). Records management practices and organizational effectiveness of universities registries in South-West, Nigeria. *International Journal of Research and Innovation in Social Science*.

International Organization for Standardization. (2016). *ISO 15489-1:2016 Information and documentation—Records management—Part 1: Concepts and principles.* ISO.

International Organization for Standardization. (2022). *ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection—Information security management systems—Requirements.* ISO.

Muhamad, J. S., Mannan, E. F., & Liman, Y. A. (2023). Assessing the impact of records and information management policy in Nigerian public universities: A qualitative review. *SCIREA Journal of Information Science and Systems Science*, *7*(2), 10–23.

Muhammad, J. S., Mannan, E. F., & Farashi, B. I. (2021). Records management practices in Nigerian public universities: The challenges. *Library Philosophy and Practice*, *2021*, 1–16.

Njoku, I. S., Chukwu, S. A. J., Njoku, B. C., & Ravichandran, R. (2023). Fostering cybersecurity in institutional repositories: A case of Nigerian universities. *African Journal of Library, Archives and Information Science*, *33*(1), 1–21.

Ogundipe, O. A. (2024). Managing digital records within Nigeria's regulatory framework. *International Journal of Science and Research Archive*, *12*(2), 2861–2868.

Ojo, J. O., Mairiga, H. M., Idakwo, I. S., & Song, U. M. (2019). Policy guidelines for records management in Nigerian university libraries. *Covenant Journal of Library and Information Science*, *2*(2).

Olugbile, O. H., Ojeniyi, J. A., & Anyachebelu, T. K. (2025). Towards a standard framework for cybersecurity readiness for Nigerian universities. *International*

© 2026. IJIRM. All rights reserved (https://www.ijirm.com.ng)

Journal of Applied Mathematics, Sciences, and Technology for National Defense, *3*(3).

Phiri, M. J., & Tough, A. G. (2018). Managing university records in the world of governance. *Records Management Journal*, *28*(1), 47–61.

Records management in institutions of higher education in Africa: A hermeneutic literature review. (2023). *Global Knowledge, Memory and Communication*, *74*(5/6), 1400–1413.

Salisu, A., Adamu, A. Y., & Yusuf, B. T. (2024). Cybersecurity policy effectiveness in shaping safe online behavior: A focus on Nigerian tertiary students in the Northeast. *Journal of Scientific Development Research*, *6*(9).

Shokunbi, O., Agbaje, M., & Ogu, E. C. (2026). Measuring Nigeria Data Protection Act (NDPA) 2023 compliance in Nigerian universities: A general compliance index and evidence of institutional decoupling. *FUDMA Journal of Sciences*, *10*(6), 291–296. https://doi.org/10.33003/fjs-2026-1006-5085

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

© 2026. IJIRM. All rights reserved (https://www.ijirm.com.ng)