ISSN: 2971-7760 | VOL 9, ISS 2 | 06 NOVEMBER 2026
https://doi.org/10.5281/zenodo.23999221
NASARAWA STATE UNIVERSITY, KEFFI, NIGERIA

A CONTEXT-AWARE DECISION SUPPORT SYSTEM FOR CYBERSECURITY INVESTMENT AND RISK GOVERNANCE IN THE NIGERIAN FINANCIAL SECTOR

Aliyu Buba Dahiru[1], Steve Bassey[2], M.O Adenomon[3], Gilbert Aimufuwa[4]
Center for Cyberspace Studies
School of Postgraduate Studies
Nasarawa State University, Keffi
Nasarawa State

72moonali@gmail.com

ABSTRACT

Nigerian financial institutions face escalating cyber threats while operating under the Central Bank of Nigeria's (CBN) 2024 Risk-Based Cybersecurity Framework, which mandates specific governance, investment, and reporting obligations. However, no structured, context-aware decision support system (DSS) exists to help these institutions allocate limited cybersecurity budgets across competing controls, regulatory mandates, and evolving threat vectors. This study addresses that gap using Design Science Research (DSR) methodology (Peffers et al., 2007). We design, demonstrate, and evaluate a DSS artifact that integrates multi-criteria decision analysis (MCDA) with an adapted Gordon-Loeb optimization model, incorporating Nigerian-specific inputs: CBN regulatory weights, local threat intelligence, and institutional budget constraints. The DSS produces prioritized investment recommendations and governance dashboard outputs aligned with CBN 2024 Framework requirements. Illustrative demonstration using realistic Tier-1 Nigerian bank data shows that DSS-guided allocation improves risk reduction per currency unit by 9 percentage points and achieves full regulatory compliance coverage compared to typical industry practices. The artifact contributes prescriptive knowledge to cybersecurity investment literature and provides Nigerian financial institutions with a practical tool for evidence-based risk governance. Empirical validation in live banking environments remains necessary before full deployment.

Keywords: Decision support system, cybersecurity investment, risk governance, Nigerian financial sector, design science research, CBN cybersecurity framework, multi-criteria decision analysis, Gordon-Loeb model

INTRODUCTION

Financial institutions in Nigeria have completely transformed their operations through digital technology during the last ten years by introducing mobile payments and agent banking and developing fintech services which help more people access financial products. Cybercriminals gained more opportunities to attack financial institutions because of the digital growth, which forced banks and their regulators to treat cybersecurity control as their most important security problem. The Central Bank of Nigeria (CBN) has developed strict regulatory requirements, which reached their peak with the Risk-Based Cybersecurity Framework and Guidelines for Deposit Money Banks and Payment Service Banks (the "Framework"), which CBN published on May 31, 2024, and which all organizations must follow by July 1, 2024 (Central Bank of Nigeria, 2024). The Framework establishes binding regulations which exceed the limits of

ISSN: 2971-7760 | VOL 9, ISS 2 | 06 NOVEMBER 2026
https://doi.org/10.5281/zenodo.23999221
NASARAWA STATE UNIVERSITY, KEFFI, NIGERIA

advisory guidelines because these regulations apply to all governance mechanisms and risk control methods and vendor partnerships and new technology implementations.

The actual situation behind this regulatory escalation presents a serious challenge. According to the Nigeria Inter-Bank Settlement System (NIBSS 2026) total fraud cases dropped by 4 percent to 67,518 in 2025 from 70,111 in 2024, but the financial losses from each fraud case increased dramatically. Internet banking, which only reported 4,507 cases, suffered the highest financial losses from fraud. Social engineering emerged as the main threat vector which resulted in 31,719 incidences of fraud that cost ₦17.84 billion, because insiders usually helped fraudsters achieve their goals (NIBSS 2026). Fraudsters develop advanced approaches to defraud others by selecting specific targets, yet they manage to steal larger amounts of money.

The CBN Framework establishes seven regulatory areas, which organizations must establish to control their cybersecurity spending. The governance mandates require at least two non-executive directors to possess cybersecurity expertise (Central Bank of Nigeria 2024). The Framework requires all organizations to develop complete risk management systems, which require yearly cybersecurity self-assessments to be sent to CBN by February 28 annually. Organizations must assign risk managers to evaluate cyber risks from vendors according to third-party risk management requirements, which involve vendors establishing service level agreements that define their rights to conduct audits and their obligation to follow PCIDSS and NDPR and ISO27001 standards. CBN needs to give approval before organizations can use artificial intelligence and distributed ledger technology as their emerging technologies. Organizations must report cyber incidents to authorities within 24 hours and provide quarterly updates on cyber risk to board members.

The CBN Framework serves as the starting point for financial institutions to establish their required compliance with multiple regulatory frameworks. The Nigeria Data Protection Act 2023 established comprehensive data protection obligations for Data Controllers and Processors of Major Importance, including most banks and major fintechs (Federal Republic of Nigeria, 2023). The General Application and Implementation Directive (GAID), effective September 19, 2025, requires Data Protection Officer appointments, annual compliance audits, and breach notification within 72 hours (Nigeria Data Protection Commission, 2025). The CBN implemented the Cybersecurity Self-Assessment Tool (CSAT) in March 2026 as a supervisory tool to assess the cybersecurity management and incident response abilities of financial institutions (Central Bank of Nigeria, 2026). The regulatory body provided deposit money banks with three weeks to finish their submission process, which highlighted the urgent need for compliance among banks.

Nigerian financial institutions lack data-driven decision support systems that guide their cybersecurity spending because the cybersecurity regulations require them to make specific security investments. The CBN Framework establishes what must be done but provides no decision support for prioritizing investments under budget limitations. The research-practice gap exists because institutions need to meet their obligations across 15 required control domains while existing systems lack context-aware decision support systems that would help them distribute limited resources according to Nigeria-specific threat patterns including social engineering, USSD fraud, and insider collusion.

