Available online at https://asric.africa/natural-sciences
ASRIC Journal on Natural Sciences Vol 3(1) (2023) 18-34

Cybersecurity Resilience Maturity Assessment Tool for Critical National Information Infrastructure

Victor Emmanuel Kulugh[1*], Uche M. Mbanaso[2] and Gloria Chukwudebe[3]

[1,2]Centre for Cyberspace Studies, Nasarawa State University, Keffi, Nigeria
[3]School of Information and Communication Technology, Federal University of Technology, Owerri, Nigeria

*Corresponding author: Kulughvictore@nsuk.edu.ng

Abstract

Cybersecurity resilience maturity assessment of critical national information infrastructure (CNII) is an important process in ensuring that organisations' capability for resilience are measured and gaps determined vis-à-vis targeted resilience for the purpose of improvements. However, existing solutions do not provide an automated quantitative tool to enable organisation conduct the assessment of their cybersecurity resilience posture at defined regular intervals. This paper presents the cybersecurity resilience maturity assessment tool (CRMAT). The CRMAT is built on the cybersecurity resilience maturity assessment framework and the cybersecurity resilience maturity assessment model (CRMAM). While the CRMAF and CRMAM provide requirements and computational algorithms for the tool respectively. The agile methodology of the software development life cycle (SDLC) was adopted with the MVC (model-view-controller) architectural pattern to implement the software. The software tool has two interfaces, namely; admin interface that enables the setup of the cybersecurity controls and other parameters that will form the basis for the assessment and a report generation interface for all the cybersecurity controls. CRMAT was demonstrated on 31 CNIII organisations and result showed its capability to successfully and accurately compute the CNII resilience index (CNIIRI) and the indexes of other cybersecurity controls indicated in the CRMAF. Comparative analysis of the results showed that 5 (16.13%) of the organisations are in Q4, 9 (29.03%) are in Q3 while 13 (41.94%) and 4 (12.90%) are in Q2 and Q1 respectively. The implication is that the organisations in Q4 has optimised resilience while those in Q1 have the weakest cybersecurity resilience.

Keywords: cybersecurity; maturity model; resilience; cybersecurity resilience; maturity assessment

Introduction

This paper is a software implementation of the cybersecurity resilience maturity assessment framework and model developed in [1]. Critical national information infrastructures (CNII) support nations and organisations to provide critical services and functions. As critical digital assets, their cybersecurity resilience has increasingly become important to sustain continuous operation of modern organisations and nations. The fact that CNII vulnerabilities are further expanding with increased application of existing and emerging technologies amidst a constantly evolving threat landscape [2] further enforces the need for increased assessment of their resilience for proactive actions, geared towards sustaining their resilience. Failure of critical digital assets have potentials for catastrophic outcomes as a result of cascading, escalating and common cause effects [3] that will be propagated through their interconnectedness and interdependencies created based on their networked nature [4]. The foregoing underpins the need to have a system that measures the resilience of CNII systems at regular intervals, especially that they are technology-based systems that are constantly evolving. However, attempts at providing solutions with respect to the maturity assessment of CNII assets fall short of providing tools that automate the process of assessment and maintain data that supports the tracking of progress made. Several works either defined the metrics, formulate frameworks and models and formulate maturity models but did not implement a software-based solution. Software-based solutions will potentially provide tools that organisations can use at set intervals to measure their resilience, establish gaps and improve on those gaps to have better resilience system. Data obtained from previous measurements can be used to track progress in cybersecurity resilience assessment.

Such tools can also be used by regulators to audit CNII organisations to ensure that they are resilient enough to support national security, economy and safety in the event of cyberattacks or other forms of failures. Consequently, this article presents the cybersecurity resilience maturity assessment tool (CRMAT) a software that is built on sound theoretical and methodological foundation. The CRMAT has the capability to support organisations' resilience assessments, compute various resilience indices based on defined metrics and indicators and compare organisations as well as compare the performance of indicators within the organisation. The rest of the paper presents the background and related works in section 2; section 3 features the methodology; conceptualization of CRMAT presented in section 4; while section 5 contains the software implementation of the CRMAT as section 6 presents the testing/results. Sections 7 and 8 present the evaluation of CRMAT and conclusion respectively.

2. Background and Related Works

Critical national information infrastructures support modern societies to provide vital functions and services to the population. However, they exposed to the vulnerabilities and threat landscape of their underlying information and operations technology. Thus, the compelling need for them to be resilient against cyberattacks. CNII resilience in this context refers to their capacity to resist cyberattacks, respond effectively to successful attacks without allowing system to degrade beyond tolerable levels and successfully recover to optimal service within set mean time to recovery (MTTR) [5]–[7]. To achieve resilience in terms of the afore mentioned capabilities (resistance, response and recovery), these capabilities have to be constantly measured [8], [9]. This can be achieved through the design and implementation of fit for purpose maturity models (MM). MMs provide data that potentially form the basis for organisations to appreciate the current state of the performance of their systems, identify gaps and point the path to closing these gaps for improved systems resilience [10]–[13]. There have been several research efforts geared towards providing solutions that constantly measure the cybersecurity resilience maturity of digital assets using maturity models (MM). For instance, [14], argued that the cyber-trust programme in the kingdom of Bahrain has the potentials to positively affect the cybersecurity resilience of organisation by increasing their compliance and implementation of cybersecurity controls. However, the work did not highlight any implementation of a process of measuring the maturity of cybersecurity resilience. Although, [15] discussed the measurement of the resilience of critical infrastructure that supports the smart city, the work was more concerned with addressing the physical threats to the physical elements of those CI and thus did not address the digital aspects of the CI. The work in [16] developed and organize effective resilience metrics for cyber systems using the resilience matrix framework developed in their earlier work. A matrix that recognises the interactions between each domain of an organisation (physical, information, cognitive and social) across each stage of the event management cycle (plan/prepare, absorb, recover and adopt) was generated for the purpose of managing the resilience of cyber systems. However, the work did not elaborate on how this matrix could be used to capture measurements of resilience in organisation that will lead to exposing the gaps in the resilience of cyber systems in the organisation. Consequently, no tool was developed, nor data generated to enable the testing of the proposed methodology. [17] illustrated how resilience could be assessed through the elucidation of indicators that might be useable in its assessment through the bridging of the gap between the theoretical and practical foundations of resilience by attempting to remove the definitional ambiguity of the concept of resilience. While the article defined a number of new resilience enhancing indicators, the authors failed to establish a relationship among these indicators that will lead to the development of a model for the assessment of resilience. [7] proposed a methodology for assessments of resilience of systems from assets/facility level, organisation and community or regional levels was proposed. However, the authors presented a basic framework for measuring resilience at the infrastructure level with a single survey. Although CI (inter)dependencies were discussed in the article, the debates did not link these dependencies and interdependencies to the underlying cyber infrastructure that are responsible for the quantum and sophistication of the interconnections leading to interdependencies with potentials for cascading and escalating failures.Consequently, the article failed to address resilience assessment at the cyber layer which constitutes the epicentre of cyber risk in today's infrastructure and also form the core of this article.

In [18] the authors focused on identifying the key components of, and formulating the structure of a cybersecurity resilience maturity measurement framework for critical information infrastructure. The article identified pillars of measurement of cybersecurity resilience and combined them to formulate the resilience framework that led to the development of a mathematical model. Four cybersecurity resilience quadrants (CRQs) were proposed with a defined range of values for each quadrant to support the comparative viewing and ranking of the resilience of measured entities. Although, the authors emphasised the need for a software tool that will support the regular assessment of the cybersecurity resilience of CNI, the proposed methodology did not lead to a software tool. Thus, the framework was not tested with empirical data to evaluate its performance. The authors [19][20]emphasised the importance of resilience assessment in the security and reliability of critical infrastructure. They argued that it provides the basis for understanding the current level of CI Resilience (CIR) and planning to improve it to target levels. [21] further reinforced this argument by developing methods for evaluating the resilience of individual or isolated elements of critical infrastructure. This methodology was tested on the control room of an electricity distribution company. The results showed potentials for the computation of the resilience of the control room. However, the fact that this methodology was designed to assess the resilience of separate elements of a CI in isolation does not account for the networked nature of critical infrastructure systems nor the organisation or national level assessment. Thus, the isolated analysis in this model does not provide for comparative ranking of the elements within the organisation. Similarly, the methodology cannot be applied for cybersecurity resilience maturity assessment at sectoral or national levels. Debates in literature support the fact that CNII resilience requires current and historical data to thrive, such data will support risk analysis by tracking improvements or decline in resilience of nations or organisations' key digital assets [22]–[24]. However, [23] examine 183 articles published on the subject for a period of 10 years (2010 – 2020), the conclusion is that, there are currently no databases available for the explicit purpose of supporting risk analysis of CNII in nations. The foregoing points to the fact that existing cybersecurity resilience assessment methodologies did not achieve the development of a software tool that could be used by individual organisations, CNII owners or regulators to gauge the cybersecurity resilience maturity of CNII at designated intervals. The absence of such tools also affirms the fact that there is no existing data set for analyses that will expose patterns in the resilience maturity of CNII. Thus, this article addresses this gap by presenting the cybersecurity resilience maturity assessment tool (CRMAT), a tool that is built on the basis of defined cybersecurity metrics for the purpose of regularly gauging the cybersecurity resilience maturity of CNII.

3. Methodology

Figure 1 describes the process for the conceptualisation and development of the cybersecurity resilience maturity assessment tool (CRMAT). Processes A, B and C have been completed in an earlier work in [1]. Where the building blocks of the cybersecurity resilience maturity assessment framework (CRMAF) were identified and used to develop the framework. CRMAF formed the basis for the development of the cybersecurity resilience assessment model (CRMAM). These phases laid the foundation the data structures and algorithms for the development of the software tool referred to as the cybersecurity resilience maturity assessment tool (CRMAT), presented in this article.

