ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26nov107

Assessment of the Cybersecurity Posture of the Federal Inland Revenue Service Against AI-Assisted Threats Using NIST, MITRE and ACGF Frameworks

Nana Fatima Abdulaziz[1]; Marion Adebiyi[2]; Prema Kirubakaran[3]

[1;2;3]Department of Information Technology, Faculty of Computing Nile University of Nigeria Abuja, Nigeria

Publication Date: 2026/11/07

Abstract: Artificial intelligence is changing how attackers target national institutions, yet most cybersecurity assessments still check whether controls exist without asking whether governance can cope with AI-assisted threats. This study assesses the cybersecurity posture of the Federal Inland Revenue Service (FIRS) in Nigeria against AI-assisted threats using an integrated model that combines the NIST Cybersecurity Framework, the MITRE adversary knowledge base and the AI Cybersecurity Governance Framework (ACGF). A qualitative document-analysis design was used. FIRS policy documents were scored against the NIST framework with the CISA Cybersecurity Evaluation Tool, AI-assisted attack scenarios were tested against the documented policies with Python scripts, governance was rated across five ACGF pillars, and a staff questionnaire provided a reality check. The three scores were combined into a weighted Cybersecurity Posture Index (CPI). FIRS scored 3.6 on NIST, 2.5 on the MITRE simulation and 2.2 on ACGF governance, giving a CPI of 2.85 out of 5, which indicates developing resilience with critical gaps. Foundations in asset management, protection and incident response are strong, but policies do not cover data poisoning, adversarial machine learning, AI-generated phishing or oversight of AI models, and staff reported low awareness and untested response plans. The paper recommends an AI governance committee, AI-specific risk categories, an AI security policy annex, upgraded awareness training and behaviour-based detection.

Keywords: *Cybersecurity Posture; Artificial Intelligence; NIST CSF; MITRE ATT&CK; AI Cybersecurity Governance Framework; Public Sector; Federal Inland Revenue Service*.

How to Cite: Nana Fatima Abdulaziz; Marion Adebiyi; Prema Kirubakaran (2026) Assessment of the Cybersecurity Posture of the Federal Inland Revenue Service Against AI-Assisted Threats Using NIST, MITRE and ACGF Frameworks.
International Journal of Innovative Science and Research Technology, 11(11), 49-53.
https://doi.org/10.38124/ijisrt/26nov107

I. INTRODUCTION

The Federal Inland Revenue Service (FIRS) is a critical national institution that collects, processes and stores large volumes of taxpayer data, with direct consequences for state revenue, taxpayer confidentiality and national security [1], [2]. Artificial intelligence (AI) is both a defensive tool and a new source of risk, because attackers now use it for automated reconnaissance, realistic social engineering content and vulnerability testing [3], [4].

The NIST Cybersecurity Framework (CSF) and the MITRE Adversarial Tactics, Techniques, and Common Knowledge (MITRE ATT&CK) knowledge base are established tools for managing risk and modelling adversary behaviour [5], [6]. Neither was designed to test whether an organisation governs AI risk. The AI Cybersecurity Governance Framework (ACGF) fills this role as an overlay that adds AI risk management, accountability and lifecycle controls to existing technical frameworks [7], [8].

Many assessments of Nigerian public agencies remain compliance-focused or perimeter-focused and do not examine AI-specific governance gaps [9], [10]. This paper therefore asks whether FIRS is prepared for AI-assisted attacks, and it answers the question with a combined NIST, MITRE ATT&CK and ACGF assessment. The objectives were:

- To examine the current cybersecurity posture of FIRS;
- To explore the nature and evolution of AI-assisted cyber threats targeting public institutions;
- To assess FIRS readiness using the NIST Cybersecurity Framework;
- To map potential AI-enhanced attack vectors using MITRE ATT&CK; and
- To recommend an AI-aware cybersecurity framework suitable for FIRS.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26nov107

The study covers the FIRS systems and processes that can be examined ethically. No destructive penetration testing was carried out, and all simulations ran in controlled, authorised test settings.