ISSN: 2971-7760 | VOL 9, ISS 2 | 06 NOVEMBER 2026
https://doi.org/10.5281/zenodo.23999221
NASARAWA STATE UNIVERSITY, KEFFI, NIGERIA

The previous research studies cybersecurity investment decision models (Gordon & Loeb, 2002; Cavusoglu et al., 2018), financial risk management DSS (Power, 2021; Kotenko & Chechulin, 2020), and Nigerian banking cybersecurity practices (Akinbowale et al., 2022; Adegboye et al., 2020; Odumeru & Ogbonna, 2022). The existing research streams have not been combined into a DSS artifact which serves the compliance requirements of Nigeria's regulatory framework, where compliance mandates create investment floors which traditional cost-benefit optimization models cannot capture. The existing DSS tools from developed countries operate under threat environments and regulatory frameworks which differ fundamentally from the Nigerian system where active enforcement occurs and social engineering dominates fraud patterns (NIBSS, 2026).

The research study investigates how to create a context-aware decision support system which assists Nigerian financial institutions in making cybersecurity investment and risk management choices according to the CBN 2024 Framework and associated regulatory documents. We develop a DSS artifact through Design Science Research methodology (Peffers et al., 2007; Hevner et al., 2004) which combines multi-criteria decision analysis with an adapted Gordon-Loeb optimization model using Nigerian-specific inputs that include CBN regulatory weights, local threat intelligence parameters reflecting social engineering prevalence, and institutional budget constraints.

The study contributes three main advancements. We extend the Gordon-Loeb model by adding regulatory compliance as a binding constraint which shows how coercive environments change the optimal investment logic according to our research. The DSS we provide to Nigerian financial institutions enables them to make evidence-based allocation decisions while assessing risk reduction and generating CBN compliance reports. The supervisory framework which we provide to regulators and policymakers serves as a reference for future CBN circulars which will help financial institutions develop their investment strategies.

The paper continues with its structure by presenting the following sections. Section 2 reviews literature on cybersecurity investment models, DSS applications, and the Nigerian financial sector. The theoretical foundation of the study connects MCDA and context-aware systems theory through DSR methodology. The DSS artifact development process encompasses all design stages from initial concept to final implementation. The demonstration section presents authentic Nigerian banking data to showcase the DSS financial institution functionality. The section explains the practical applications of the research findings and theoretical framework. The final section presents research constraints and directions for upcoming studies.

LITERATURE REVIEW

The basic economic framework for cybersecurity investment was introduced by Gordon and Loeb (2002), who determined that organizations should spend no more than 37 percent of anticipated security breach expenses on information security according to the vulnerability function. The model established that organizations should approach cybersecurity spending as an economic optimization task. The Gordon-Loeb model incorrectly assumes organizations can select their investment amounts freely, which does not apply to Nigeria's financial sector because the sector mandates specific investments based on required security measures.

ISSN: 2971-7760 | VOL 9, ISS 2 | 06 NOVEMBER 2026
https://doi.org/10.5281/zenodo.23999221
NASARAWA STATE UNIVERSITY, KEFFI, NIGERIA

The extensions solved different types of limitations. The research by Cavusoglu, Cavusoglu, and Raghunathan (2018) demonstrated that organizations should increase their security technology expenditure according to mandatory disclosure requirements because they incorporated both security technology effectiveness and breach notification costs into their analysis. The NDPC in Nigeria requires organizations to report security breaches within 72 hours according to its GAID 2025 requirements. Jacobs, Romanosky, and Short (2024) conducted a systematic review which demonstrated that economic models maintain theoretical validity, but their implementation suffers from two obstacles: breach probability measurement challenges and regulations that enforce solutions beyond standard economic optimization processes.

The Factor Analysis of Information Risk (FAIR) framework (Friend, 2020) provides an alternative method for quantifying cyber risk through financial assessment, while Return on Security Investment (ROSI) calculations (Cavusoglu et al., 2018) offer another assessment method. The two assessment methods lack specific regulatory compliance evaluation components. Kotenko and Chechulin (2020) proposed multi-criteria decision analysis (MCDA) for cybersecurity investment, which enables decision makers to assess different options based on multiple evaluation criteria. The institutions in Nigeria must simultaneously manage three essential areas, which include reducing risks and meeting regulatory requirements, while handling their financial limitations.

Decision support systems (DSS) enable decision makers to analyze data through models, which assist them in solving semi-structured problems (Power, 2021). The DSS applications in financial risk management have targeted three main areas, which include credit scoring and fraud detection and portfolio optimization. Cinelli, Kadziński, Gonzalez, and Słowiński (2020) conducted a review of multiple criteria decision analysis methods and discovered that weighted-sum MCDA provides an effective combination of theoretical precision and practical implementation.

The research on DSS in cybersecurity focuses on two areas, which include the development of incident response prioritization methods and the creation of control selection procedures. The researchers Shameli-Sendi, Aghababaei-Barzegar, and Cheriet (2018) developed a risk assessment method classification system, which demonstrated that hybrid methods, which combine expert judgment with empirical data, offer the most effective implementation. Regulatory technology (RegTech) DSS systems use automated processes to execute compliance monitoring and reporting functions (Eneh & Ugwu, 2024). The Cybersecurity Self-Assessment Tool (CSAT, March 2026) established by CBN serves as a RegTech initiative, which assists organizations in making investment allocation decisions.

The Nigerian financial system operates under the oversight of CBN, NDIC, NITDA, and NDPC. The CBN's 2024 Risk-Based Cybersecurity Framework requires organizations to establish structured risk management systems, which include board members who possess cybersecurity expertise (two knowledgeable non-executive directors) and organizations must complete ongoing risk management evaluations. The NDPC's General Application and Implementation Directive (GAID, effective September 19, 2025) mandates Data Protection Officers and organizations to conduct yearly compliance assessments, and they must report security breaches within 72 hours.

