International Journal of
Advances in Scientific Research and Engineering (ijasre)

E-ISSN : 2454-8006

DOI: 10.31695/IJASRE.2020.33695

Volume 6, Issue 1
January - 2020

# CYBER SECURITY FRAMEWORK FOR NIGERIAN CIVIL AVIATION AUTHORITY, HEADQUARTERS

**Roger-Nick Anaedevha & Aminat Ajibola**

Computer Science Department,

University of Abuja, Nigeria.

## ABSTRACT

*The practice of defending assets from unauthorized access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction is as ancient as man's existence on earth. Cybersecurity, information security, and computer security are further attempts of man to continue the same ancient practice. This is due to the unavoidably prevalent need and use of information and communication technologies in this century, which has left the man with such vulnerability and insecurity through its devices and infrastructures. The aviation industry, being one of the most economic and leisure viable industry in the world has been at the top-notch of the use of these technologies for better services to man. Nigeria Aviation industry is one of the largest and most viable in Africa is opened to the vulnerabilities and cyber threats that comes with these advanced technologies. However, several methods and programs have been employed by various organizations and stakeholders, but, the Nigerian Civil Aviation Authority (NCAA), been the apex governing body that control, monitor and regulate the economic and safety oversight of the entire Aviation industry in Nigeria seems not to have gotten it right with the recent trends of cyber warfare in the industry as opposed to their counterparts in the world over. Therefore, this research study attempts to employ data from existing literature and questionnaires to analyze the existing practices of cyber/information security programs (if any) within the NCAA and to design an adaptable cybersecurity framework that is robust enough for its safety. By using version 3.9.3 of Waikato Environment for Knowledge Analysis (WEKA) software, Naïve Bayes, Bayes Net, Decision Table, IBK (Linear NNSearch), REP Tree, J48, SMO, Simple Logistic, and Bagging are the nine algorithms employed to determine and predict tier classes as existing profile and target profile respectively for NCAA within the framework. SMO emerge best fit to predict the target profile while the Bagging algorithm emerges best fit to determine the current profile. Gaps and implementable action plans were deduced. Thereafter, the RNA Cyber Security Framework (RNA-CSF) is conceptually developed, analyzed and proposed for NCAA and for any other organization that has the need to use it.*

**Keywords**: Nigeria civil aviation Authority, Cyber security framework, WEKA tools, Predicting algorithms, Conceptual model.

## 1. INTRODUCTION

Aviation Industry is said to be supporting 6.8 million jobs and makes a $72.5 billion contribution to Africa Gross Domestic Product (GDP) [1]. This accounts for 11% of the jobs and 3% of the GDP supported by the air transport industry worldwide. In Nigeria, Air transport directly provides about 93,000 jobs and supports more than 650,800 jobs including tourism-related employment. While contributing about $10 billion to the country's GDP, it is also forecasted that over the next ten to twenty years passenger volumes in Nigeria will be growing between 7 to 15% annually, [[2], [3], [4]]. The growth and sustenance of such economically viable industry can be challenged through its critical infrastructures that are highly dependent on computer technologies, cyber networks, and information systems. According to [5], cyber systems hackers bombard aviation industry globally with over 1,000 attacks per month. Nigeria Aviation industry has recorded sort of such attacks as Arik Air booking database system was hacked in 2012 [6].

No doubt, several attempts may have been made by corporations in the Nigeria Aviation industry concerning its computer systems, networks and applications, from cyber risk management processes to technical IT security applications in order to improve its cyber environment. The IT security start-up solutions provided through International Civil Aviation Organization's (ICAO) Standards and Recommended Practices (SARPs) have been developed over the years [7]. [8] had also enumerated some of the milestone moves by ICAO to curb the increasing menace of cyber security in Aviation. And in fact, on 7th to 9th of May, 2018, ICAO still had a regional program, [7] among other several past programs to establish and build cyber security risk management system among member nations. Yet, individual national civil aviation authorities such as the Nigeria Civil Aviation Authority (NCAA) have not been able to develop blue print plan to build its cyber security management structure nor in regulating same on the rest industry organizations to take cue [9]. With safety as a top priority, International Air Transport Authority (IATA) conducts yearly audits mandated by governments and provides airlines with a cyber-security toolkit that has a traditional risk assessment approach [10]. This has served many airlines in a way though not much among Nigerian airlines as lot of bookings among other operations is still manually done. On the other hand, IATA approach plan to cyber security is mainly for airlines and associated organizations which had nothing or little to do with the regulatory body like NCAA. Though basic IT security that comes with IT infrastructures and use are in place, but, as long as there had not been a major attack, like every other organization would be, NCAA seem not to have prioritize cyber security management in its IT operations. Hence, this study provides a cyber-security framework (CSF) for NCAA that is holistic in application by assessing its current cyber security management plan, its functionality, vulnerability, competence, as well as unravel critical niches of improvement. The cyber security framework of the United States' National Institute of Standards and Technology (NIST) is adopted to design the framework.