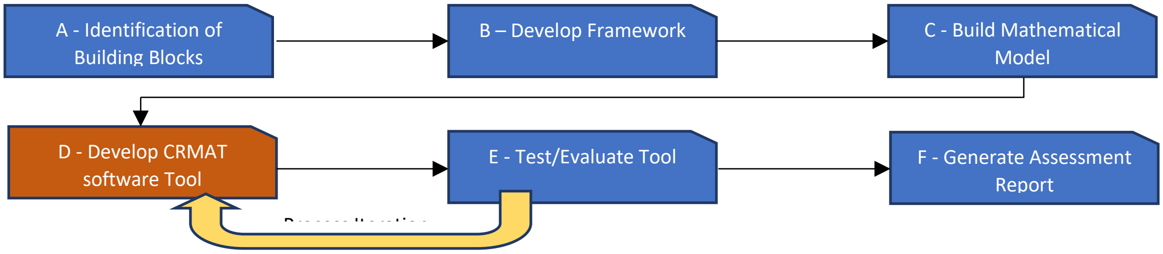

A - Identification of Building Blocks
B – Develop Framework
C - Build Mathematical Model
D - Develop CRMAT software Tool
E - Test/Evaluate Tool
F - Generate Assessment Report
Process Iteration

Figure 1: CRMAT Development Process

The development of CRMAT software tool (process – D) followed the agile methodology of the software development life cycle (SDLC). This is to support continuous iteration and refinement of the tool as indicated in the process iteration between processes D and E. The MVC (Model – View – Controller) architectural pattern was adopted to support separation of concerns between the different elements of CRMAT. The detailed process of the development methodology is explained in section 5.

4. Conceptualisation of the Cybersecurity Resilience Maturity Assessment Framework

Figure 2 adopted from [1] shows the Cybersecurity Resilience Maturity Assessment Framework (CRMAF) core for Critical National Information Infrastructure (CNII). The framework derived from the national cyberspace operational structure described in [25], which describes three layers of national cyber operations, namely: government, organisation and the individual. In context, The CRMAF is designed for organisational cybersecurity resilience measurement. Nevertheless, the organisational cybersecurity resilience for key CNIIs can be aggregated and normalised to provide insights for national cybersecurity resilience. The CRMAF as illustrated in Figure 2 consists of three major components: the cybersecurity controls, cybersecurity resilience mathematical model (a computational algorithm) and the CNII resilience quadrant (CNIIRQ)

Cybersecurity controls: these are a set of functions and sub-functions that provide the basis for the measurement of the degree of maturity – that is, the cybersecurity resilience maturity of CNII. In the CRMAF, cybersecurity controls are broken down into five distinct but connected layers; namely resilience temporal dimensions (RTD) based on [5], [7], [26] which define resilience in terms of a system's ability to prevent an incident from occurring (pre-event); minimise the impact and duration of attack (event-management); and recover to optimal service after an attack (post-event). The other layers with each of the layer providing inputs to the layer immediately adjoining it from left to right. The theoretical concepts and cybersecurity frameworks described in this article were adopted to conceptualise the building blocks of the framework core. The components are described in details in the following sections.

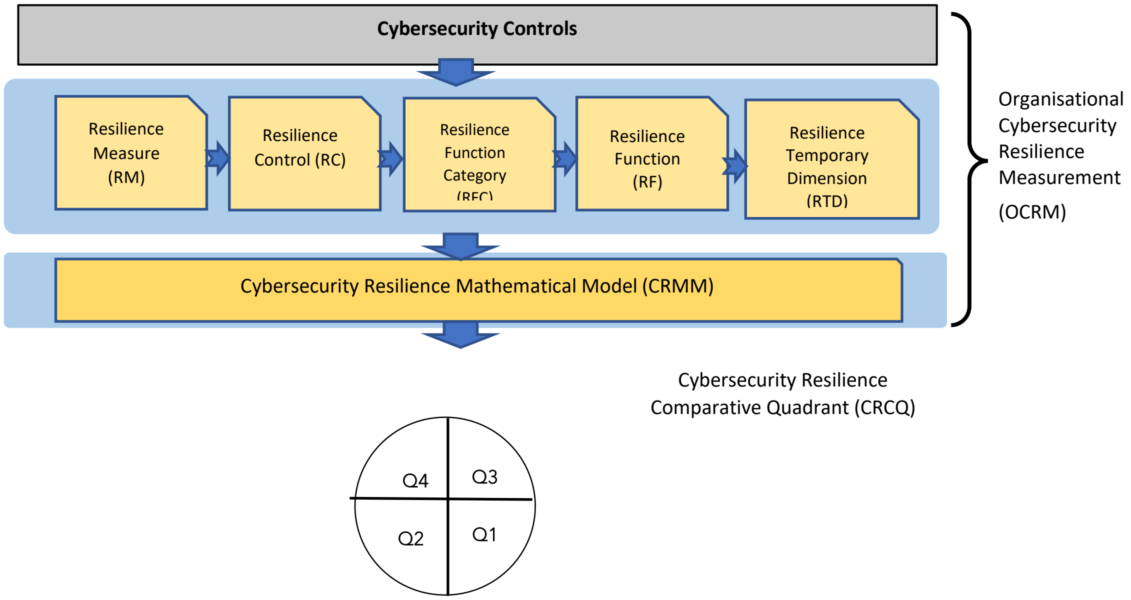

Cybersecurity Controls
Resilience Measure (RM)
Resilience Control (RC)
Resilience Function Category (RFC)
Resilience Function (RF)
Resilience Temporary Dimension (RTD)
Cybersecurity Resilience Mathematical Model (CRMM)
Organisational Cybersecurity Resilience Measurement
(OCRM)
Cybersecurity Resilience Comparative Quadrant (CRCQ)
Q4
Q3
Q2
Q1

Figure 2:Cybersecurity Resilience Maturity Assessment Framework (CRMAF)
Redrawn from [1]

The RTDs are linked to the resilience functions (RFs), the resilience functions supply inputs into the RTDs. There are five RFs derived from the five pillars of the NIST cybersecurity framework [27] (i.e. identify, protect, detect, respond and recover) and mapped into the three resilience RTDs. Consequently, pre-event RTD has identify, detect and protect; respond and recover RFs are mapped onto the event-management and post-event RTDs respectively. Other cybersecurity controls are resilience functions category (RFCs) and the resilience controls (RCs), each providing inputs into their adjoining layers of the cybersecurity controls. Thus, RFCs are mapped into the relevant RFs and RCs are mapped into relevant RFCs,

Resilience Measure (RM) illustrated as the first of the cybersecurity controls on the CRMAF from the left in Figure 2 is the granular unit of measure of the actual cybersecurity practices against baseline cybersecurity controls described in the framework. Its quantitative weights are defined on a 5-level ratio scale between 0 – 4 and provides equal intervals between adjoining levels of the RM. This is appropriate as the ratio scale starts from zero (0) and advances to higher weights [28]; zero represents the absence of control, which is vital for the quantification of measurement. The weights of the resilience measure are described in Table 1.

Table 1: Cybersecurity Resilience Measure Scale adopted from [1]

Weight	Qualitative	Description
0	Not achieved	Complete absence of cybersecurity controls in place.
1	Loosely achieved	Negligible cybersecurity controls are in place and incoherently applied.
2	Partially achieved	Moderate cybersecurity controls are in place but not consistently and structurally organised; many and/or important elements are missing.
3	Largely achieved	Cybersecurity controls are structurally implemented but some elements are missing.
4	Fully achieved	Best practices in cybersecurity practices and controls are comprehensively implemented.

Based on the scale presented in Table 1, CNII organisations that apply the highest weight (4) in the assessment of their cybersecurity practices will be more resilient compared to those that apply 1, 2 or 3. Those that have zero (0) compliance, equally have zero (0) resilience. The RM is built into the CRMAT to enable the quantification of resilience during assessment.

Cybersecurity Resilience Mathematical Model (CRMM)

The CRMM derived from the cybersecurity controls presented in Figure 2 and described in the preceding section provides the algorithmic functions for the computational engine of the CRMAT that underpin the quantitative assessment of the cybersecurity resilience maturity of a CNII. the CRMM is presented in equation. The complete derivation of the CRMM is presented in [1].

$CNIIRI = 0.55(PRTDI_N) + 0.30(EMRTDI) + 0.15(PoRTDI)$ ………………………...Equation (1)

Thus, *CIINRI*, which lies between 0.00 – 1.00 represents the composite *CNIIRI* value of a CNII organisation.

Cybersecurity Resilience Comparative Quadrant (CRCQ)

The CRCQ also referred to here as the CNII resilience quadrant (CNIIRQ) intuitively analyse and compare the Cybersecurity Resilience Maturity of organisations. CNII resilience index (CNIIRI) scores are grouped into a four-band scale called the cybersecurity resilience comparative quadrant (CRCQ). The CRCQ provides a mechanism for a single view of the CNIIRI of several CNII organisations for ranking and visualisation of the degree of resilience maturity of CNII organisation[29]. This comparative tool is also helpful in comparing the performance of the control metrics at different levels as a way of determining the effects of contributing elements relative to one another. For instance, the scores of the individual elements of the RTD (i.e., pre-event, during event and post-event) can be compared to determine their contributing effects in quantifying the Cybersecurity Resilience Maturity of a CNII organisation. Table 2 provides the scale range defined for the four quadrants, labelled Q1, Q2, Q3 and Q4 respectively. The table also provides a detailed interpretation of each quadrant.

Table 2: CNII Cybersecurity Resilience Comparative Quadrant (CNIICRCQ) [29].

Quadrant	Composite Value	Note
Q1	0.00 – 0.25	**Initial**: very low level of resilience resulting from a few resilience controls in place that are incoherently adopted.
Q2	0.26 – 0.51	**Defined**: This demonstrates a low level of resilience as a result of the inconsistent and unstructured application of resilience controls with many and/or important elements of resilience controls missing.
Q3	0.51 – 0.75	**Managed**: High resilience occasioned by a structured but inconsistent implementation of resilience controls with a few and/or minor elements missing.
Q4	0.76 – 1.00	**Optimised**: Optimal resilience achieved based on best practices and application of cybersecurity controls are comprehensively implemented.

5. Implementation of the (CRMAT)

The MVC architectural pattern was used for the implementation of the CRMAT– MVC separates an application into three major parts, namely; Model, View and controller. This architectural pattern supports separation of concerns that improves security and a modularised code-base that is easier to maintain. The model (M) represents the database, view (V) is the front end where users (administrator and organisations – respondents) interface with the application while the controller serves as the coordinating frame between the view and the model. The model (database), view (front end) and the controller (backend) were implemented using *MySQL*, React js and Laravel (PHP) respectively. This is detailed in the following section.