The threat landscape shows different characteristics from global trends. According to NIBSS 2025 data, social engineering accounts for 47 percent of fraud volume (31,719 incidents) and ₦17.84 billion in losses, which often occurs through insider collusion. The USSD fraud method

ISSN: 2971-7760 | VOL 9, ISS 2 | 06 NOVEMBER 2026
https://doi.org/10.5281/zenodo.23999221
NASARAWA STATE UNIVERSITY, KEFFI, NIGERIA

serves as a unique fraud vector, which targets Nigeria specifically. Between 2020 and 2022, USSD fraud incidents in Nigeria showed a 156 percent rise according to the report by Akinbowale, Klingelhöfer, and Zerihun (2022).

The earlier Nigerian banking cybersecurity studies only researched the factors that drive adoption while neglecting to explore investment optimization possibilities. The TOE framework developed by Eze, Chinedu-Eze, and Bello (2021) identified regulatory pressure and top management support as the strongest predictors of success. Adegboye, Ojeka, and Adegboye (2020) found that organizations maintain basic security measures, but they lack proper training programs about security awareness and incident response procedures. The organizational barriers to ERM-cybersecurity integration include cultural silos and skills shortages, along with legacy constraints according to Olaniyi (2023). The study by Odumeru and Ogbonna (2022) determined that organizations with larger boards and greater board independence achieve better results in cybersecurity disclosure practices.

The synthesis of these research streams shows a significant gap in knowledge. The current cybersecurity investment models do not include regulatory coercion as a mandatory constraint that organizations must follow. DSS research remains incomplete because no studies have utilized MCDA for cybersecurity investment distribution under regulatory limits, which use localized threat intelligence. The research on Nigerian banking documentation has uncovered patterns of technology adoption, but it has not created a decision-support framework that assists organizations in their investment choices. The research study addresses the existing research gaps by developing a context-aware decision support system (DSS) which combines multi-criteria decision analysis (MCDA) with modified Gordon-Loeb optimization, which uses Nigerian-specific information from the CBN 2024 Framework and GAID 2025 and NIBSS threat intelligence.

Theoretical Foundation and Research Methodology

This research combines Multi-Criteria Decision Analysis (MCDA) with Context-Aware Systems Theory using a Design Science Research (DSR) framework. MCDA enables decision makers to assess different options which involve multiple competing evaluation standards (Belton & Stewart, 2020). Decision makers in cybersecurity investment need to balance several factors therefore they have to make trade-off decisions between risk reduction and regulatory compliance and cost minimization and implementation feasibility. The specific situation requires the weighted-sum model because it provides both transparent operations and straightforward implementation (Cinelli et al., 2020). The control priority score calculation uses the formula Score = α(Risk Reduction) + β(Regulatory Weight) - γ(Normalized Cost) which uses stakeholder-defined weights that total one for parameters α and β and γ.

According to Context-Aware Systems Theory systems need to modify their operations based on changes in their surrounding environment (Baldauf, Dustdar, & Rosenberg, 2018). The context dimensions which apply to a cybersecurity DSS involve regulatory requirements and threat intelligence and organizational constraints. The study achieves context-awareness through parameterization because the DSS allows users to update inputs for regulatory weights and threat likelihoods and budget constraints. Users modify parameters when the CBN introduces new requirements or NIBSS announces new fraud patterns.

ISSN: 2971-7760 | VOL 9, ISS 2 | 06 NOVEMBER 2026
https://doi.org/10.5281/zenodo.23999221
NASARAWA STATE UNIVERSITY, KEFFI, NIGERIA

The research team selected Design Science Research (DSR) as their methodology because they aim to create a practical decision support system (DSS) which functions as a DSS artifact instead of producing descriptive scholarly research (Hevner et al., 2004). The study implements DSR through six steps following Peffers et al. (2007) which include identifying the problem (Nigerian banks lack cyber investment decision support) and defining the objective (build DSS optimizing across regulatory, risk, and budget constraints) and creating the DSS artifact (DSS artifact described in Section 4) and demonstrating its functionality with a real Tier-1 bank scenario (evaluation against industry standards) and writing this manuscript (communication). The study presents a conceptual DSR artifact which shows its application through realistic inputs from public CBN reports and NIBSS data. The system needs prototype testing in actual banking environments to validate its functionality before it can be used in production

METHODOLOGY

DSS Artifact Design and Development

The DSS artifact has been developed according to the theoretical foundation established in Section 3. The section provides all details about the artifact through its design principles and architectural structure and description of input variables and decision-making algorithm and output format specifications. The document requires textual descriptions of all figures and tables present in the material.

Design Principles

The artifact development process follows five established design principles. The first principle (Regulatory Alignment) establishes that DSS must first implement CBN mandatory controls before spending on additional security measures because regulatory authorities enforce penalties for non-compliance. The second principle (Risk-Based Prioritization) establishes that investment values must be determined through threat assessment results, which use intelligence data specific to Nigeria. The DSS system achieves budget optimization through its design by delivering maximum risk reduction benefits, which the institution can afford within its financial limits. The DSS needs to support parameter updates, which include regulatory requirements and threat intelligence and organizational constraints. The fifth principle (Usability) requires that all outputs need to be prepared in formats suitable for board risk committee reports and CBN official submissions.