## 2. THE NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST) CYBER SECURITY FRAMEWORK (CSF)

On February 12, 2013, Executive Order 13636 of the United States Government, through the Commerce Department's National Institute of Standards and Technology (NIST), provided information technology leaders with a cyber-security Framework (CSF). The CSF provides a set of voluntary cyber security guidelines designed as a model to enable organizations to take steps in improving security and resiliency, thereby improving critical infrastructure cyber security.

Example of organizations that have used and apply the NIST CSF is Intel [11]. After using the Framework, Intel stated that "the Framework can provide value to even the largest organizations and has the potential to transform cyber security on a global scale by accelerating cyber security best practices". A group of professional companies in Japan called "The Cross-Sector Forum" has adopted the NIST CSF in their various companies with successful results of top-notch information security practices [12]. The University of Pittsburgh Information Technology was drastically improved by the adoption of the NIST cyber security framework and use of NIST 800 -171 [13]. Accordingly, this enable thorough mapping of the gaps to the risk consequences and thereby creates the action plans successfully for implementation.

### 2.1 The three components of NIST cyber security framework

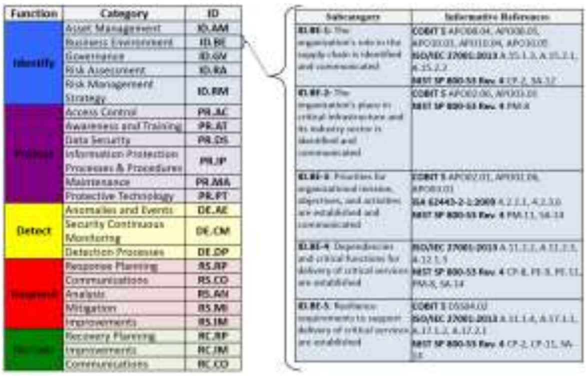
The three main components of the NIST Framework are the Core, the Framework Implementation Tiers (Tiers), and the Profile.

CORE
TIERS
CYBERSECURITY
FRAMEWORK
PROFILE

**Figure 1: The NIST Cyber Security Framework (Source: [11])**

The **Core** is a set of "cyber security activities, desired outcomes, and applicable Informative References that are common across critical infrastructure sectors." The Core comprises four elements: Functions, Categories, Subcategories, and Informative References. **Functions** provide a high-level, strategic view of the lifecycle of an organization's management of cyber security. There are five elements comprising the Functions: Identify, Protect, Detect, Respond, and Recover. Each Function is divided into Categories, Subcategories, and Informative References. The **C**ategories are cyber security outcomes that are closely tied to programmatic needs and particular activities. The Subcategories are specific outcomes of technical and/or management activities that support achievement of each Category. Informative References are specific cross-sector standards, guidelines, and effective practices that illustrate a method to achieve the outcomes associated with each Subcategory. This covers topics across cyber, physical, and personnel, with a focus on business outcomes.

DOI: 10.31695/IJASRE.2020.33695



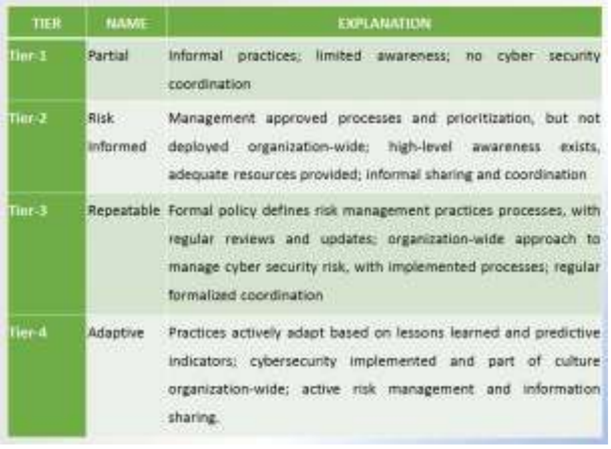
| Function | Category | ID |
|---|---|---|
| Identify | Asset Management | ID.AM |
| | Business Environment | ID.BE |
| | Governance | ID.GV |
| | Risk Assessment | ID.RA |
| | Risk Management Strategy | ID.RM |
| Protect | Access Control | PR.AC |
| | Awareness and Training | PR.AT |
| | Data Security | PR.DS |
| | Information Protection Processes & Procedures | PR.IP |
| | Maintenance | PR.MA |
| | Protective Technology | PR.PT |
| Detect | Anomalies and Events | DE.AE |
| | Security Continuous Monitoring | DE.CM |
| | Detection Processes | DE.DP |
| Respond | Response Planning | RS.RP |
| | Communications | RS.CO |
| | Analysis | RS.AN |
| | Mitigation | RS.MI |
| | Improvements | RS.IM |
| Recover | Recovery Planning | RC.RP |
| | Improvements | RC.IM |
| | Communications | RC.CO |