Data Model Domain

Figure 3 describes the entity relationship diagram (ERD) that represents the database structure upon which the CRMAT application is built. Two user roles are defined in the CRMAT database in the *crmatusers* entity in Figure 3, namely: administrator (*is_admin*) and respondent (which is represented as organisation: *org_id*) using the tool to assess their cybersecurity resilience. The role of the administrator spans the entire database entities. It is prominent in setting up all the values against the variables set in the entities. For instance, the administrator performs the following operations in the database entities: setup the quadrants and their ranges in *crmatquadrant* entity, add sectors in *crmatsectors*, organisations in *crmatorganisations*, resilience measures in *crmatresilience_measures*, resilience measure scales in *crmatresilient_measure_scales*, resilience temporal dimensions (RTD) in *crmatresilience_temporal_dimensions*, resilience controls in *crmatresilience_control*, etc. In the respondent/organisation role; the *crmatorganisation* entity is the central table that ties together most of the other entities in the model. It is connected to other entities through an associative entity called *crmatusers*. Note that the user table contains the two user roles as earlier explained in the preceding paragraph. The actions of the respondents (*crmatusers*) in performing the assessments generates the numerical data that is stored in the *resilience_measure_responses* entity. The values in this entity are used for the computation of other entities like: *crmatresilience_controls*, *crmatresilience_functions_categories*, *crmatresilience_functions*, *crmatcniir_indices*, and *crmatresilience_temporal_dimensions*

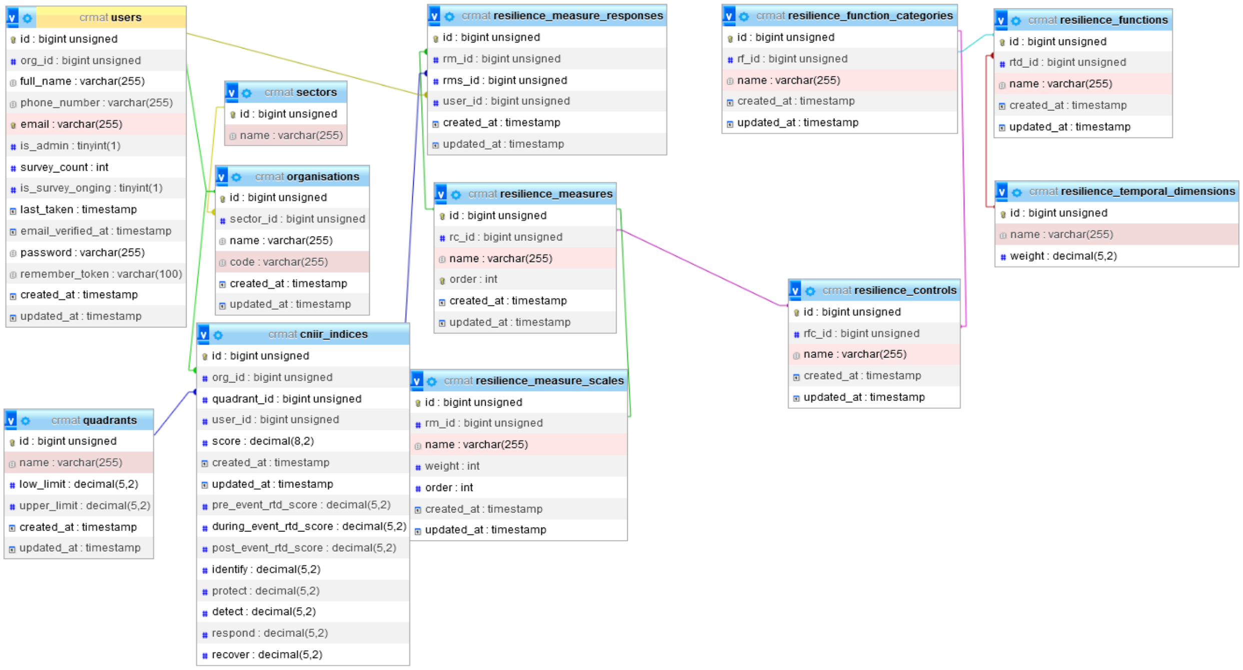


Figure 3: CRMAT Entity Relationship Diagram (ERD)

View Domain

The view domain describes the interfaces for interaction with the CRMAT application. Like the model domain, the two user roles are reflected in the view domain. For example, the administrator's interface supports administrative operations on the CRMAT at the backend while the organisation (respondents) interface enables organisations carryout cybersecurity resilience maturity assessment of their organisations and view summarised results of the assessments. Figure 5 describes the CRMAT domain view.

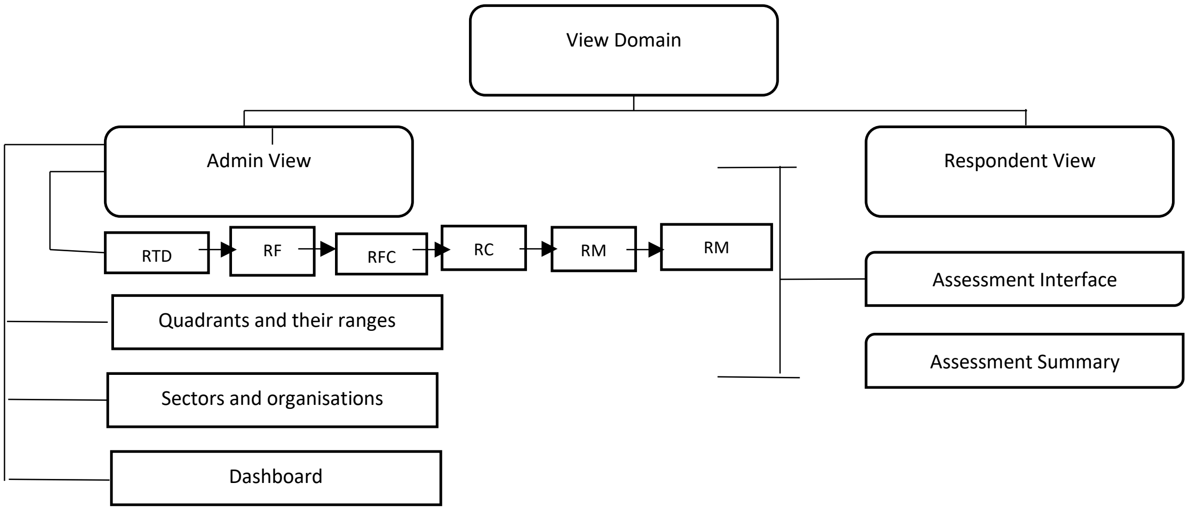


Figure 4: Description of Domain View

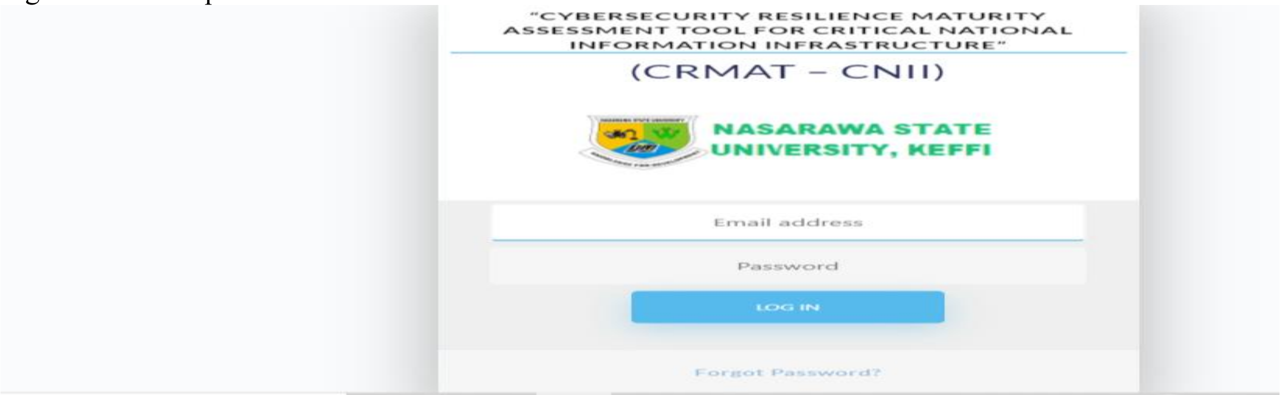
Figure 4 is the view domain design that shows the operations that can be done at the two interfaces of the view domain, namely admin view and the respondent view. At the admin view, the administrator setups the values of the resilience temporal dimensions (RTD), resilience functions (RF), resilience function categories (RFC), resilience controls (RC), resilience measure (RM) and the resilience measure scales (RMS). In addition, admin can setup CNIIRQ and their ranges (quadrants and ranges), add sectors and organisations. The dashboard at the administrator's view also provides comparative information on the performance of the assessed organisations and between other elements like the RTDs, RFs, RFCs, etc. The respondent view on the other hand provides for organisations through their respondents to access the assessment interface and carry out their cybersecurity resilience maturity assessment and view the summary of the assessment as computed and presented from the system.

Control Domain

The control domain provides the business logic of the CRMAT that enables the computation of the various metrics and indicators ranging from the CNII resilience index (CNIIRI), resilience temporal dimensions (RTDs), resilience functions (RFs), resilience functions categories (RFCs) and resilience controls (RCs). The comparative logic illustrated in the CRCQ is powered in the control domain. The details of this logic are presented in the sub-section on Cybersecurity Resilience Mathematical Model (CRMM).

6. Test and Results

Figures 5 – 11 describe some key administrator's interfaces while Figures 12 – 14 describe organisations (respondents) interfaces. The CRMAT is coded to accommodate changes in requirements of system without necessarily re-programming the tool. This is taking into account the fact that requirements may change in the future. For example, the CRMAT currently has three temporal dimensions (RTDs), if and when the RTD increases or reduces, the administrator will only be required to add, delete or modify the RTD as the case may be. Consequently, the administrator's log-in page presented in Figure 6 authenticates access to the interface of the CRMAT that enables the administrator to configure the software tool based on organisations' requirements.