II. RELATED WORK

➢ *Posture Assessment in Public Organisations*

Cybersecurity posture covers governance, technology, people and process readiness [11]. Studies in Nigeria report weak integrated governance and uneven adoption of frameworks such as NIST CSF across public agencies [1], [9]. The NIST CSF itself has been criticised for gaps in governance of emerging technologies [12].

➢ *AI in Cyber Offence and Defence*

Attackers use AI for scalable, adaptive attacks while defenders use machine learning to predict threats [3], [4]. Detectors that perform well on standard datasets can still be defeated by adversarial examples, poisoning and model-inversion attacks [10], [13]. This makes explainable models and clear oversight important [8].

➢ *ACGF and Framework Integration*

The ACGF adds AI lifecycle controls to cybersecurity governance: data provenance and labelling, model validation and drift detection, human-in-the-loop oversight, and ethical compliance, linked to procurement, vendor management and auditability [7], [14]. NIST CSF supplies the risk functions and MITRE ATT&CK the adversary techniques, and hybrid uses of the two have improved assessment performance [15], [16]. Most of these integrations stop at technical mapping and leave out AI governance.

➢ *Research Gap*

Existing assessments concentrate on technical controls and threat intelligence and rarely examine AI governance, model lifecycle controls, procurement oversight or accountability. For an institution holding large sensitive datasets and likely to adopt AI for analytics, this is a blind spot that adversaries can exploit. This study closes the gap by combining ACGF, NIST CSF and MITRE ATT&CK in one validated index.

III. METHODOLOGY

➢ *Research Design*

A qualitative design based on document analysis was used. It is non-intrusive, needs no direct system access, and treats FIRS policy documents (the cybersecurity policy, incident response plan, risk management policy and related records) as data to be analysed systematically. The study followed five phases: (1) system profiling and documentation review; (2) baseline posture review using NIST CSF; (3) adversarial threat mapping using MITRE ATT&CK; (4) governance alignment and AI risk assessment against the five ACGF pillars of Governance, Risk, AI Oversight, Incident Management and Compliance; and (5) development and validation of the Cybersecurity Posture Index (CPI).

➢ *Proposed Framework*

The proposed NIST, MITRE ATT&CK and ACGF framework links governance, operational controls and adversary behaviour (Fig 1). FIRS data sources feed a data collection layer. MITRE ATT&CK technique mapping and attack simulation produce threat data and simulation results for the NIST functions of Identify, Protect, Detect, Respond and Recover. Alerts and response data pass to ACGF governance, where incident management, risk and compliance, AI oversight and policy and ethics are assessed. The results feed a CPI dashboard and a continuous improvement loop.