| Subcategory | Informative References |
|---|---|
| **ID.BE-1:** The organization's role in the supply chain is identified and communicated | **COBIT 5** APO08.04, APO08.05, APO10.03, APO10.04, APO10.05<br>**ISO/IEC 27001:2013** A.15.1.3, A.15.2.1, A.15.2.2<br>**NIST SP 800-53 Rev. 4** CP-2, SA-12 |
| **ID.BE-2:** The organization's place in critical infrastructure and its industry sector is identified and communicated | **COBIT 5** APO02.06, APO03.01<br>**NIST SP 800-53 Rev. 4** PM-8 |
| **ID.BE-3:** Priorities for organizational mission, objectives, and activities are established and communicated | **COBIT 5** APO02.01, APO02.06, APO03.01<br>**ISA 62443-2-1:2009** 4.2.2.1, 4.2.3.6<br>**NIST SP 800-53 Rev. 4** PM-11, SA-14 |
| **ID.BE-4:** Dependencies and critical functions for delivery of critical services are established | **ISO/IEC 27001:2013** A.11.2.2, A.11.2.3, A.12.1.3<br>**NIST SP 800-53 Rev. 4** CP-8, PE-9, PE-11, PM-8, SA-14 |
| **ID.BE-5:** Resilience requirements to support delivery of critical services are established | **COBIT 5** DSS04.02<br>**ISO/IEC 27001:2013** A.11.1.4, A.17.1.1, A.17.1.2, A.17.2.1<br>**NIST SP 800-53 Rev. 4** CP-2, CP-11, SA-14 |

**Figure 2: Example of Categories, Subcategories and Informative References (Source: [11] )**

### 2.2 The tiers

The framework defines tiers that describe the level to which the requirements are implemented. The tiers are sometimes referred to as maturity levels, but according to NIST these are more a tool for internal communication between cyber security risk management and operational risk management, and should not be seen as maturity level. Nevertheless, higher tiers represent higher degree of sophistication and maturity in the management of cyber security risks and responses. The tiers describe an organization's approach to "cyber security risk and the processes in place to manage that risk," ranging from Tier 1 (Partial), Tier 2 (Risk Informed), Tier 3 (Repeatable), to Tier 4 (Adaptive).



| TIER | NAME | EXPLANATION |
|---|---|---|
| Tier-1 | Partial | Informal practices; limited awareness; no cyber security coordination |
| Tier-2 | Risk informed | Management approved processes and prioritization, but not deployed organization-wide; high-level awareness exists, adequate resources provided; informal sharing and coordination |
| Tier-3 | Repeatable | Formal policy defines risk management practices processes, with regular reviews and updates; organization-wide approach to manage cyber security risk, with implemented processes; regular formalized coordination |
| Tier-4 | Adaptive | Practices actively adapt based on lessons learned and predictive indicators; cybersecurity implemented and part of culture organization-wide; active risk management and information sharing. |

**Figure 3: Tiers and their Explanation (Source: [14])**

## 3.0 ANALYSIS

Data from questionnaires based on the core of the framework which involved the five functions of Identify, Protect, Detect, Respond, and Recover are collected from 120 out of 430 staff of NCAA headquarters, Lagos. Hence, according to the NIST CSF structure described, the analysis of the organization data determines the current Tier of the organization and also predict the target profile (Tier). Thereby providing the gaps between the current profile and the target profile. By using version 3.9.3 of Waikato Environment for Knowledge Analysis (WEKA) software, nine algorithms were tested in determining and predicting current tier as existing profile and target profile respectively for NCAA within the framework. Thereafter, from the approach of [15] and other industry practitioners, the risk factors corresponding to NCAA current Tier, and the gaps will be determined at step 4 of figure 4.

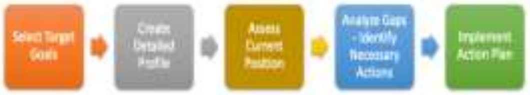


**Figure 4: Steps to Implement NIST CSF (Source: [15] )**

Step 1 is to set target goals for the organisation. This will be suggested as the next phase of the target profile which NCAA could implement to close the gaps exposed from currently observe profile and Tier. Step 2 is to create a detailed profile. It involves determining details of the organisation's Risk Management Processes, Integrated Risk management Program and External Participation, which are Process, tools and people respectively related. This step 2 will be contracted with step 3 in this study because it defines one among the four Tiers of the framework and there by opens all necessary metrics necessary for the risk assessment. Step 3 is to basically determine the risk assessment position of the organization through its people, tools and

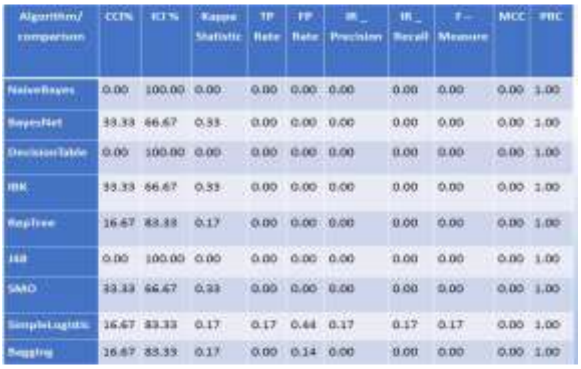
DOI: 10.31695/IJASRE.2020.33695

processes. Finally, the gaps created by the risk factors associated with the identified Tier will be analysed and proffered actions necessary for implementation by the organisation for progress to target profile will be uncovered.