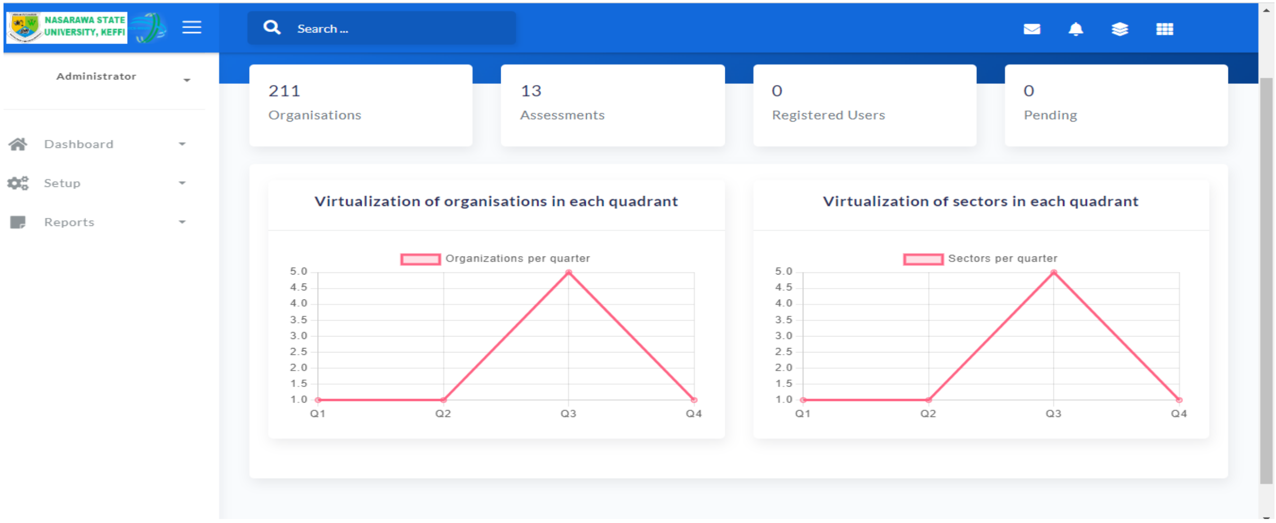
"CYBERSECURITY RESILIENCE MATURITY ASSESSMENT TOOL FOR CRITICAL NATIONAL INFORMATION INFRASTRUCTURE"

(CRMAT – CNII)

NASARAWA STATE UNIVERSITY, KEFFI

Figure 5: CRMAT Log in Page for Administrator Operations

Figure 6 presents the CRMAT dashboard where some key sets of information contained in the application's database are summarised for administrator's consumption.



211 Organisations

13 Assessments

0 Registered Users

0 Pending

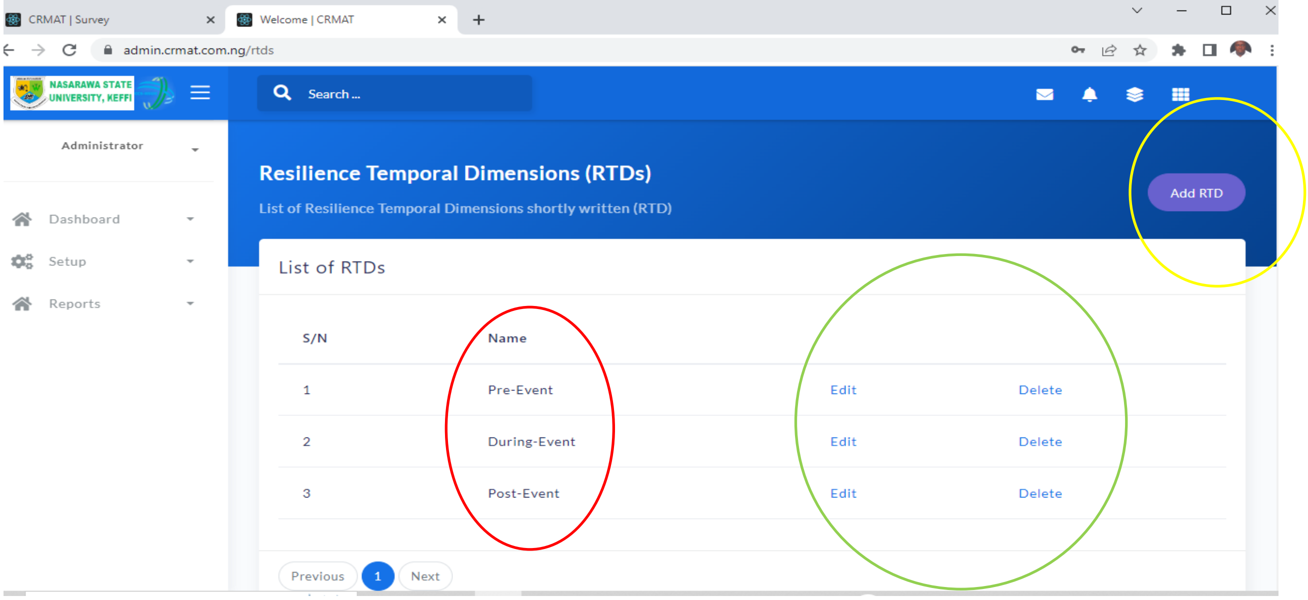
Virtualization of organisations in each quadrant

Virtualization of sectors in each quadrant

Figure 6: CRMAT Admin Dashboard

As can be seen in Figure 6, a summary of information on the number of organisations that can access the tool and carryout assessments, number of assessments already conducted, number of registered users. For example, the dashboard presented in Figure 6 shows that 211 organisations and 13 assessments currently exist in the database while there are zero users and pending assessments respectively. Figure 6 also provides a visualisation of how organisations place in the different quadrants of the CRMAM, that is, the number of organisations in Q1, Q2, Q3 or Q4 as well as how the measured metrics compare against each other. The left-hand pane of the dashboard contains the setup menu for all the cybersecurity controls defined in the in the framework in Figure 2.

Figure 7 presents the interface that enables the administrator to add, delete or edit resilience temporal dimensions (RTD) by clicking on the ***Add RTD*** (circled in yellow)***, delete or edit*** (circled in green) buttons. Note the three RTDs namely; pre-event, during-event (event management) and post-event have been added as circled in red.



Resilience Temporal Dimensions (RTDs)

List of Resilience Temporal Dimensions shortly written (RTD)

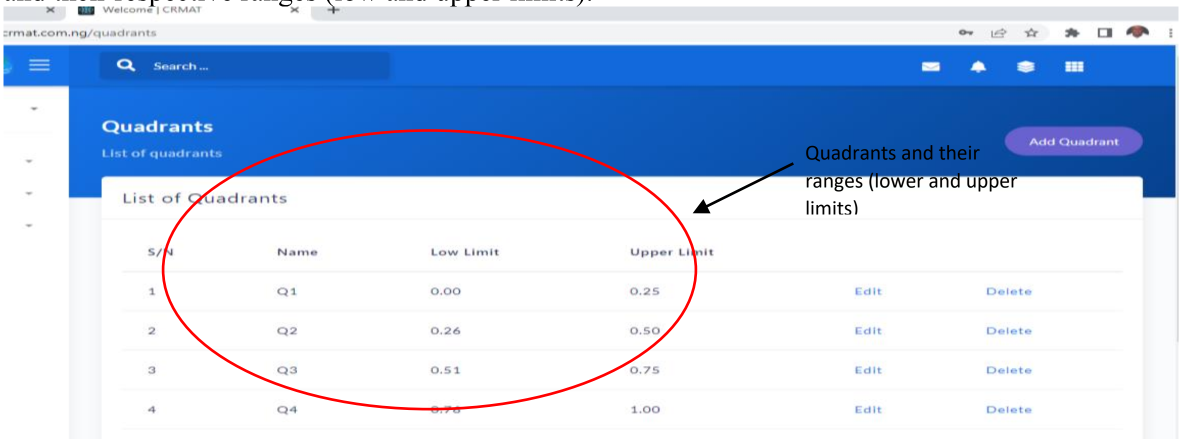
List of RTDs

S/N	Name		
1	Pre-Event	Edit	Delete
2	During-Event	Edit	Delete
3	Post-Event	Edit	Delete

Figure 7: Add Resilience Temporal Dimensions (RTD)

Clicking on the *Add RTD* button opens up a dialog box that enables the admin to add more RTDs to the tool. Note that the delete/edit buttons allow for the deletion or edit of an already added RTD. Similar interfaces exist in the application to enable one add several elements of the.

Figure 8 is the interface that allows the administrator to add, delete or edit the quadrants defined in Table 2 and their respective ranges (low and upper limits).



Quadrants

List of quadrants

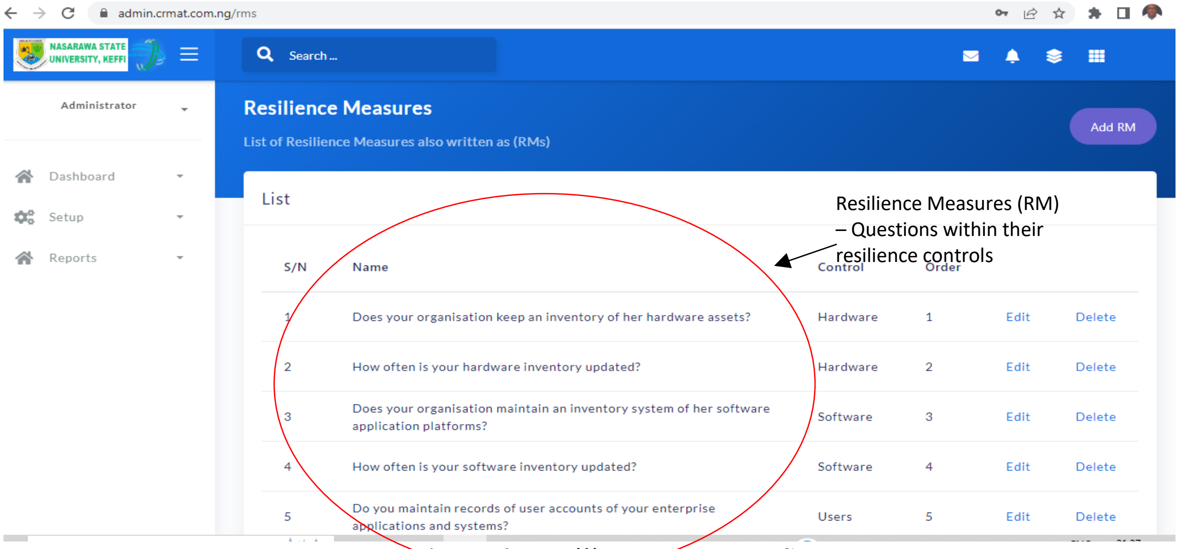
Quadrants and their ranges (lower and upper limits)

List of Quadrants

S/N	Name	Low Limit	Upper Limit		
1	Q1	0.00	0.25	Edit	Delete
2	Q2	0.26	0.50	Edit	Delete
3	Q3	0.51	0.75	Edit	Delete
4	Q4	0.76	1.00	Edit	Delete

Figure 8: CNII Resilience Quadrants (CNIIRQ) Setup

These quadrants, labelled as Q1 – Q4 were exhaustively described in Table 2. The quadrants are the basis for ranking of the cybersecurity resilience index described as the CNIIRI and other metrics like the resilience function (RF), resilience function category (RFC) and resilience controls. Figure 9 is the resilience measure (RM) interface. The RMs are the questions that guide the process of the cybersecurity resilience maturity assessment. This interface enables the additions of RMs according to their resilience controls (RC).