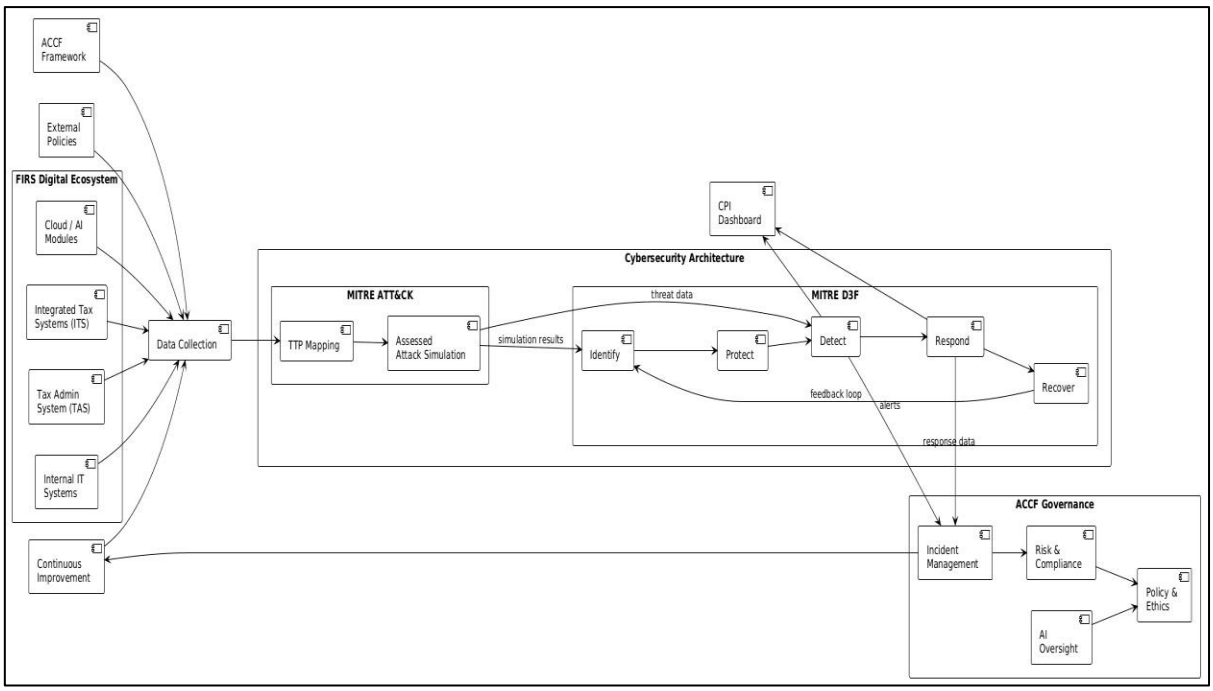


Fig 1 Architecture of the Integrated NIST, MITRE ATT&CK and ACGF Assessment Model

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26nov107

➢ *Data Collection and Analysis*

Evidence came from FIRS policy documents, a staff questionnaire on perceptions of cybersecurity and AI threats, and expert review workshops. The NIST CSF 2.0 module of the CISA Cybersecurity Evaluation Tool (CSET) was used to score the documented controls. Custom Python scripts, written in the PyCharm environment, mapped twelve MITRE ATT&CK techniques to AI-assisted attack scenarios, compared each scenario with the parsed policy text, and scored policy coverage. The ACGF pillars were rated from the policy text on maturity levels from Non-Existent to Developing. Questionnaire responses were coded, themes were extracted, and findings were compared with the framework scores.

The CPI combines the three component scores on a 0 to 5 scale, with weights of 0.4 for NIST and 0.3 each for MITRE and ACGF, as in (1).

$$CPI = 0.4\ NIST + 0.3\ MITRE + 0.3\ ACGF \quad (1)$$

➢ *Ethical Considerations*

All data handling complied with FIRS data protection policies and the Nigerian Cybercrime Act (2015). Permission was obtained before any analysis or simulation, and questionnaire responses were anonymised.

IV. RESULTS AND DISCUSSION

➢ *NIST CSF Baseline*

The CSET assessment shows a well-developed foundation for traditional cybersecurity (Table 1). Identify, Protect and Respond scored 4 out of 5 (Adaptive), while Govern, Detect and Recover scored 3 out of 5 (Repeatable). The five functions used in the composite (Identify, Protect, Detect, Respond and Recover) average 3.6.

Table 1 NIST CSF 2.0 Maturity Results

Function	Score (out of 5)	Key observation
Govern	3 / 5 (Repeatable)	Roles defined, but board-level reporting is not mandated.
Identify	4 / 5 (Adaptive)	Asset management and risk assessment are well defined and used to inform strategy.
Protect	4 / 5 (Adaptive)	Comprehensive access control, encryption and awareness training policies.
Detect	3 / 5 (Repeatable)	Monitoring procedures exist, but detection tool integration and advanced analytics are not documented.
Respond	4 / 5 (Adaptive)	Detailed incident response plan with clear roles and a full lifecycle.
Recover	3 / 5 (Repeatable)	Restoration is planned, but formal recovery testing schedules are absent.

➢ *MITRE ATT&CK Simulation*

The simulated AI-assisted techniques exposed weaknesses in detection and response (Table 2). The simulation was a what-if stress test of the policies. It asked whether they would hold against a capable AI-enabled attacker. The mean policy coverage score across the twelve techniques was 2.5.