### 3.1 Determining Current Profile

In this study classification rather than regression algorithms are chosen using WEKA due to the imbalance dataset where the class distribution is not uniform among the classes, typically comprising majority (negative) class and the minority (positive) class. The stratification is between the “Data” instance class and the “Tier” class. Bagging algorithm was sampled in the experiment rather than *CostSensitiveClassifier* algorithm in the “Meta” classifier for this imbalanced dataset. This is due to the limiting factor of the “Tier” class instances associated with the dataset towards “CostSensitiveClassifier”. These nine algorithms (NaiveBayes, BayesNet, DecisionTable, IBK (Linear NNSearch), REPTree, J48, SMO, SimpleLogistic, and Bagging are better fit to be applied to strongly imbalanced datasets such as obtained in this study in which the number of negatives outweighs the number of positives significantly [16]. Which is why PRC than ROC provides more accurate prediction of future classification performance. This is due to the fact that PRC evaluate the fraction of true positives among positive predictions. Cross Validation is set to 6 (folder) in the experiment “setup” phase to be maximum with number of instances in the dataset. The experiment is “Run” without any error before testing with “Paired T-Tester (corrected)” in the “analyze” phase as shown with the output results in figure 5.

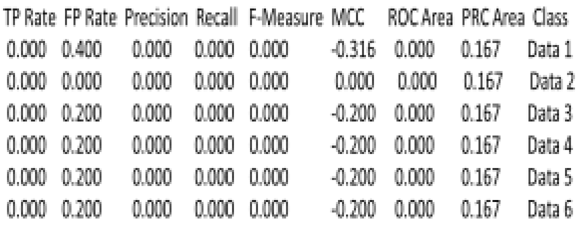
**Table 1: The 9 algorithms and their comparison (source: Derived)**



| Algorithm/ comparison | CCI% | ICI % | Kappa Statistic | TP Rate | FP Rate | IR_ Precision | IR_ Recall | F-- Measure | MCC | PRC |
|---|---|---|---|---|---|---|---|---|---|---|
| NaiveBayes | 0.00 | 100.00 | 0.00 | 0.00 | 0.00 | 0.00 | 0.00 | 0.00 | 0.00 | 1.00 |
| BayesNet | 33.33 | 66.67 | 0.33 | 0.00 | 0.00 | 0.00 | 0.00 | 0.00 | 0.00 | 1.00 |
| DecisionTable | 0.00 | 100.00 | 0.00 | 0.00 | 0.00 | 0.00 | 0.00 | 0.00 | 0.00 | 1.00 |
| IBK | 33.33 | 66.67 | 0.33 | 0.00 | 0.00 | 0.00 | 0.00 | 0.00 | 0.00 | 1.00 |
| RepTree | 16.67 | 83.33 | 0.17 | 0.00 | 0.00 | 0.00 | 0.00 | 0.00 | 0.00 | 1.00 |
| J48 | 0.00 | 100.00 | 0.00 | 0.00 | 0.00 | 0.00 | 0.00 | 0.00 | 0.00 | 1.00 |
| SMO | 33.33 | 66.67 | 0.33 | 0.00 | 0.00 | 0.00 | 0.00 | 0.00 | 0.00 | 1.00 |
| SimpleLogistic | 16.67 | 33.33 | 0.17 | 0.17 | 0.44 | 0.17 | 0.17 | 0.17 | 0.00 | 1.00 |
| Bagging | 16.67 | 83.33 | 0.17 | 0.00 | 0.14 | 0.00 | 0.00 | 0.00 | 0.00 | 1.00 |

Based on the CCI and Kappa Statistic analysis, BayeNet, IBK, and SMO with 33.33% records seems better than RepTree, SimpleLogistic and Bagging algorithms of 16.67% records, while NaïveBayes, DecisionTable and J48 with 0.00% records are less fit. However, the result is accepted because no single algorithm always performed the best for each dataset [17] especially experimental level. Therefore, this comparison, according to [18], is enough to define which of the algorithms evaluated in the experiment had the best performance in order to create a good performance model, and the rank of algorithms by performance. The rank of algorithms by performance will enable the prediction of the target tier next to the current profile. Based on the foregoing, the second three algorithms which are REPTree, SimpleLogistic and Bagging with single instance of CCI represented by 16.67 %, are best to be considered in determining that particular class instance. Thereafter, the BayeNet, IBK, and SMO algorithms with two best CCI represented with 33.33% will be experimented for prediction of target profile. In experimenting the classification of algorithms using “Ranking” in “Test Base”, it is shown that Bagging algorithm under meta classifier is preferred over simpleLogistic under function classifier and REPTree under trees classifier. This means the class tier instance must be considered separately using the WEKA “Explorer”. In exploring the Bagging algorithm, Tier 1 is determined from the cluster of all class instance of “tier”. According to [19], classification results are taken on maximum number of votes for classification purpose, which in this case is the data1 representing tier1. The primary advantage of Bagging is that variation is reduced and performance is improved for unsteady classifiers which differ meaningfully with small changes in the dataset, especially with an imbalanced dataset.