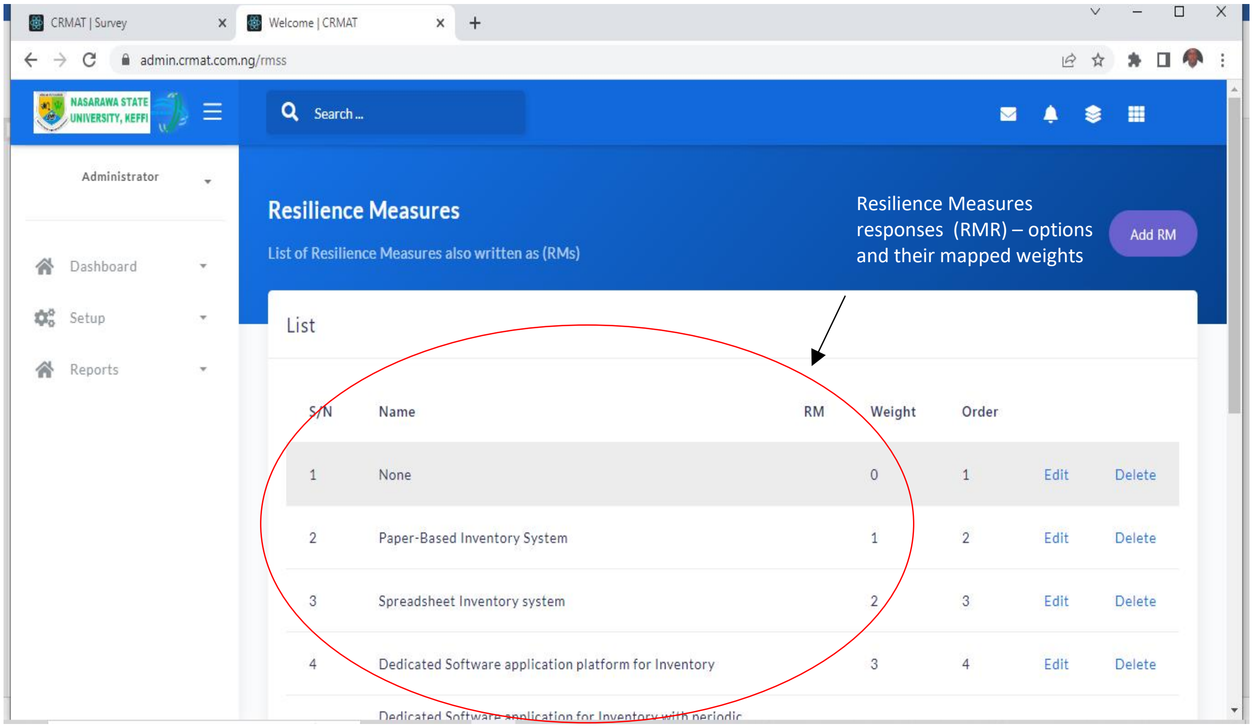


Resilience Measures (RM) – Questions within their resilience controls

S/N	Name	Control	Order		
1	Does your organisation keep an inventory of her hardware assets?	Hardware	1	Edit	Delete
2	How often is your hardware inventory updated?	Hardware	2	Edit	Delete
3	Does your organisation maintain an inventory system of her software application platforms?	Software	3	Edit	Delete
4	How often is your software inventory updated?	Software	4	Edit	Delete
5	Do you maintain records of user accounts of your enterprise applications and systems?	Users	5	Edit	Delete

Figure 9: Resilience Measures Setup

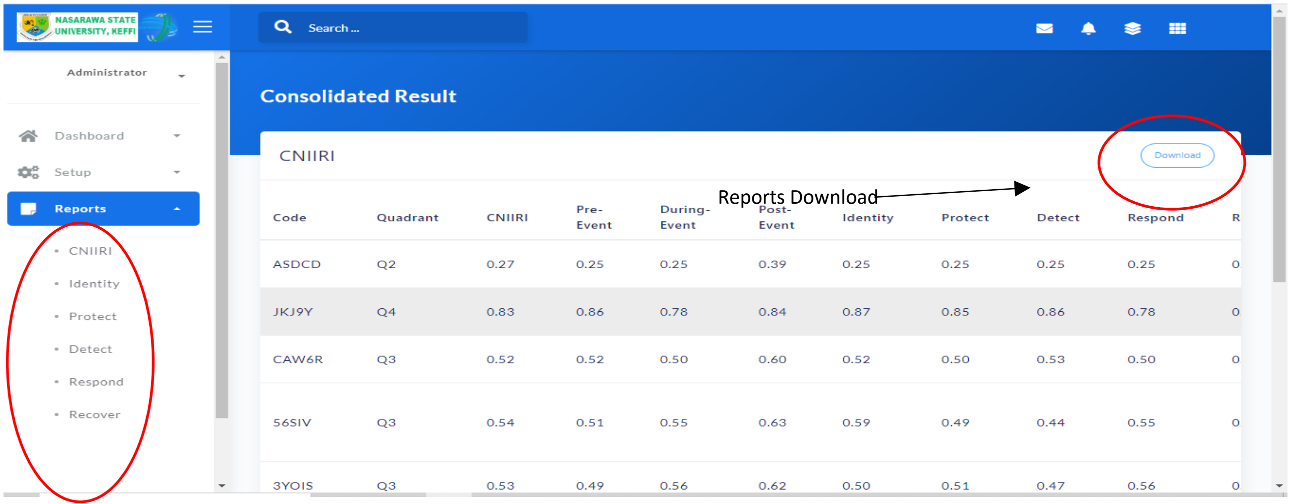
Figure 10 shows the resilience measure responses (RMR) which provides the interface to add the possible options to each RM. There are five possible options (RMRs) to each RM, each of these options are mapped to their corresponding numerical weights between (0-4) which Figure 10 provides the capability for tying each option to its corresponding weight relative to its RM.



Resilience Measures responses (RMR) – options and their mapped weights

S/N	Name	RM	Weight	Order		
1	None		0	1	Edit	Delete
2	Paper-Based Inventory System		1	2	Edit	Delete
3	Spreadsheet Inventory system		2	3	Edit	Delete
4	Dedicated Software application platform for Inventory		3	4	Edit	Delete
	Dedicated Software application for Inventory with periodic					

Figure 10: Resilience Measure Responses (RMR) Setup



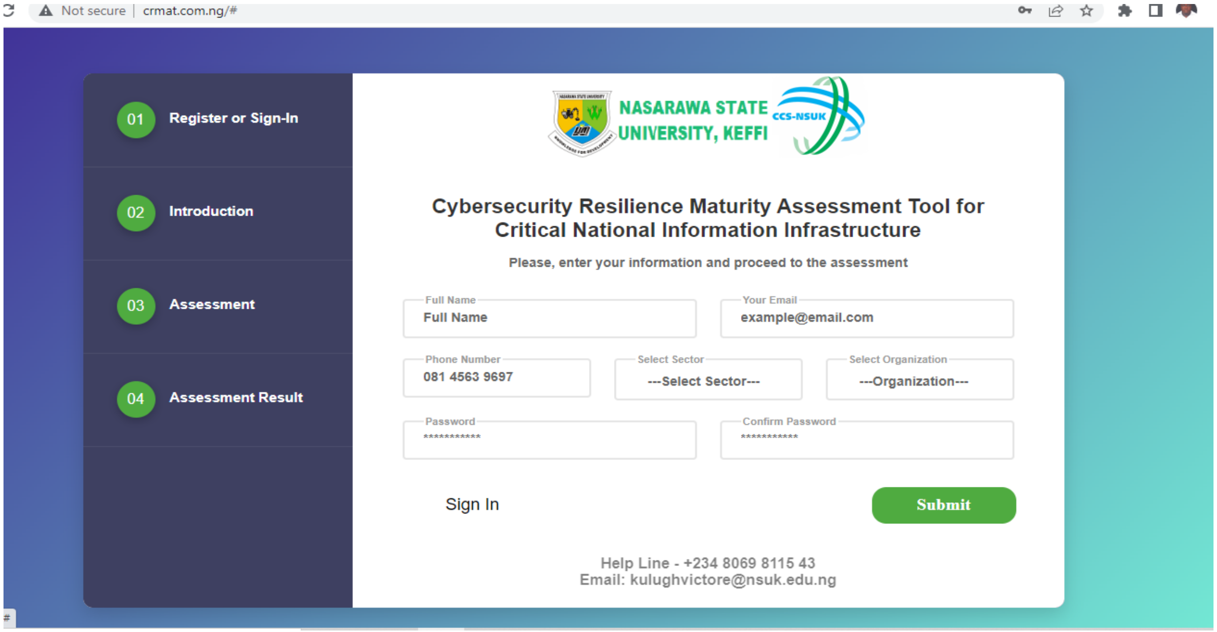
Consolidated Result

CNIIRI

Code	Quadrant	CNIIRI	Pre-Event	During-Event	Post-Event	Identity	Protect	Detect	Respond	R
ASDCD	Q2	0.27	0.25	0.25	0.39	0.25	0.25	0.25	0.25	0
JKJ9Y	Q4	0.83	0.86	0.78	0.84	0.87	0.85	0.86	0.78	0
CAW6R	Q3	0.52	0.52	0.50	0.60	0.52	0.50	0.53	0.50	0
56SIV	Q3	0.54	0.51	0.55	0.63	0.59	0.49	0.44	0.55	0
3YOIS	Q3	0.53	0.49	0.56	0.62	0.50	0.51	0.47	0.56	0

Figure 11: Reports

Figure 11 is the sample CNIIRI report from the CRMAT, similar reports can be generated for the identify, protect, detect, respond and recover RFs as well as for the RFCs. The reports menu contains a download feature that enables users to export data from the CRMAT into other statistical tools for further analysis and visualisations.