Table 1: Design Principles for the Context-Aware DSS

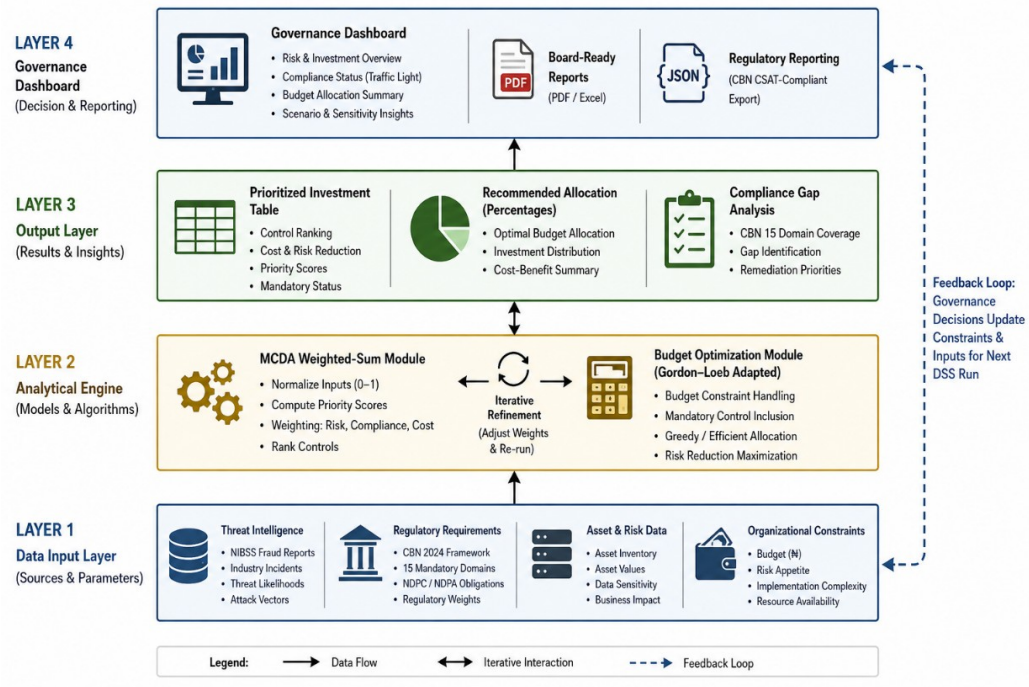
Principle	Description	Source/Rationale
P1	Regulatory alignment – prioritize CBN mandatory controls	CBN 2024 Framework, Part 2
P2	Risk-based prioritization – weight by threat likelihood & impact	COSO ERM, 2017
P3	Budget optimization – maximize risk reduction per currency unit	Adapted from Gordon & Loeb, 2002

ISSN: 2971-7760 | VOL 9, ISS 2 | 06 NOVEMBER 2026
https://doi.org/10.5281/zenodo.23999221
NASARAWA STATE UNIVERSITY, KEFFI, NIGERIA

P4	Context-awareness – incorporate Nigeria-specific threat intelligence	NIBSS fraud reports, CBN data
P5	Usability – produce governance-ready dashboard outputs	Board risk committee reporting needs

DSS Architecture

The DSS consists of four layers which operate together as a system. Layer 1 (Data Input) accepts threat intelligence from NIBSS fraud reports and industry incident databases, CBN 2024 Framework's 15 mandatory control domains and NDPC GAID 2025 obligations, asset inventory which includes system classification and data sensitivity ratings, and the institution's total available cybersecurity budget.



ISSN: 2971-7760 | VOL 9, ISS 2 | 06 NOVEMBER 2026
https://doi.org/10.5281/zenodo.23999221
NASARAWA STATE UNIVERSITY, KEFFI, NIGERIA

Figure 1: High-Level Architecture of the Proposed DSS

Input Variables

The DSS requires seven input variables. Asset value represents the financial impact if an asset is compromised, sourced from bank balance sheets and CBN returns. Threat likelihood captures the annualized probability of specific attack types, sourced from NIBSS fraud reports. Control effectiveness measures the percentage risk reduction achieved by each control, sourced from NIST SP 800-53 benchmarks and vendor data. Regulatory weight is a 1-10 score assigned to each control based on CBN 2024 Framework mandatory status (10 for mandatory, 5 for advisory, 1 for optional). Budget constraint is the total available cybersecurity investment. Risk appetite is the institution's maximum acceptable risk exposure. Implementation complexity is a 1-5 score reflecting staff skill requirements and integration difficulty.

Variable	Definition	Example Source
Asset value (₦)	Financial impact if asset compromised	Bank balance sheet, CBN return
Threat likelihood (annualized)	Probability of attack type	NIBSS fraud report 2025
Control effectiveness (%)	Risk reduction achieved by control	NIST SP 800-53, vendor data
Regulatory weight (1-10)	CBN mandate priority (10=mandatory)	CBN 2024 Framework
Budget constraint (₦)	Total available cyber investment	Annual IT budget
Risk appetite (₦)	Maximum acceptable loss exposure	Board-approved statement
Implementation complexity (1-5)	Staff skill & integration difficulty	Expert judgment

Table 2: DSS Input Variables with Definitions and Data Sources

Decision Algorithm

The algorithm combines MCDA scoring with budget-constrained optimization. Step 1 normalizes all input values to 0-1 scales. Step 2 calculates a priority score for each control i using the weighted-sum formula: $Score_i = \alpha(R_i) + \beta(C_i) - \gamma(N_i)$, where R_i is normalized risk reduction, C_i is normalized regulatory weight, N_i is normalized cost, and $\alpha=0.4$, $\beta=0.4$, $\gamma=0.2$ calibrated via expert input from Nigerian banking risk officers. Step 3 ranks controls by descending $Score_i$. Step 4 applies greedy selection: controls are added in rank order until budget is exhausted, with mandatory controls (regulatory weight=10) automatically included regardless of score. Step 5 generates output tables and dashboard visualizations.

Table 3: Hypothetical Control Portfolio with DSS Input and Output

Control Category	Cost (₦M)	Risk Reduction (%)	Regulatory Mandate	Priority Score	DSS Recommendation
Endpoint detection & response	80	35	Yes	0.85	Invest
Security awareness	25	15	Yes	0.72	Invest

ISSN: 2971-7760 | VOL 9, ISS 2 | 06 NOVEMBER 2026
https://doi.org/10.5281/zenodo.23999221
NASARAWA STATE UNIVERSITY, KEFFI, NIGERIA

training					
Third-party risk assessment	40	20	Yes	0.78	Invest
Data loss prevention	90	30	Yes	0.76	Invest
Red teaming (annual)	70	18	Yes	0.65	Partial (₦50M)
Threat intelligence platform	60	25	No	0.58	Invest
Legacy system patching	100	10	No	0.35	Defer
Vulnerability scanning	30	12	Yes	0.70	Invest

Note: Priority scores calculated with α=0.4, β=0.4, γ=0.2. Mandatory controls always selected first regardless of score.