**Table 2: Bagging Algorithm of class “data” instance (Source: derived)**



| TP Rate | FP Rate | Precision | Recall | F-Measure | MCC | ROC Area | PRC Area | Class |
|---|---|---|---|---|---|---|---|---|
| 0.000 | 0.400 | 0.000 | 0.000 | 0.000 | -0.316 | 0.000 | 0.167 | Data 1 |
| 0.000 | 0.000 | 0.000 | 0.000 | 0.000 | 0.000 | 0.000 | 0.167 | Data 2 |
| 0.000 | 0.200 | 0.000 | 0.000 | 0.000 | -0.200 | 0.000 | 0.167 | Data 3 |
| 0.000 | 0.200 | 0.000 | 0.000 | 0.000 | -0.200 | 0.000 | 0.167 | Data 4 |
| 0.000 | 0.200 | 0.000 | 0.000 | 0.000 | -0.200 | 0.000 | 0.167 | Data 5 |
| 0.000 | 0.200 | 0.000 | 0.000 | 0.000 | -0.200 | 0.000 | 0.167 | Data 6 |

DOI: 10.31695/IJASRE.2020.33695

With the bagging algorithm result, it is deduced that the most classified instance which is data1 has the highest FP Rate of 0.400 and lowest MCC of -0.316 to be taken as the existing tier of NCAA in the NIST cyber security framework. This connotes that informal practices; limited awareness; and absence cyber security coordination are most likelihood in the organization. This will further be analyzed with the target profile to find the actual gaps.

### 3.2 Predicting target Profile

To Predict target profile, the BayeNet, IBK, and SMO algorithms with each of 33.33% records of CCI are to be experimented. The record shows the CCI significance of 2 out of 6 instances. This is accomplished by first "ranking" the algorithms through the "test base" of the experiment and clustering the "Tier" class Instances of each of the highest rank algorithm. On the ranking, with confidence of 0.05 (two tailed) SMO is ranked best fit before IBK and lastly bayesNet. Hence, the result of the prediction of the "farthestFirst" and "Expectation and Maximization (EM)" clusterers of Tier class instance in SMO is shown as follows; FarthestFirst:

```
Clustered Instances
            0      5 ( 83%)
            1      1 ( 17%)
            Class attribute: TIER
            Classes to Clusters:
            0 1  <-- assigned to cluster
            0 1 | Tier1
            2 0 | Tier2
            2 0 | Tier3
            1 0 | Tier4
            Cluster 0 <-- Tier2
            Cluster 1 <-- Tier1
            Incorrectly clustered instances : 3.0          50 % ( this still due to the imbalanced data set)
```

While the EM (Expectation and Maximization) clusterer, still using the "classes to clusters evaluation" mode outputs tier 2 directly as predicted tier.

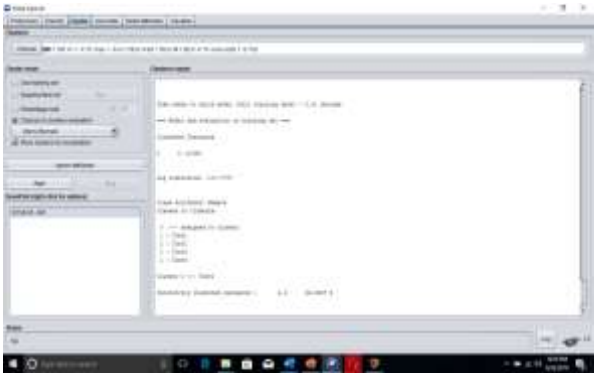


**Figure 5: EM cluster of SMO, predicting Target Profile (tier2) (Source: Derived)**

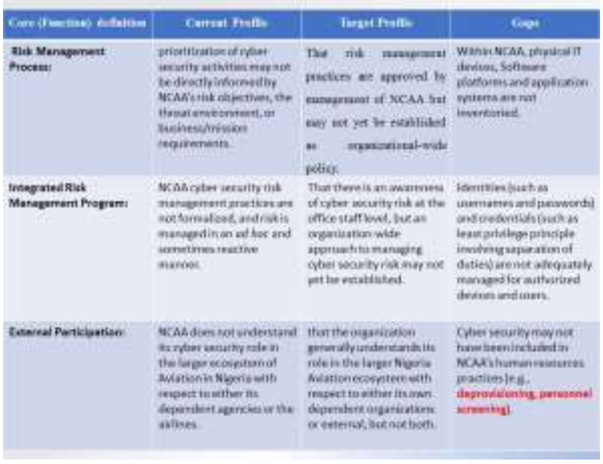
This study uses "classes to clusters evaluation" instead of "use training set" due to the variability of the "tier" class to determine the predicted "tier" class. Hence, among the 4 tiers, Tier2 is predicted as the target profile after the existing tier 1 profile. The kappa statistic which compare the "observed" and "expected" accuracy is – 0.2, which according to [20] and [21] signifies satisfactory classification for such an imbalanced dataset prediction. This guides to the gaps between tier 1 and tier 2 in the framework function's categories and subcategories to be addressed in the organization's information security.