Table 2 Selected MITRE ATT&CK Simulation Outcomes

AI-assisted technique	ATT&CK ID	Outcome
AI-generated spear phishing	T1566.002	Bypassed standard keyword filters. Policies give no guidance for verifying highly personalised AI-crafted requests.
Automated credential stuffing	T1110.004	Slow, distributed attempts evaded lockout thresholds tuned to high-volume single-source attacks.
Data poisoning (conceptual)	T1556, T1195	No mechanism validates the integrity of training data for AI or ML models used in analytics or fraud detection.

➢ *ACGF Governance Evaluation*

The ACGF review revealed the largest gaps (Table 3). FIRS governance is sound for traditional IT but does not treat AI as a new category of risk. The absence of AI oversight and the immature handling of AI risk are strategic exposures. The averaged ACGF score, scaled to 0 to 5, was 2.2.

Table 3 ACGF Pillar Evaluation

Pillar	Maturity	Finding
Governance	Initial	IT governance is defined, but no ownership of AI model risk, ethics or performance.
Risk Management	Developing	Assessments are mandated, but AI or ML threats are not listed as distinct risks.
AI Oversight	Non-Existent	Policies are silent on validating and overseeing automated decision-making.
Incident Management	Initial	The response plan has no playbooks for attacks on AI systems.
Compliance	Developing	National strategy is referenced, but AI regulations and ethics frameworks are not.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26nov107

➢ *Cybersecurity Posture Index*

Applying (1) to the component scores in Table 4 gives a CPI of 1.44 + 0.75 + 0.66 = 2.85 out of 5. Sensitivity testing with weights varied by 10 percent gave a range of 2.71 to 2.99, and the weighting rationale was reviewed by independent cybersecurity experts. A score of 2.85 corresponds to developing resilience with critical gaps. About 1.44 points come from the strong traditional controls, while the MITRE and ACGF components contribute 1.41 and expose the AI-specific shortfall.

Table 4 Composite CPI calculation

Component	Score	Weight	Contribution
NIST CSF	3.6	0.4	1.44
MITRE ATT&CK	2.5	0.3	0.75
ACGF	2.2	0.3	0.66
CPI			2.85

➢ *Staff Questionnaire and Discussion*

The questionnaire acted as a reality check on the framework scores. Staff reported that policies are hard to find, outdated and not reviewed, which contradicts the Identify score of 4. Incident response confidence was moderate and procedures were seen as undocumented, which contradicts the Respond score of 4. Backup failure and untested disaster recovery matched the weaker Recover score, and low AI awareness with no recent training matched the low ACGF score. Change management was named as the biggest operational challenge, a point the framework scores did not capture.

Taken together, the findings show that a NIST-only assessment would overstate readiness. The strong Respond policy score sits beside low staff awareness, which points to a policy-implementation gap. The low ACGF score also explains the specific gaps found by the MITRE simulation, such as no defence against data poisoning. The integrated approach therefore delivers the holistic view that the research problem called for.

V. CONCLUSION AND RECOMMENDATIONS

➢ *Conclusion*

FIRS has a strong foundation in standard information security, but its policies have not kept pace with AI-assisted threats. The main exposure is governance, not technology: no one owns AI risk, AI models are not overseen, and AI threats are absent from the risk register. The MITRE ATT&CK tests show that AI sharpens familiar attacks such as phishing and credential stuffing, and that no single framework gives the full picture. The CPI of 2.85 out of 5 summarises this position.

➢ *Recommendations*

- Governance: create an AI governance committee, or assign AI model risk to the Chief Information Security Officer, with authority to approve, monitor and audit AI and machine learning projects.
- Risk management: add data poisoning, model bias and drift, adversarial machine learning and AI supply chain compromise to the risk register and risk policy.
- Policy: develop an AI and machine learning security policy annex covering data lineage, training and retirement of models.
- People: extend awareness training to deepfakes, voice cloning and AI-generated phishing, with simulated exercises.
- Detection: adopt behaviour analytics and next-generation SIEM tools able to flag slow, low-volume AI-driven attacks.
- Supply chain and capacity: require transparency on training data and testing from AI vendors, build in-house adversarial machine learning skills, and join AI security communities.