Cybersecurity Resilience Maturity Assessment Tool for Critical National Information Infrastructure

Please, enter your information and proceed to the assessment

Full Name: Full Name

Your Email: example@email.com

Phone Number: 081 4563 9697

Select Sector: ---Select Sector---

Select Organization: ---Organization---

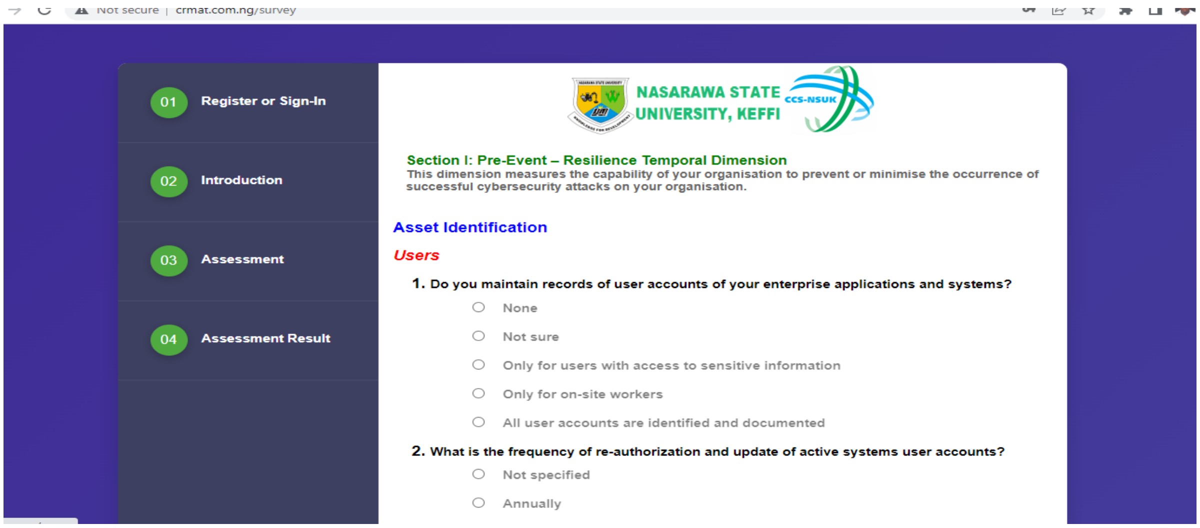
Password: ***********

Confirm Password: ***********

Help Line - +234 8069 8115 43
Email: kulughvictore@nsuk.edu.ng

Figure 12: Organisation (Respondent) Login Page

Figure 12 presents the log-in page for organisations that use the tool for assessment. It requires users to provide their names, phone number, email, password, sector and organisations for registration. Figure 13 on the other hand shows the assessment interface where items are provided with options to be selected using radio buttons, each item selected here has it mapped quantitative value recorded in the database for computation of the various indices defined in the model. In Figure 14, the assessment summary is provided for organisations that use the CRMAT to conduct their resilience assessment. It provides the CNIIRI score of the organisation and the corresponding quadrant upon which they fall. This summary also present reports on the RTD scores namely; pre-event, event management and post-event scores.



Section I: Pre-Event – Resilience Temporal Dimension

This dimension measures the capability of your organisation to prevent or minimise the occurrence of successful cybersecurity attacks on your organisation.

Asset Identification

Users

1. Do you maintain records of user accounts of your enterprise applications and systems?

○ None

○ Not sure

○ Only for users with access to sensitive information

○ Only for on-site workers

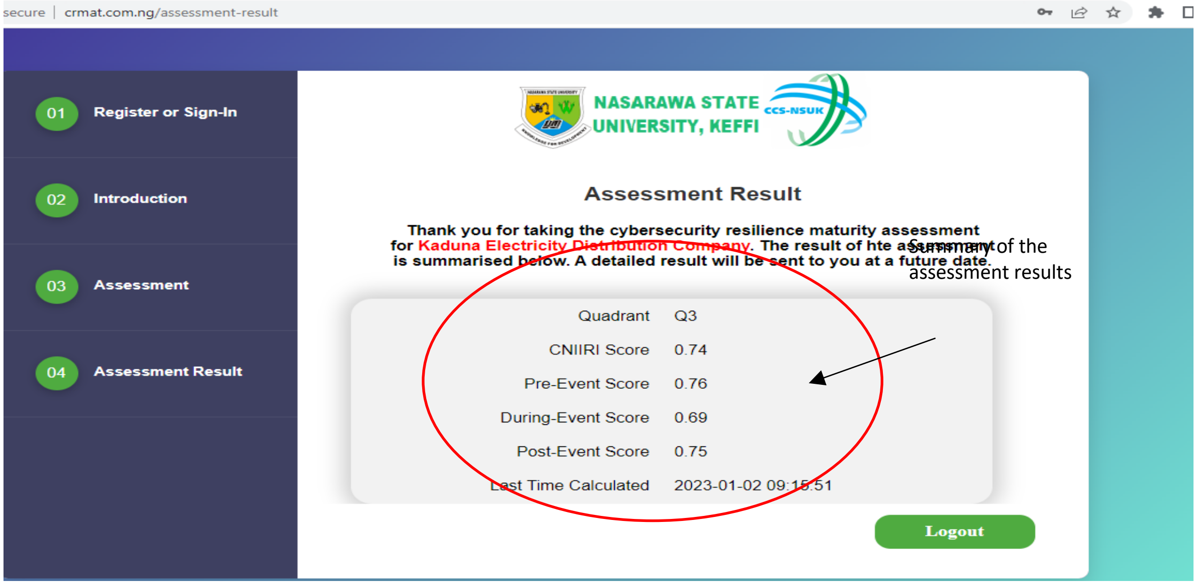
○ All user accounts are identified and documented

2. What is the frequency of re-authorization and update of active systems user accounts?

○ Not specified

○ Annually

Figure 13: Sample Assessment Interface


secure | crmat.com.ng/assessment-result
01 Register or Sign-In
02 Introduction
03 Assessment
04 Assessment Result
NASARAWA STATE UNIVERSITY, KEFFI
CCS-NSUK
Summary of the assessment results
Logout

Assessment Result

Thank you for taking the cybersecurity resilience maturity assessment for Kaduna Electricity Distribution Company. The result of hte assessment is summarised below. A detailed result will be sent to you at a future date.

Quadrant	Q3
CNIIRI Score	0.74
Pre-Event Score	0.76
During-Event Score	0.69
Post-Event Score	0.75
Last Time Calculated	2023-01-02 09:15:51

Figure 14: Sample Assessment Summary

7. Evaluation of CRMAT

The CRMAT was deployed to collect data from 31 CNII organisations representing 10 CNII sectors to carry out the two-fold exercises of evaluating the CRMAT and performing cybersecurity resilience assessment of the organisations based on data generated and computation carried out by CRMAT's computational engine. The names of the organisations and sectors were anonymised to address the inherent conflict between information sharing and security [23]. The evaluation took into account all three (3) Resilience Temporal Dimensions (RTDs); all five (5) Resilience Functions (RFs). Similarly, all five (5) resilience function categories (RFCs) in the identify, protect and respond RFs; and all three (3) RFCs in the detect and recover RFs respectively. Note that each RFC has several RCs and RCs have RMs (the numerical values at the granular levels that are mapped to actual cybersecurity practices at the organisational context). Data collected was based on organisations within the CNII sectors as defined in the Nigerian national cyber security strategy and policy (NCSSP) [30] document as presented in Table 3. It (Table 3) contains a summary of sectors, number of organisations per sector and number of respondents per organisation. To reduce the effect of the biases that will be introduced into the data by respondents, the CRMAT is designed with the capability to aggregate responses from multiple respondents per organisation, average them and report a single value for the organisation. Thus, organisations were encouraged to have a minimum of 2 respondents to participate in the assessment.

Table 3: Summary Responding CNII Sectors and Organisations

#	Sector	No. of Organisations	Respondents
1	SECT001	3	9
2	SECT002	2	5
3	SECT003	2	4
4	SECT004	6	12
5	SECT005	5	15
6	SECT006	3	6
7	SECT007	4	8
8	SECT008	2	4
9	SECT009	1	2
10	SECT010	3	6
	Total	**31**	**71**

Table 4 shows the CNIIRI scores of 31 CNII organisations and their distribution in the CNII resilience quadrant (CNIIRQ). The CNIIRI scores as distributed in the CNIIRQ show that 4(12.90%), 8(25.81%), 15(48.39%) and 4(12.90%) are in Q4, Q3, Q2 and Q1 respectively. The groupings reflect the overall resilience of these organisations with respect to the cybersecurity controls (resilience measures - RMs) applied in their computation. Consequently, it can be inferred from this distribution that organisations in Q4 are the most resilient while those in Q1 are the least resilient.

Table 5 presents the pre-event RTD index (PRTDI) of the 31 CNII organisation that participated in the assessment and their distribution in the CNIIRQ. The CNIIRQ distribution of the PRTDI shows that 5 (16.13%) of the organisations are in Q4, 9 (29.03%) are in Q3 while 13 (41.94%) and 4 (12.90%) are in Q2 and Q1 respectively.

Table 6 on the other hand represents the event management resilience temporal dimension index (EMRTDI) of the 31 CNII organisation and their distribution in the CNIIRQ. The distribution showed that 3(9.68%) of the organisations are in Q4, 9 (29.03%) are in Q3 while 13(41.94 and 6(19.35%) are in Q2 and Q1 respectively.

The post-event resilience temporal dimension index (PoRTDI) of the 31 CNII organisations are presented in Table 7. The distribution of the PoRTDI scores in the CNIIRQ shows that Q4 has 6(19.35) organisations, Q3 has 8 (25.81%), Q2 and Q1 have 13 (41.94%) and 4 (12.90%) respectively.