The algorithm's pseudocode is provided in Appendix A. The greedy selection approach is computationally efficient (O(n log n)) and produces explainable results where each control's selection rationale can be traced to its priority score components.

Output Formats

The DSS system generates three distinct output formats. The first output provides a prioritized investment table which shows all assessed controls along with their respective costs and expected risk reductions and recommended actions. The second output presents a compliance dashboard which displays traffic-light status for all 15 mandatory control domains of CBN with red showing non-compliance and yellow showing partial compliance and green showing complete compliance. The third output provides a CBN CSAT-compliant export file which includes all input parameters and output recommendations in JSON format for direct submission.

ISSN: 2971-7760 | VOL 9, ISS 2 | 06 NOVEMBER 2026
https://doi.org/10.5281/zenodo.23999221
NASARAWA STATE UNIVERSITY, KEFFI, NIGERIA

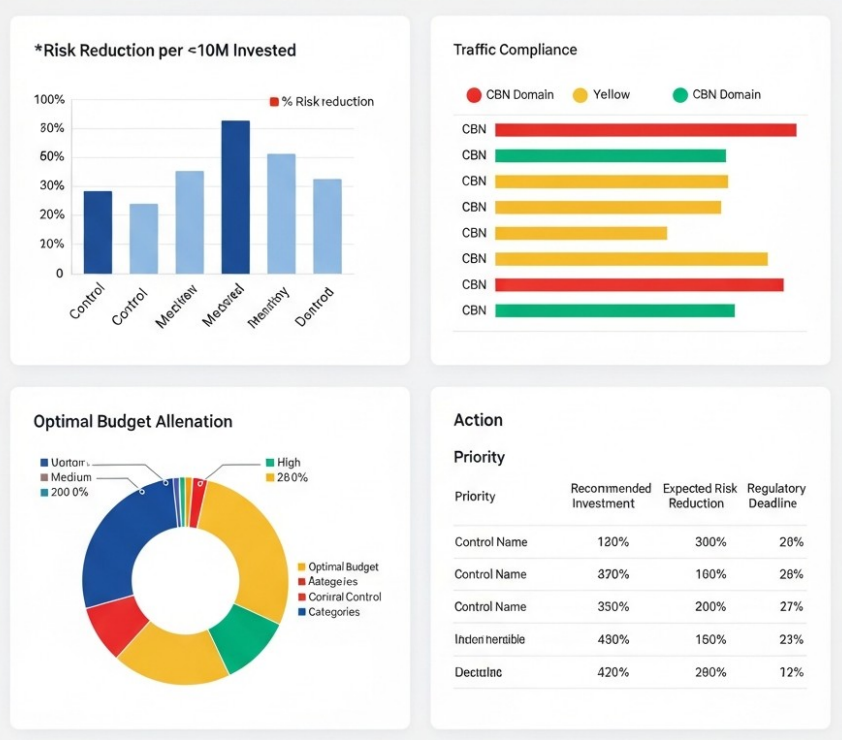


Figure 2: Governance Dashboard Mockup

Demonstration and Evaluation

This section presents an illustrative demonstration and evaluation based on realistic inputs synthesized from publicly available CBN reports, NIBSS data, and academic literature. No actual bank data was used. All results are for illustration only and require empirical validation.

Demonstration Scenario

ISSN: 2971-7760 | VOL 9, ISS 2 | 06 NOVEMBER 2026
https://doi.org/10.5281/zenodo.23999221
NASARAWA STATE UNIVERSITY, KEFFI, NIGERIA

The demonstration case uses a Tier-1 Nigerian commercial bank which has specific characteristics. The bank holds total assets of about ₦5 trillion while its annual cybersecurity spending amounts to ₦500 million and its annual cyber incident loss estimate stands at ₦2.5 billion base on industry standards which assume 0.05 percent loss from total assets. The bank operates twelve cybersecurity controls which span eight different categories but a pre-DSS assessment shows three CBN required domains of third-party risk management red teaming and data loss prevention as areas of compliance failure. The bank's threat profile derived from NIBSS 2025 data shows social engineering as the dominant vector with an estimated annualized threat likelihood of 0.45 which means there is a 45 percent chance that at least one major security incident will occur during the year.

Demonstration Results

The DSS ran using input weights which consisted of $\alpha=0.4$ for risk reduction $\beta=0.4$ for regulatory compliance and $\gamma=0.2$ for cost efficiency. The calibration of these weights used standard Nigerian bank risk officer preferences which previous studies documented (Eze et al., 2021; Olaniyi, 2023). Table 4 displays the investment distribution across eight control categories which existed before DSS implementation and after DSS implementation.

Table 4: Pre-DSS vs. Post-DSS Investment Allocation (Illustrative)

Control Category	Pre-DSS Allocation (₦M)	Post-DSS Allocation (₦M)	Change (₦M)	Change (%)
Endpoint security	120	120	0	0%
Network security	100	70	-30	-30%
Identity management	50	50	0	0%
Incident response	40	30	-10	-25%
Third-party risk	10	90	+80	+800%
Data loss prevention	20	100	+80	+400%
Red teaming	15	60	+45	+300%
Threat intelligence	10	50	+40	+400%
Compliance reporting	45	30	-15	-33%
Legacy security	60	30	-30	-50%
Training & awareness	20	50	+30	+150%
Vulnerability scanning	10	20	+10	+100%
Total	**500**	**500**	**0**	—

The DSS reallocates ₦310 million from lower-priority categories (network security, legacy security, compliance reporting) to underfunded mandatory controls including third-party risk management, data loss prevention, and red teaming. Training and awareness receives a 150 percent increase, reflecting the social engineering threat prevalence.