### 3.3 The Gaps and Implementable Plan

Risk Management process, Integrated Risk Management Program and External Participation are the three implementation headings that summarises the core five functions, categories to subcategories of the NIST CSF in which gaps can be simply classified [11]. This enables the tracing of the gaps as the summarized example in table 3.

DOI: 10.31695/IJASRE.2020.33695

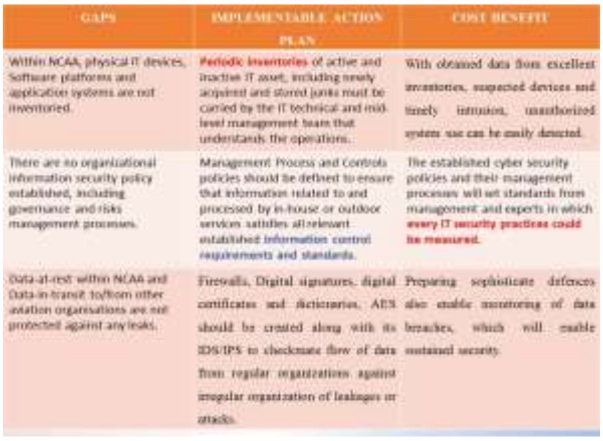
**Table 3: Summarized example of NCAA current tier, Target profiles and the gaps (Source: Derived)**



| Core (Function) definition | Current Profile | Target Profile | Gaps |
|---|---|---|---|
| **Risk Management Process:** | prioritization of cyber security activities may not be directly informed by NCAA's risk objectives, the threat environment, or business/mission requirements. | The risk management practices are approved by management of NCAA but may not yet be established as organizational-wide policy. | Within NCAA, physical IT devices, Software platforms and application systems are not inventoried. |
| **Integrated Risk Management Program:** | NCAA cyber security risk management practices are not formalized, and risk is managed in an ad hoc and sometimes reactive manner. | That there is an awareness of cyber security risk at the office staff level, but an organization-wide approach to managing cyber security risk may not yet be established. | Identities (such as usernames and passwords) and credentials (such as least privilege principle involving separation of duties) are not adequately managed for authorized devices and users. |
| **External Participation:** | NCAA does not understand its cyber security role in the larger ecosystem of Aviation in Nigeria with respect to either its dependent agencies or the airlines. | that the organization generally understands its role in the larger Nigeria Aviation ecosystem with respect to either its own dependent organizations or external, but not both. | Cyber security may not have been included in NCAA's human resources practices (e.g., deprovisioning, personnel screening). |

Table 4 is a summarized example of the implementable action plan against the gaps with their corresponding benefits. The sources of the implementation plan and cost benefits are summaries from [11] and [22].

**Table 4: summarized example of the Implementable Action plan against Gaps and their corresponding Benefits. (Source: Derived)**



| GAPS | IMPLEMENTABLE ACTION PLAN | COST BENEFIT |
|---|---|---|
| Within NCAA, physical IT devices, Software platforms and application systems are not inventoried. | Periodic inventories of active and inactive IT asset, including newly acquired and stored junks must be carried by the IT technical and mid-level management team that understands the operations. | With obtained data from excellent inventories, suspected devices and timely intrusion, unauthorized system use can be easily detected. |
| There are no organizational information security policy established, including governance and risks management processes. | Management Process and Controls policies should be defined to ensure that information related to and processed by in-house or outdoor services satisfies all relevant established information control requirements and standards. | The established cyber security policies and their management processes will set standards from management and experts in which every IT security practices could be measured. |
| Data-at-rest within NCAA and Data-in-transit to/from other aviation organisations are not protected against any leaks. | Firewalls, Digital signatures, digital certificates and dictionaries, AES should be created along with its IDS/IPS to checkmate flow of data from regular organizations against irregular organization of leakages or attacks. | Preparing sophisticate defences also enable monitoring of data breaches, which will enable sustained security. |

## 4 THE PROPOSED FRAMEWORK FOR NIGERIAN CIVIL AVIATION AUTHORITY (NCAA)

Combining [23] work on the four major steps to obtain cyber security maturity model with the five steps in [15] to obtain that maturity, the NIST Cyber Security Framework just analyzed could be remodeled. Hence, the derived framework is here referred to as the RNA cyber security framework (RNA-CSF)