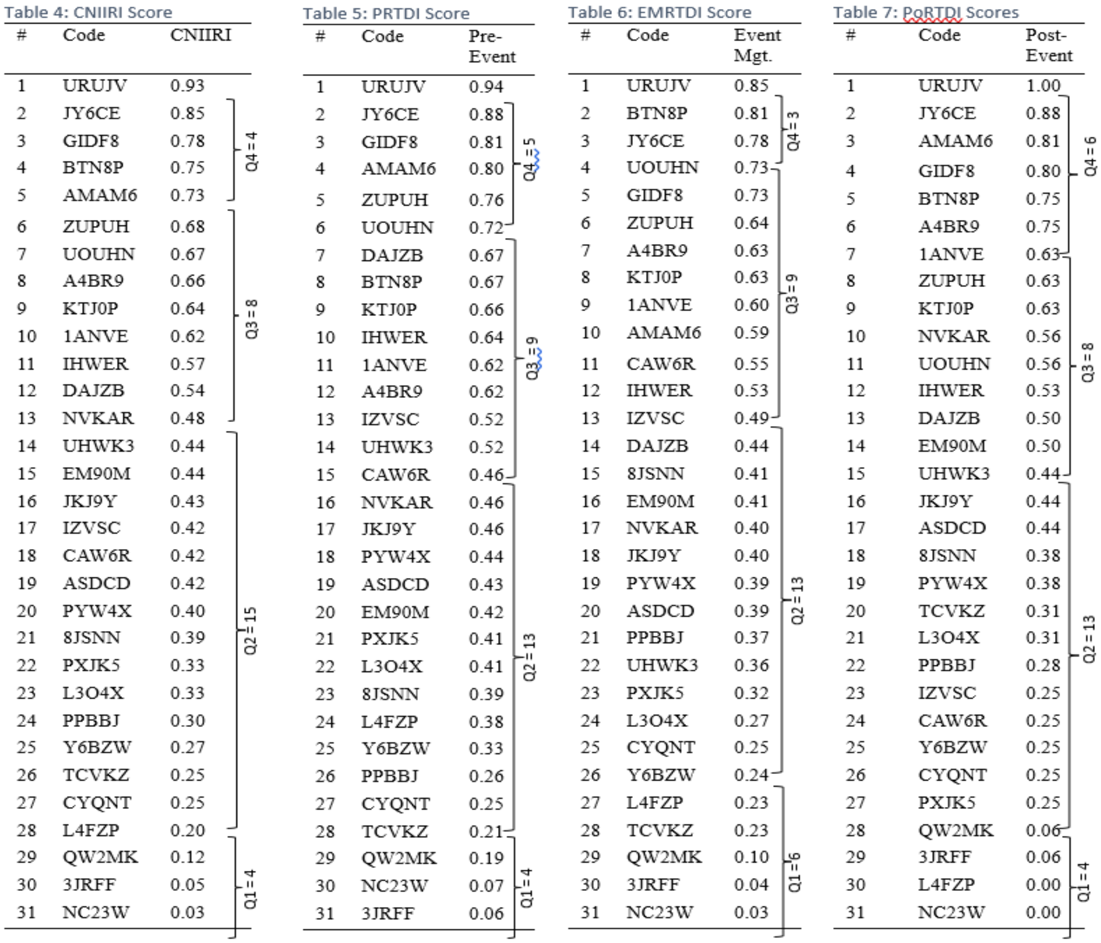


Table 4: CNIIRI Score

#	Code	CNIIRI	
1	URUJV	0.93	
2	JY6CE	0.85	Q4 = 4
3	GIDF8	0.78	
4	BTN8P	0.75	
5	AMAM6	0.73	
6	ZUPUH	0.68	Q3 = 8
7	UOUHN	0.67	
8	A4BR9	0.66	
9	KTJ0P	0.64	
10	1ANVE	0.62	
11	IHWER	0.57	
12	DAJZB	0.54	
13	NVKAR	0.48	
14	UHWK3	0.44	Q2 = 15
15	EM90M	0.44	
16	JKJ9Y	0.43	
17	IZVSC	0.42	
18	CAW6R	0.42	
19	ASDCD	0.42	
20	PYW4X	0.40	
21	8JSNN	0.39	
22	PXJK5	0.33	
23	L3O4X	0.33	
24	PPBBJ	0.30	
25	Y6BZW	0.27	
26	TCVKZ	0.25	
27	CYQNT	0.25	
28	L4FZP	0.20	
29	QW2MK	0.12	Q1 = 4
30	3JRFF	0.05	
31	NC23W	0.03	

Table 5: PRTDI Score

#	Code	Pre-Event	
1	URUJV	0.94	
2	JY6CE	0.88	Q4 = 5
3	GIDF8	0.81	
4	AMAM6	0.80	
5	ZUPUH	0.76	
6	UOUHN	0.72	
7	DAJZB	0.67	Q3 = 9
8	BTN8P	0.67	
9	KTJ0P	0.66	
10	IHWER	0.64	
11	1ANVE	0.62	
12	A4BR9	0.62	
13	IZVSC	0.52	
14	UHWK3	0.52	
15	CAW6R	0.46	
16	NVKAR	0.46	Q2 = 13
17	JKJ9Y	0.46	
18	PYW4X	0.44	
19	ASDCD	0.43	
20	EM90M	0.42	
21	PXJK5	0.41	
22	L3O4X	0.41	
23	8JSNN	0.39	
24	L4FZP	0.38	
25	Y6BZW	0.33	
26	PPBBJ	0.26	
27	CYQNT	0.25	
28	TCVKZ	0.21	
29	QW2MK	0.19	Q1 = 4
30	NC23W	0.07	
31	3JRFF	0.06	

Table 6: EMRTDI Score

#	Code	Event Mgt.	
1	URUJV	0.85	
2	BTN8P	0.81	Q4 = 3
3	JY6CE	0.78	
4	UOUHN	0.73	
5	GIDF8	0.73	Q3 = 9
6	ZUPUH	0.64	
7	A4BR9	0.63	
8	KTJ0P	0.63	
9	1ANVE	0.60	
10	AMAM6	0.59	
11	CAW6R	0.55	
12	IHWER	0.53	
13	IZVSC	0.49	
14	DAJZB	0.44	Q2 = 13
15	8JSNN	0.41	
16	EM90M	0.41	
17	NVKAR	0.40	
18	JKJ9Y	0.40	
19	PYW4X	0.39	
20	ASDCD	0.39	
21	PPBBJ	0.37	
22	UHWK3	0.36	
23	PXJK5	0.32	
24	L3O4X	0.27	
25	CYQNT	0.25	
26	Y6BZW	0.24	
27	L4FZP	0.23	Q1 = 6
28	TCVKZ	0.23	
29	QW2MK	0.10	
30	3JRFF	0.04	
31	NC23W	0.03	

Table 7: PoRTDI Scores

#	Code	Post-Event	
1	URUJV	1.00	
2	JY6CE	0.88	Q4 = 6
3	AMAM6	0.81	
4	GIDF8	0.80	
5	BTN8P	0.75	
6	A4BR9	0.75	
7	1ANVE	0.63	
8	ZUPUH	0.63	Q3 = 8
9	KTJ0P	0.63	
10	NVKAR	0.56	
11	UOUHN	0.56	
12	IHWER	0.53	
13	DAJZB	0.50	
14	EM90M	0.50	
15	UHWK3	0.44	
16	JKJ9Y	0.44	Q2 = 13
17	ASDCD	0.44	
18	8JSNN	0.38	
19	PYW4X	0.38	
20	TCVKZ	0.31	
21	L3O4X	0.31	
22	PPBBJ	0.28	
23	IZVSC	0.25	
24	CAW6R	0.25	
25	Y6BZW	0.25	
26	CYQNT	0.25	
27	PXJK5	0.25	
28	QW2MK	0.06	
29	3JRFF	0.06	Q1 = 4
30	L4FZP	0.00	
31	NC23W	0.00	

Distribution of CNIIRI and RTDs in the CNIIRQ

Table 8 summarises the distributions of the resilience parameters in the CNIIRQ as shown in Figures Tables 4-7. It shows that although, the CNIIRI is derivative of the cumulative effects of the RTDs; It values does not necessarily match the values of the RTDs upon which it is derived. For example, 4 organisations are in the Q4 quadrants based on CNIIRI. However, the RTDs presents unmatching patterns for the same quadrant, namely; PRTDI = 5, EMRTDI = 3 and PoRTDI = 6. This is similar to the distributions in other quads as shown in Table 4. The implication is that, organisations must explore further to establish the indicators that account for their high performance (and even low scores). This will expose indicators with low scores but which effects are compensated by high performing indicators, thus hiding the gaps.

Table 8: Distribution of CNIIRI and RTDs in the CNIIRQ

#	Indicator	Q4	Q3	Q2	Q1
1	CNIIRI	4	8	15	4
2	PRTDI	5	9	13	4
3	EMRTDI	3	9	13	6
4	PoRTDI	6	8	13	4

Comparison of RTDs and RFs

Figure 15 represents a comparison of the averages of the RTD computed by the CRMAT based on the 31 CNII organisation taken for the 3 RTDs (i.e., PRTDI, EMRTDI and PoRTDI). Similarly, Figure 16 is a representation of the averages of the 5 RFs (namely: identify, protect, detect, respond and recover). These Figures compare the performance of these cybersecurity resilience controls based on data generated from the CRMAT.

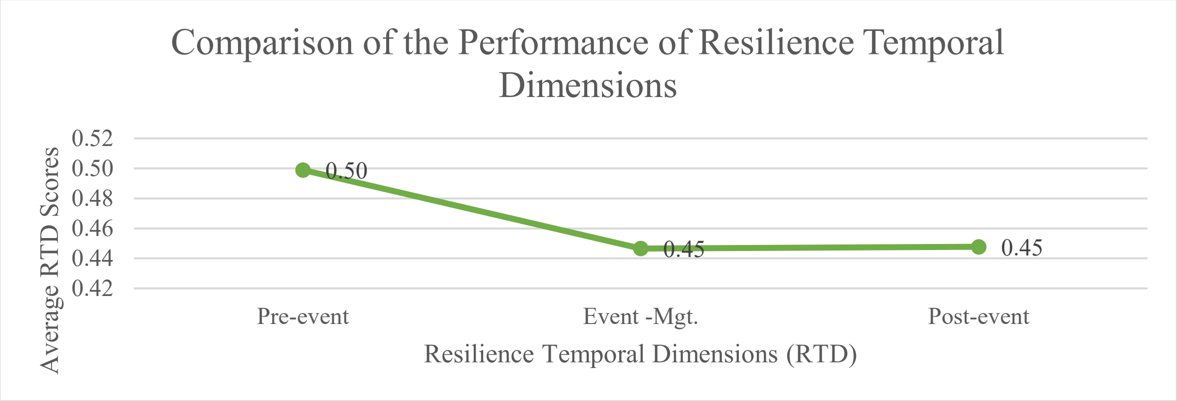


Figure 15: Comparison of the Performance of RTDs

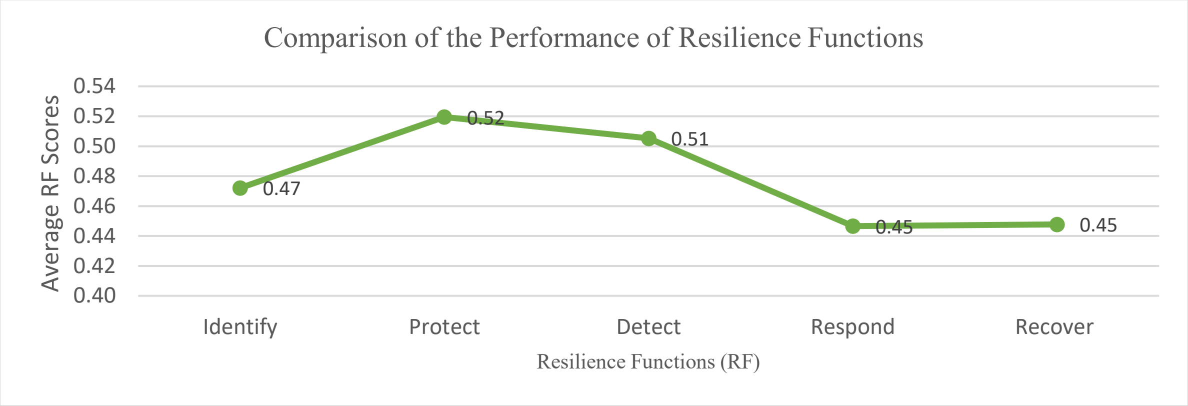


Figure 16: Comparison of the Performance of RFs

Figure 15 indicates a trend that showed higher average score on the pre-event RTD (0.50) as compared to the averages in event-management and post-event RTDs (0.45) respectively. Although, 0.50 averages place the organisations at the lowest boundary of Q3 quad, it indicates that organisations are generally more prepared to prevent cybersecurity incidents compared to their response and recovery efforts which scored average of 0.45 (i.e., a Q2 placements). Figure 16 presents a Q2 average value of 0.47 on the identify RF, indicating vulnerabilities in this phase as the resilience of unidentified assets cannot be optimised. Similarly, the protect and detect RFs are at the lowest boundary of the Q3, this combines with the identify RF generally make the pre-event RTD vulnerable. Again, the respond and recover RFs are weak at 0.45 both and depict the fact that these organisations have poor response and recovery mechanisms.