➢ *Limitations*

The assessment relies mainly on written policy, so it shows design and intent rather than operational effectiveness. It is a snapshot of a fast-changing field, and the MITRE ATT&CK tests ran in a controlled setting that may not reflect a real AI-driven attack.

ACKNOWLEDGMENT

The authors thank the staff of the Federal Inland Revenue Service and the faculty and staff of the Department of Information Technology, Nile University of Nigeria, for their time, support and feedback.

REFERENCES

[1]. F. T. Ogunleye and R. Adeniran, “Assessing cybersecurity-posture maturity in Nigerian government institutions,” Int. J. Digital Security, vol. 10, no. 1, pp. 45–61, 2023.
[2]. R. O. Adebayo, T. A. Ogunyemi and A. J. Bello, “Cybersecurity maturity and organizational resilience in Nigeria’s public sector,” J. Information Security and Privacy, vol. 12, no. 4, pp. 55–68, 2022.
[3]. N. Moustafa, S. Milajerdi and J. Slay, “AI-driven network anomaly detection for cyber-physical systems,” Computers & Security, vol. 134, art. 103470, 2023.
[4]. Y. Huang, X. Chen and Z. Wang, “Adaptive AI-based phishing generation and defense mechanisms,” Expert Systems with Applications, vol. 221, art. 119837, 2023.
[5]. NIST, Framework for improving critical infrastructure cybersecurity, Version 2.0. National Institute of Standards and Technology, 2023.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26nov107

[6]. MITRE, MITRE ATT&CK knowledge base of adversary tactics and techniques. The MITRE Corporation, 2024. [Online]. Available: https://attack.mitre.org
[7]. H. Aslam and A. Bary, "AI Cybersecurity Governance Framework (ACGF): A model for responsible AI risk management," IEEE Access, vol. 12, pp. 11022–11034, 2024.
[8]. L. P. Nguyen, K. Tran and V. Dao, "Explainable AI in cybersecurity governance frameworks: Challenges and future trends," J. Information Systems Security, vol. 12, no. 4, pp. 79–95, 2023.
[9]. M. Oladele and F. Mbah, "Applying NIST CSF to Nigeria's telecom industry for risk governance," African J. Computing and ICT, vol. 15, no. 3, pp. 210–225, 2022.
[10]. J. Chio and T. Freeman, "Adversarial learning and intrusion evasion in cybersecurity systems," ACM Computing Surveys, vol. 55, no. 7, pp. 1–25, 2023.
[11]. A. Bada, P. Johnson and U. Eze, "Cybersecurity posture in the African public sector: Challenges and opportunities," African J. Information Systems, vol. 13, no. 2, pp. 112–130, 2021.
[12]. D. Meza, L. Carter and G. Hinton, "Comparative analysis of NIST CSF and ISO 27001 frameworks for infrastructure resilience," J. Cybersecurity Research, vol. 11, no. 3, pp. 142–158, 2023.
[13]. Y. Li, D. Zhou and H. Xu, "Deep neural networks for intelligent phishing detection," Information Sciences, vol. 600, pp. 453–467, 2022.
[14]. Y. Alotaibi and O. El-Gayar, "Integrating NIST CSF and MITRE ATT&CK for healthcare cybersecurity resilience," Information Systems Frontiers, vol. 25, no. 5, pp. 1301–1316, 2023.
[15]. F. Alghamdi, Y. Alotaibi and M. Alzahrani, "A hybrid cybersecurity-posture assessment model for public agencies," J. Cyber Policy and Risk, vol. 8, no. 1, pp. 89–110, 2024.
[16]. T. Bary, C. Mensah and D. Gopal, "Simulation-based hybrid framework for cybersecurity risk prioritization," J. Information Assurance and Security, vol. 18, no. 3, pp. 77–93, 2022.