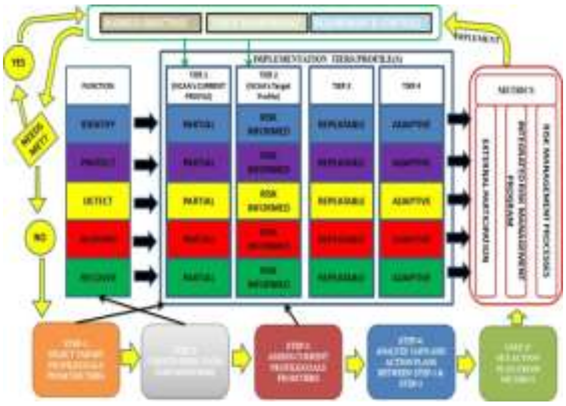

IMPLEMENT
IMPLEMENTATION TIERS/PROFILE(S)
YES
NEEDS MET?
NO
FUNCTION
IDENTIFY
PROTECT
DETECT
RESPOND
RECOVER
TIER 1 (NCAA's CURRENT PROFILE)
TIER 2 (NCAA's Target Profile)
TIER 3
TIER 4
PARTIAL
RISK INFORMED
REPEATABLE
ADAPTIVE
METRICS
EXTERNAL PARTICIPATION
INTEGRATED RISK MANAGEMENT PROGRAM
RISK MANAGEMENT PROCESSES
STEP 4 ANALYZE GAPS AND ACTION PLANS BETWEEN STEP 1 & STEP 3

**Figure 6: RNA Cyber Security Framework (RNA-CSF) (source: Derived)**

DOI: 10.31695/IJASRE.2020.33695

The RNA Cyber security Framework (RNA-CSF) in figure 6 is a conceptual model to mitigate against cyber/information security as derived from various concepts and analysis of this study. From the moment an organization exists with business objective, it is already having an information/cyber threat environment around it and therefore will have requirements and control needs to remain sustainable in the midst of unavoidable attacks. It therefore means the option of "prevention" as a function in this framework is irrelevant due to unavoidable threats and attack incident the organization may have been exposed. **Step-1** in the framework begins to address the organization needs by selecting a target profile, also called a target goal from the tiers as much the tiers suites the expected outcome/needs of the organization. The **step-2** is employed to create specific needs from the subcategories embedded in the categories of the framework's function. This is necessary due to detail recommendations and strategies already designed within the subcategories. **Step-3** enables the organization to assess its current profile/state from the tiers. The tiers are in a progressive degree of security capabilities, as it is protruding from the function, tier-1 is partial, tier-2 is risk informed, tier-3 is repeatable, and tier-4 is adaptive as they have been described and used in this study. However, irrespective of the assess status of tier which the organization falls into, there must be gaps between that tier and the target profile/tier which is needed. Therefore, the organization must analyze these gaps from the subcategories under the different tiers and been able to trace and deduce right implementable plans. This forms the **step-4** of the framework. **Step-5** is to set action plans from the three metrics. The metrics are actionable breakdown of the implementable plans into 3 categories for easy execution and to achieve needed result in the organization. When the action plans are implemented in the form of metrics, they can be measured by indicators within the metrics. The next step is to see if the implementation fits into the organizations business objective. If it does, the cyber security set needs of the organization are met and business can be continued for better sustainability otherwise the organization may proceed recursively to step-1 for the selection of next desired and target profile from the tiers and the loop continues till there is sustainability.

## 5 CONCLUSION

Outside the Nigerian Civil Aviation Authority, the RNA Cyber Security Framework (RNA-CSF) can provide value regardless of size, type of organization, or degree of cyber security risk or sophistication already existing in any organization. This is due to the fact that the robustness of the framework as well as the specific and strategic steps that directs the use, will make any organization understand and address different threats, vulnerabilities, risks, and risk tolerances. RNA-CSF is systematic enough that NCAA should adopt in approaching cyber security as it require much engagement from the Directorates, Boards, Management and other senior executives to protect critical business information without constraining operations and growth. Direct technical approach to solving such organization's cyber security problem, or at least part of the problem, can often have a negative impact on the objectives by tightly constraining how contractors, other aviation organizations and employees interact with its applications, data and physical infrastructure.

## REFERENCES

[1] ATAG (Air Transport Group) (2016). Aviation: Benefits beyond borders. (online). Available at: https://www.atag.org/component/attachments/attachments.html?id=607 (Accessed: October 19, 2018).

[2] Oxford Economics (2012), Economic Benefits from Air Transport in Nigeria. UK: Oxford.

[3] Stephens M.S., Ikeogu V., Stephens O.B., Ukpere W.I. (2014). Empirical Analysis of the Contribution of the Aviation Industry to the Nigerian Economy, *Mediterranean Journal of Social Sciences*, 5(3), pp. 115 - 125.