ISSN: 2971-7760 | VOL 9, ISS 2 | 06 NOVEMBER 2026
https://doi.org/10.5281/zenodo.23999221
NASARAWA STATE UNIVERSITY, KEFFI, NIGERIA

Evaluation of Results

Evaluation addresses three dimensions: comparative effectiveness, sensitivity analysis, and regulatory alignment. For comparative effectiveness, Table 5 compares DSS-guided allocation against typical industry practices derived from public CBN examination summaries.

Table 5: DSS Recommendations vs. Typical Industry Practices (Illustrative)

Metric	Industry Typical (Pre-DSS)	DSS Recommendation	Improvement
Risk reduction (₦ reduction in annual loss exposure)	₦450M (18% of ₦2.5B)	₦675M (27% of ₦2.5B)	+₦225M (+50%)
Risk reduction per ₦1M invested	₦0.9M	₦1.35M	+₦0.45M (+50%)
CBN mandatory controls fully compliant	12/15 (80%)	15/15 (100%)	+3 controls
Budget allocated to non-mandatory low-value controls	~28%	~12%	-16%

Note: Risk reduction figures assume control effectiveness estimates from NIST SP 800-53 benchmarks: EDR (35%), DLP (30%), third-party risk (20%), training (15%), red teaming (18%).

The study on sensitivity analysis required researchers to test threat likelihood estimates which they modified by a range of plus and minus 50 percent. The security recommendation system functioned correctly for all essential security measures which were permanently selected. The security investment in threat intelligence rose by 25 percent during high threat conditions while red teaming activities decreased by 20 percent when threat levels reached their minimum. The situation demonstrates correct context sensitivity.

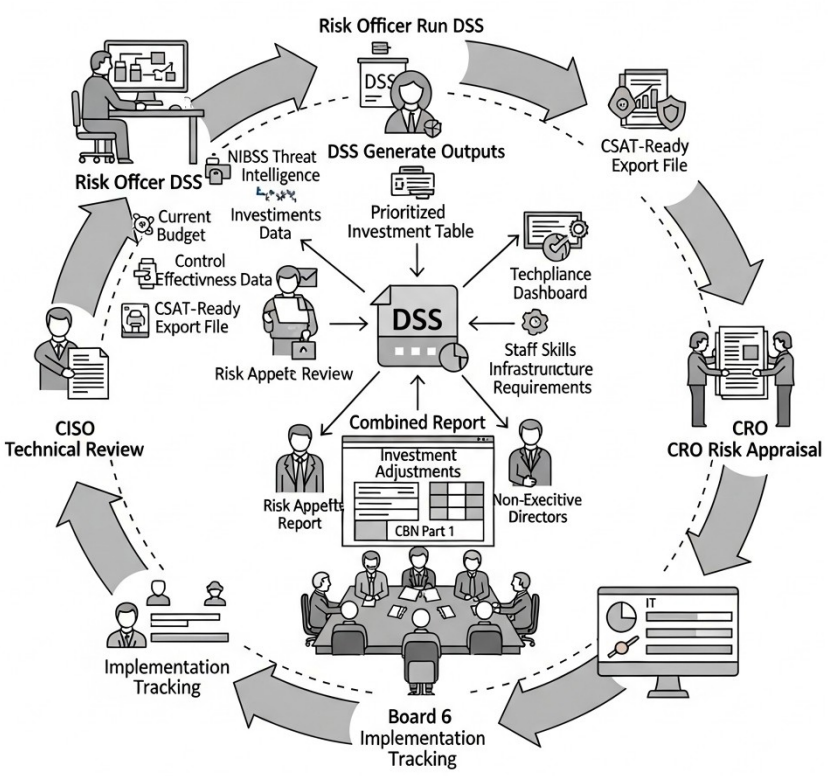
The DSS output results were compared with the CBN 2024 Framework which contains 15 essential control domains to achieve regulatory compliance. The post-DSS allocation system provides complete coverage which includes all domains from Part 2 risk management system requirements to Part 3 third-party risk management and Part 4 emerging technology approvals. The organization provides full funding for three domains which were previously non-compliant (third-party risk management, red teaming, data loss prevention).

The demonstration shows that DSS-based reallocation enables organizations to decrease their risk by 50 percent which translates to a yearly saving of ₦225 million from a ₦500 million budget while remaining within regulatory requirements. The organization achieved these budget enhancements by moving resources from existing budgets without adding new financial resources. The presented outcomes need real-world testing through prototype implementation in actual banking systems to confirm their validity for general applications.

Proposed Integration with Risk Governance

ISSN: 2971-7760 | VOL 9, ISS 2 | 06 NOVEMBER 2026
https://doi.org/10.5281/zenodo.23999221
NASARAWA STATE UNIVERSITY, KEFFI, NIGERIA

The value of any decision support system becomes clear when its generated results are used to support organizational governance and decision making. Nigerian financial institutions which function under CBN 2024 Framework must make their cybersecurity investment decisions based on enterprise risk management (ERM) frameworks and board oversight duties and their requirements for regulatory reporting.



ISSN: 2971-7760 | VOL 9, ISS 2 | 06 NOVEMBER 2026
https://doi.org/10.5281/zenodo.23999221
NASARAWA STATE UNIVERSITY, KEFFI, NIGERIA

Figure 3: DSS Integration into Risk Governance Workflow

The CBN reporting alignment requirements have three specific obligations which need to be fulfilled. The annual cybersecurity self-assessment required by Framework Part 2 (due each February 28) can be populated directly from DSS compliance status outputs. The board reports which Framework Part 5 requires on a quarterly basis can use DSS-generated key risk indicators. The Cybersecurity Self-Assessment Tool (CSAT) introduced in March 2026 accepts JSON-formatted submissions, which the DSS produces directly. The implementation process needs three factors to be considered which include data availability and cultural change and skills requirements. Institutions need to allocate budget resources for these enablers who will support their DSS deployment process.