8. Conclusion

The economy, security, economic security, health and safety of citizens of modern societies will experience monumental disaster of catastrophic proportion if the CNII experience huge and sustained cyberattacks. To proactively address this concern, organisations and nations need to regularly and quantitatively gauge the maturity of their cybersecurity resilience to cyberattacks. Proposed solutions do not provide tools that simplify the process and maintain data so that organisations, CNII owners, operators and regulators can track improvements or decline in resilience of their digital assets. This paper presents the cybersecurity resilience maturity assessment tool (CRMAT) that addresses this gap. CRMAT was conceptualised from a theoretical and methodological background that provided the requirements (building blocks) that were further refined to formulate the computational algorithms. The software tool was built using the agile development process with the MVC architectural pattern. CRMAT has a built-in setup frame that allows organisation to add or drop cybersecurity controls on the admin panel as per their needs. The data generated from the software can be exported into other data analytics tools for further analyses and insights. The CRMAT system stores data of assessment with timestamp to enable organisations track their resilience performance in terms of improvements on the revealed gaps. CRMAT relies solely on data provided by organisations for its computation, this data could be subjected to biases and thus, may not provide accurate insights into the resilience maturity of assessed organisations. However, an attempt has been made to address this by ensuring that more than one respondent participates per organisation and the scores aggregated and averaged, this will potentially limit the effects of any biases that may be introduced. Additionally, the assessment programme (questionnaire) has follow-up questions that checks biases that may be introduced by respondents. The software has been tested based on input data received from 31 organisations and has shown capability to accurately compute the performances of the various cybersecurity controls defined within the framework (CRMAF – Figure 2). A comparative analysis of the results on the CNIIRQ showed that 12.90% of the 31 assessed organisation fall within Q4 which depicts an optimised level of resilience, however, nearly half of these organisations (48.39%) and 12.90% fell in Q2 and Q1 respectively. Thus, depicting a generally weak cybersecurity resilience posture of the participating organisations. A comparison of the performance of the resilience temporal dimensions showed that majority of the organisations have more pre-event capabilities as compared to their ability to respond and recover from cybersecurity incidents. Overall, it can be inferred from the assessment of the organisation that the general cybersecurity resilience posture of the organisations is weak.

Acknowledgement

Conflict of Interest This article is part of the Cybersecurity and Critical National Infrastructure (CNI) research project which is supported by TETFund National Research Fund (NRF) research grant TETF/ DR&D/CE/NRF/UNI/KEFFI/VOL.1/B5 to Nasarawa State University, Keffi, Nigeria.

References

[1] V. E. Kulugh, U. M. Mbanaso, and G. Chukwudebe, “Cybersecurity Resilience Maturity Assessment Model for Critical National Information Infrastructure,” *SN Comput Sci*, vol. 3, no. 3, May 2022, doi: 10.1007/s42979-022-01108-x.

[2] M. Panfili, A. Giuseppi, A. Fiaschetti, H. B. Al-jibreen, and A. Pietrabissa, “A Game-Theoretical Approach to Cyber-Security of Critical Infrastructures Based on Multi-Agent Reinforcement Learning,” pp. 460–465, 2018.

[3] S. M. Rinaldi, J. P. Peerenboom, and T. K. Kelly, “Identifying, understanding, and analyzing critical infrastructure interdependencies,” *IEEE Control Systems Magazine*, vol. 21, no. 6, pp. 11–25, 2001, doi: 10.1109/37.969131.

[4] B. Rød, D. Lange, M. Theocharidou, and C. Pursiainen, “From risk management to resilience management in critical infrastructure,” *Journal of Management in Engineering*, vol. 36, no. 4:04020039, 2020, doi: DOI: 10.1061/(ASCE)ME.1943-5479.0000795.

[5] M. Bruneau *et al.*, “A Framework to Quantitatively Assess and Enhance the Seismic Resilience of Communities,” *Earthquake Spectra*, vol. 19, no. 4. Earthquake Engineering Research Institute, pp. 733–752, 2003. doi: 10.1193/1.1623497.

[6] M. Bruneau and A. Reinhorn, “Overview of the Resilience Concept.”

[7] J. L. Carlson *et al.*, “Resilience: Theory and Application.,” Argonne, IL (United States), Feb. 2012. doi: 10.2172/1044521.

[8] G. Stergiopoulos, P. Kotzanikolaou, M. Theocharidou, G. Lykou, and D. Gritzalis, “Time-based critical infrastructure dependency analysis for large-scale and cross-sectoral failures,” *International Journal of Critical Infrastructure Protection*, vol. 12, pp. 46–60, Mar. 2016, doi: 10.1016/j.ijcip.2015.12.002.

[9] S. Puuska *et al.*, “Nationwide critical infrastructure monitoring using a common operating picture framework,” *International Journal of Critical Infrastructure Protection*, vol. 20, pp. 28–47, 2018, doi: 10.1016/j.ijcip.2017.11.005.

[10] G. Sharkov, “Assessing the Maturity of National Cybersecurity and Resilience,” vol. 4, no. 4, pp. 5–24, 2020.

[11] M. Levesque, “Understanding Cybersecurity Maturity Models Within the Context of Energy Regulations,” Europe and Eurasia, 2020.

[12] W. Miron and K. Muita, “Cybersecurity Capability Maturity Models for Providers of Critical Infrastructure,” *Technology Innovation Mnagement Review*, vol. 4, no. 10, pp. 33–39, 2014.

[13] T. Mettler, “Maturity assessment models : a design science research approach,” vol. 3, 2011.

[14] K. Shaheen and A. H. Zolait, “The impacts of the cyber-trust program on the cybersecurity maturity of government entities in the Kingdom of Bahrain,” *Information and Computer Security, Emerald Publishing Limited*, 2023.

[15] D. Rehak, T. Lovecek, M. Hromada, N. Walker, and I. Haring, “Critical Infrastructures Resilience in the Context of a Physical Protection System,” in *Advances in Engineering and Information Science Toward Smart City and Beyond*, R. Shinkuma, F. Xhafa, and T. Nishio, Eds., 5th ed.Springer , 2023, pp. 1–33.

[16] I. Linkov, D. A. Eisenberg, K. Plourde, T. P. Seager, J. Allen, and A. Kott, “Resilience metrics for cyber systems,” pp. 471–476, 2013, doi: 10.1007/s10669-013-9485-y.

[17] P. Tim, “Measuring Critical Infrastructure Resilience : Possible Indicators,” Zurich, 2014.

[18] U. M. Mbanaso, L. Abrahams, and O. Z. Apene, “Conceptual design of a cybersecurity resilience maturity measurement (CRMM) framework,” *The African Journal of Information and Communication*, vol. 23, no. 23, pp. 1–26, 2019, doi: 10.17159/2077-7213/2019/n23a2.

[19] D. Rehak and M. Hromada, “Failures in a Critical Infrastructure System,” in *System of System Failures*, InTech, 2018. doi: 10.5772/intechopen.70446.

[20] D. Rehak, M. Hromada, and J. Ristvej, “Indication of critical infrastructure resilience failure,” no. December, 2017.

[21] D. Rehak, P. Senovsky, M. Hromada, and T. Lovecek, “Complex approach to assessing resilience of critical infrastructure elements,” *International Journal of Critical Infrastructure Protection*, vol. 25, pp. 125–138, 2019, doi: 10.1016/j.ijcip.2019.03.003.

[22] A. Larsson and C. Groβe, “Data use and data needs in critical infrastructure risk analysis,” *J Risk Res*, 2023, doi: 10.1080/13669877.2023.2181858.

[23] C. Große, A. Larsson, and O. Björkqvist, “Information-flawing filters in critical infrastructure protection: the deficient information basis in a Swedish approach,” *International Journal of Critical Infrastructures, Inderscience Enterprises Ltd*, vol. 9, no. 1, pp. 40–57, 2023.

[24] C. Große, “Enhanced information management in inter-organisational planning for critical infrastructure protection: Case and framework,” in *ICISSP 2021 - Proceedings of the 7th International Conference on Information Systems Security and Privacy*, SciTePress, 2021, pp. 319–330. doi: 10.5220/0010186803190330.

[25] U. M. Mbanaso and R. A. Koleoso, “AN INVESTIGATION OF CYBERSECURITY VULNERABILITY LANDSCAPE,” in *International Conference on Emerging Application and Technologies for Industry 4.0*, 2020, pp. 110–123.

[26] A. Smith and A. Stirling, “Transitions Social-ecological resilience and socio-technical transitions: critical issues for sustainability governance,” 2008. [Online]. Available: www.steps-centre.org

[27] NIST, “Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1,” Gaithersburg, MD, Apr. 2018. doi: 10.6028/NIST.CSWP.04162018.

[28] J. Uher, “Quantitative Data from Rating Scales :An Epistemological and Methodological Enquiry,” *Front Psychol*, vol. 9, no. 2599, 2018.

[29] U. M. Mbanaso and V. E. Kulugh, “Empirical Findings of Assessment of Critical Infrastructure Degree of Dependency on ICT,” in *First International Conference on Cybersecurity in Emerging Digital Era*, R. Agrawal, G. Sanyal, K. Curran, V. E. Balas, and M. S. Gaur, Eds., Greater Nodia: Communications in Computer and Information Science, Oct. 2020, pp. 3–17.

[30] ONSA, “NATIONAL CYBERSECURITY POLICY AND STRATEGY 2021,” ABUJA, Mar. 2021.