[4] Adekola, Shola (2017), "Air transport contributes $8.2bn to Nigeria's GDP —IATA", *Nigerian Tribune (Aviation)*, August 17, 2017. (online). Available at: http://www.tribuneonlineng.com/air-transport-contributes-8-2bn-nigerias-gdp-iata/ (Accessed: May 2, 2018)

[5] Valero J. (2016), "Hackers bombard aviation sector with over 1,000 attacks per month", *Euractiv (Justice & Home Affairs).* (online). Available at: https://www.euractiv.com/section/justice-home-affairs/news/hackers-bombard-aviation-sector-with-more-than-1000-attacks-per-month/ (Accessed: April 15, 2018)

[6] Ogala E. (2012). "Hackers attack Arik Air website in protest of poor customer service", *Premium Times, (News)* (online). Availble from: http://www.premiumtimesng.com/news/101768-hackers-attack-arik-air-website-in-protest-of-poor-customer-service.html (Accessed: June 23, 2017).

DOI: 10.31695/IJASRE.2020.33695

[7] ICAO (Iternational Civil Aviation Organization) (2018), ICAO SUMMIT ON CYBERSECURITY IN CIVIL AVIATION EUROPE, MIDDLE EAST AND AFRICA (EMEA). (online). Available at: https://www.icao.int/Meetings/CYBER2018 (Accessed: May 26, 2018)

[8] Lim B. (2014). Emerging Threats from Cyber Security in Aviation – Challenges and Mitigations, Ministry of Transport, Singapore, Journal of Aviation Management, (), pp. 83 - 91.

[9] NCAA (Nigerian Civil Aviation Authority) (2018), "NCAA Responsibilities", *Nigerian Civil Aviation Authority*, (online). Available at: http://www.ncaa.gov.ng/about-ncaa/ncaa-responsibilities/ (accessed: April 29, 2018)

[10] IATA (International Air Transport Association (2015), ANNUAL REVIEW 2015. (online). Available at: https://www.iata.org/about/Documents/iata-annual-review-2015.pdf (Accessed: June 15, 2018)

[11] NIST (National Institute of Standards and Technology) (2018), uses and benefits of the framework, (online). *National Institute of Standards and Technology*, Available at: https://www.nist.gov/cyberframework/online-learning/uses-and-benefits-framework (Accessed: March 21, 2018)

[12] Ueno K. (2018), https://www.nist.gov/document/japancrosssectorforumsuccessstorypdf (Accessed: October 20, 2018)

[13] Silverstein J. C. (2018) https://www.nist.gov/document/nistframeworksuccessstory-finalpdf (Accessed: October 20, 2018)

[14] SSH Communications Security (2017), "NIST Cyber Security Framework", *Compliance*. (Online). Available at: https://www.ssh.com/compliance/cybersecurity-framework/(Accessed: November 2, 2018).

**[15]** *Sahai* A. (2018), 5 Steps to Turn the NIST Cybersecurity Framework into Reality, *(articles)*. (online). Available at: https://www.securitymagazine.com/articles/88624-steps-to-turn-the-nist-cybersecurity-framework-into-reality (accessed: October 21, 2018)

[16] Saito T. and Rehmsmeier M. (2015), The Precision-Recall Plot Is More Informative than the ROC Plot When Evaluating Binary Classifiers on Imbalanced Datasets, (online), Available at: https://doi.org/10.1371/journal.pone.0118432 (Accessed: September 19, 2019)

[17] Ranjita D (2013), Selection Of The Best Classifier From Different Datasets Using WEKA. (online). Available at: https://www.researchgate.net/profile/Ranjita_Dash/publication/313648961_Selection_Of_The_Best_Classifier_From_Different_Datasets_Using_WEKA/links/58a178bd92851c7fb4bf615f/Selection-Of-The-Best-Classifier-From-Different-Datasets-Using-WEKA.pdf (Accessed: June 5, 2019).

[18] Brownlee J.(2019), Weka Machine Learning, (online). Available at: https://machinelearningmastery.com/how-to-run-your-first-classifier-in-weka/ (Accessed: September 19, 2019)

[19] Bal R. and Sharma S. (2016), Review on Meta Classification Algorithms using WEKA, *International Journal of Computer Trends and Technology*, 35(1), pp. 38 – 47.

[20] Landis, J.R. and Koch, G.G. (1977), The Measurement of Observer Agreement for Categorical Data, *Biometric*, 33, pp. 159-174.

[21] Mahajan A. and Ganpati A. (2014), Performance Evaluation of Rule Based Classification Algorithms, *International Journal of Advanced Research in Computer Engineering & Technology*, 3(10), pp. 3546 -3550.

22] Barrett M. (2017), "How to Use the NIST Cybersecurity Framework", blogs (security blogs). (online). Available at: https://www.securitymagazine.com/blogs/14-security-blog/post/88890-how-to-use-the-nist-cybersecurity-framework (Accessed: November 2, 2018)

[23] Johnson J. T. (2019), Cybersecurity maturity model lays out four readiness levels, (online). Available at: https://searchsecurity.techtarget.com/tip/Cybersecurity-maturity-model-lays-out-four-readiness-levels (Accessed: September 19, 2019)

DOI: 10.31695/IJASRE.2020.33695