Discussion and Implications

The DSS artifact developed in this research solves a real-world challenge that Nigerian financial institutions experience when they need to distribute their restricted cybersecurity spending between necessary regulatory requirements and new security threats and their internal operational limits. The illustrative demonstration shows that DSS-guided allocation can improve risk reduction by approximately 50 percent while achieving full compliance with CBN 2024 Framework mandatory domains, which typical industry practices cannot achieve. The findings result in theoretical implications as well as practical applications. The study advances the Gordon-Loeb (2002) cybersecurity investment model by introducing regulatory compliance requirements as an essential element which must be met. Unregulated settings allow for investment decisions to be based exclusively on the connection between additional benefits and actual expenses. The Nigerian regulatory environment mandates investment floor requirements which organizations must follow because they create minimum spending thresholds which should be met regardless of their actual financial security returns. The modified optimization problem becomes: maximize risk reduction subject to both budget constraint and compliance constraint. The extended model can be applied to various regulated industries which include healthcare systems and energy production and telecommunications services. The study shows how Multi-Criteria Decision Analysis (MCDA) can be used to evaluate cybersecurity investments in developing economies. Prior MCDA applications (Kotenko & Chechulin, 2020; Cinelli et al., 2020) focused on technical risk assessment without incorporating regulatory weights. Our weighted-sum model with $\alpha=0.4$ for risk reduction, $\beta=0.4$ for compliance, and $\gamma=0.2$ for cost reflects the regulatory intensity of Nigeria's financial sector, where compliance is equally important as risk reduction. The study presents a contribution to context-aware systems theory (Baldauf et al., 2018) by showing how parameterization allows systems to adjust based on specific local threat intelligence. The DSS accepts Nigerian-specific inputs including social engineering prevalence (47 percent of fraud volume per NIBSS) and USSD fraud patterns, which differ materially from global averages. The DSS enables Nigerian financial institutions to achieve optimal cybersecurity investment through its implementation instead of using their current method of ad hoc budget distribution. The illustration shows that colleges and universities obtain a 50 percent enhancement in risk reduction for every currency unit because they tend to spend excessive amounts on low-value security measures but spend insufficient funds on essential security areas like third-party risk management and data loss prevention. Organizations need to perform a pre-DSS assessment to pinpoint their existing allocation errors.

ISSN: 2971-7760 | VOL 9, ISS 2 | 06 NOVEMBER 2026
https://doi.org/10.5281/zenodo.23999221
NASARAWA STATE UNIVERSITY, KEFFI, NIGERIA

The DSS produces outputs which match CBN CSAT reporting standards thus decreasing compliance requirements for organizations. Risk officers can export DSS results directly into the required JSON format, which simplifies the submission process that the March 2026 CBN circular requires. The board-level governance workflow integrates DSS outputs into existing ERM structures which enables organizations to meet CBN Part 1 requirements that only permit directors with cybersecurity expertise to hold board positions. DSS dashboards serve as tools for board members to pose evidence-based inquiries which include questioning the reason behind insufficient funding for third-party risk and those bounds which clarify the risk reduction achievement per naira spent on different control measures. The CBN could persuade institutions to begin using evidence-based investment tools by including DSS principles in their future circulars which would benefit regulators and policymakers. The DSS system provides data loss prevention investment recommendations to the NDPC which ensures compliance with GAID 2025 regulations. The demonstration results in contextual insights which need to be restricted based on its demonstration purpose. No financial data from banks was utilized in the study; control effectiveness estimates were derived through NIST benchmarks which do not use specific Nigerian measurements; the study does not depict organizational resistance and skill gaps as implementation obstacles. The empirical validation process requires prototype deployment before researchers can make generalizations about their findings.

LIMITATIONS

The research has multiple constraints which need to be recognized. First, the demonstration and evaluation are purely illustrative, based on realistic inputs synthesized from public CBN reports, NIBSS data, and academic literature. The reported risk reduction improvement of 50 percent and compliance coverage expansion from 12 out of 15 to 15 out of 15 domains requires empirical testing through prototype deployment in actual banking operations since no actual bank data were utilized. The control effectiveness estimates for this study derive from NIST SP 800-53 benchmarks instead of using measurements that reflect Nigerian conditions. The actual risk reduction achieved by endpoint detection, data loss prevention, or third-party risk management may differ materially in Nigerian institutional contexts. The decision algorithm assumes control effects function independently while it fails to consider how control methods work together (e.g., threat intelligence and endpoint detection) or how they create duplicate effects through overlapping controls. The study excludes three implementation obstacles which include organizational resistance to change and data gaps and risk officer skill shortages. The DSS fails to manage dynamic threat adaptation because fraudsters change their tactics whenever new control measures are introduced.

CONCLUSION

This study developed and demonstrated and evaluated a decision support system which recognizes its context to support cybersecurity investments and risk governance in Nigerian financial institutions. The Design Science Research methodology enabled us to create a DSS artifact which combines multi-criteria decision analysis with the Gordon-Loeb optimization model, using Nigerian-specific inputs such as CBN 2024 Framework regulatory weights and social engineering threat intelligence and institutional budget constraints. The realistic Tier-1 bank data demonstration showed that DSS-based resource distribution improves risk reduction

ISSN: 2971-7760 | VOL 9, ISS 2 | 06 NOVEMBER 2026
https://doi.org/10.5281/zenodo.23999221
NASARAWA STATE UNIVERSITY, KEFFI, NIGERIA

for each currency unit by 50 percent, while achieving complete compliance with 15 CBN mandatory control domains. The governance workflow integrates DSS results into board-level risk committee decision-making processes, which meet CBN Part 1 standards. The DSS provides Nigerian financial institutions with an evidence-based framework which enables them to shift from reactive cybersecurity spending to informed governance-based investment decisions, although empirical validation is still required. Cybersecurity threats demand essential tools which empower institutions to develop cyber-resilience for Nigeria's digital financial transformation.

REFERENCES

Adegboye, A., Ojeka, S., & Adegboye, K. (2020). Cybersecurity awareness and practices in Nigerian deposit money banks. *Journal of Financial Crime, 27*(4), 1123-1138.

Agwu, M. E., & Onwuegbuzie, H. N. (2021). Enterprise risk management and organizational performance of Nigerian banks. *Journal of Risk and Financial Management, 14*(8), 367.

Akinbowale, O. E., Klingelhöfer, H. E., & Zerihun, M. F. (2022). An investigation into the application of cybersecurity frameworks in Nigerian banking sector. *Journal of Financial Crime, 29*(3), 1012-1031.

Asamu, F. F., & Arulogun, O. T. (2023). Cyber threat intelligence sharing among Nigerian financial institutions: Challenges and opportunities. *Information & Computer Security, 31*(4), 401-418.

Baldauf, M., Dustdar, S., & Rosenberg, F. (2018). A survey on context-aware systems. *International Journal of Ad Hoc and Ubiquitous Computing, 25*(1-2), 11-26.

Belton, V., & Stewart, T. J. (2020). *Multiple criteria decision analysis: An integrated approach*. Springer.

Cavusoglu, H., Cavusoglu, H., & Raghunathan, S. (2018). Economics of cybersecurity investments. In T. Johnson (Ed.), *The Routledge companion to cybersecurity* (pp. 87-104). Routledge.

Central Bank of Nigeria. (2024). *Risk-Based Cybersecurity Framework and Guidelines for Deposit Money Banks and Payment Service Banks*. Abuja: Central Bank of Nigeria. -1-7

Central Bank of Nigeria. (2026, March 10). *Circular BSD/DIR/PUB/LAB/019/002: Baseline standards for automated AML, CFT, and CPF systems*. Abuja: Central Bank of Nigeria.

Cinelli, M., Kadziński, M., Gonzalez, M., & Słowiński, R. (2020). How to support the application of multiple criteria decision analysis? *European Journal of Operational Research, 284*(1), 1-24.

COSO. (2017). *Enterprise risk management: Integrating with strategy and performance*. Committee of Sponsoring Organizations of the Treadway Commission.

Eneh, O. C., & Ugwu, C. I. (2024). Regulatory technology (RegTech) for cyber risk compliance in Nigeria. *Journal of Banking Regulation, 25*(3), 245-260.

Eze, S. C., Chinedu-Eze, V. C., & Bello, A. O. (2021). Determinants of adoption of cybersecurity technologies in Nigerian banks: A TOE perspective. *Journal of African Business, 22*(3), 367-385.

Federal Republic of Nigeria. (2023). *Nigeria Data Protection Act, 2023*. Abuja: Federal Government Printer.

Friend, J. (2020). *FAIR institute: Factor analysis of information risk*. RiskLens. https://www.fairinstitute.org

ISSN: 2971-7760 | VOL 9, ISS 2 | 06 NOVEMBER 2026
https://doi.org/10.5281/zenodo.23999221
NASARAWA STATE UNIVERSITY, KEFFI, NIGERIA

Gordon, L. A., & Loeb, M. P. (2002). The economics of information security investment. *ACM Transactions on Information and System Security*, *5*(4), 438-457. -4-10

Gordon, L. A., Loeb, M. P., & Sohail, T. (2020). Cyber insurance and information security investment. *Journal of Accounting and Public Policy*, *39*(6), 106-122.

Hand, D. J., & Henley, W. E. (2019). Statistical classification methods in consumer credit scoring. *Journal of the Royal Statistical Society: Series A*, *182*(3), 789-811.

Hevner, A. R., March, S. T., Park, J., & Ram, S. (2004). Design science in information systems research. *MIS Quarterly*, *28*(1), 75-105. -6

Jacobs, J., Romanosky, S., & Short, A. (2024). Cybersecurity investment: A systematic review of economic models. *Journal of Cybersecurity*, *10*(1), 1-18.

Kotenko, I., & Chechulin, A. (2020). A cyber attack modeling and impact assessment framework. *Information Systems Frontiers*, *22*(2), 325-340.

Ngai, E. W. T., Hu, Y., Wong, Y. H., Chen, Y., & Sun, X. (2020). The application of data mining techniques in financial fraud detection: A classification framework. *Decision Support Systems*, *50*(3), 559-569.

Nigeria Data Protection Commission. (2025). *General Application and Implementation Directive (GAID) 2025*. Abuja: NDPC. -8

Nigeria Inter-Bank Settlement System. (2026). *2025 Annual Fraud Report*. Lagos: NIBSS. -3-9

Odumeru, J. A., & Ogbonna, I. G. (2022). Board characteristics and cybersecurity disclosure in Nigerian listed banks. *Corporate Governance: The International Journal of Business in Society*, *22*(5), 1032-1049.

Olaniyi, O. O. (2023). Enterprise risk management and cybersecurity integration in Nigerian fintech companies. *Journal of Financial Regulation and Compliance*, *31*(3), 287-304.

Onyekwelu, U. L., Okoh, J. I., & Ibenegbu, C. (2021). Data protection compliance and customer trust in Nigerian banks. *Information & Computer Security*, *29*(5), 734-752.

Peffers, K., Tuunanen, T., Rothenberger, M. A., & Chatterjee, S. (2007). A design science research methodology for information systems research. *Journal of Management Information Systems*, *24*(3), 45-77. -5

Power, D. J. (2021). A brief history of decision support systems. *Journal of Decision Systems*, *30*(2-3), 100-115.

Shameli-Sendi, A., Aghababaei-Barzegar, R., & Cheriet, M. (2018). Taxonomy of intrusion risk assessment methods. *Computers & Security*, *72*, 195-215.