Conceptual Design of a Cybersecurity Resilience Maturity Measurement (CRMM) Framework

Uche M. Mbanaso
Director, Centre for Cyberspace Studies, Nasarawa State University, Keffi, Nigeria; and Visiting Researcher, LINK Centre, University of the Witwatersrand (Wits), Johannesburg
https://orcid.org/0000-0003-2784-7415

Lucienne Abrahams
Director, LINK Centre, University of the Witwatersrand (Wits), Johannesburg
https://orcid.org/0000-0002-5219-8448

Oghenevovwero Zion Apene
PhD student, Computer Science Department, Nasarawa State University, Keffi, Nigeria
https://orcid.org/0000-0001-8051-2695

Abstract

African countries are at high risk with respect to cybersecurity breaches and are experiencing substantial financial losses. Amongst the top cybersecurity frameworks, many focus on guidelines with respect to detection, protection and response, but few offer formal frameworks for measuring actual cybersecurity resilience. This article presents the conceptual design for a cybersecurity resilience maturity measurement (CRMM) framework to be applied in organisations, notably for critical information infrastructure (CII), as part of cyber risk management treatment.

The main thrusts of the framework are to establish, through assessment in terms of quantitative measures, which cybersecurity controls exist in an organisation, how effective and efficient these controls are with respect to cybersecurity resilience, and steps that need to be taken to improve resilience maturity. The CRMM framework we outline is conceptualised as being applicable both pre- and post-cyber attack. Drawing on the NIST cybersecurity framework (NIST CSF) and other relevant frameworks, the CRMM approach conceptualised in this article would be able to depict an organisation's cybersecurity practices and gauge the organisation's cybersecurity maturity at regular intervals. This CRMM approach is grounded in the idea that, by quantifying an organisation's current practices against established baseline security controls and global best practices, the resulting status measurement can provide the appropriate basis for managing cyber risk in a consistent and proportionate fashion. The CRMM framework defines four cybersecurity resilience quadrants (CRQs), which depict four different degrees of organisational preparedness, in terms of both risk and resilience.

Keywords

cybersecurity, cybersecurity resilience maturity measurement (CRMM), cybersecurity resilience quadrants (CRQs), critical information infrastructure (CII), NIST cybersecurity framework (NIST CSF), cyber risk management, cybersecurity resilience, cybersecurity controls

DOI: https://doi.org/10.23962/10539/27535

Recommended citation

Mbanaso, U. M., Abrahams, L., & Apene, O. Z. (2019). Conceptual design of a cybersecurity resilience maturity measurement (CRMM) framework. *The African Journal of Information and Communication (AJIC), 23*, 1–26.
https://doi.org/10.23962/10539/27535

1. Introduction

Cyber threats create high levels of economic and safety uncertainty across African countries. Consulting house Serianu noted, in its *Africa Cyber Security Report 2017,* that the top cybersecurity threats on the continent in 2017 were: fake news; insider threats; ransomware; cyber bullying; the cybersecurity skills gap; theft of funds from mobile and internet banking customers; weak security infrastructure; phishing, cyber pyramid frauds; and hacking of government systems (Serianu, 2017a). The estimated cost of cybercrime to African businesses in 2017 was USD3.5 billion (Serianu, 2017a, p. 58). In five countries (Ghana, Kenya, Nigeria, Tanzania and Uganda), Serianu found that the most costly type of cybsersecurity breach (costing an estimated USD352 million across the five countries in 2017) was insider threats (Serianu, 2017a, p. 59). Individual Serianu country reports are available for Kenya, Nigeria, Tanzania and Uganda (see Serianu 2017b; 2017c; 2017d; 2017e). Serianu concluded that "over 90% of African businesses are operating below the 'cyber security poverty line'", i.e., below the minimum level of security required (Serianu, 2017a, p. 9).

Cyber threats have generated significant shifts in policy that are changing political and economic debates (Mbanaso & Dandaura, 2015), noting, for example, Nigeria's Cybercrime Act of 2015 and South Africa's Cybercrimes Bill of 2018.

Organisational cybersecurity frameworks tend to prescribe generic guidelines for *how* to secure an organisation's critical information infrastructure (CII), without providing ways of measuring precisely *what* the strengths and weaknesses are, as the basis for specific improvements. There is currently no tool to measure the current maturity level of an organisation's cybersecurity resilience. Thus, the research problem informing our work is the absence of available tools for precise measurement of organisational cybersecurity resilience maturity.

Effective cybersecurity risk management requires attention to organisational-level resilience, in order to build country-level resilience. The cybersecurity resilience maturity measurement (CRMM) framework we propose in this article is conceived as a maturity framework tool to help organisations ascertain their cybersecurity status by matching their current cybersecurity practices against baseline security controls and best practices. The implementation version of the CRMM framework, to be developed based on the conceptualisation outlined in this article, would address the full cybersecurity ecosystem within an organisation. The framework would enable organisations to identify where their practices are weak, or not adequately implemented, and would provide for security controls to be proportionately entrenched throughout the cyber risk management process.

A CRMM approach can, we contend, provide a unique way to measure organisation-wide progress made in embedding cybersecurity controls in day-to-day and strategic operations. It can measure a range of activities—including risks associated with leadership and governance, human resources management, procurement management, operations and technology management, processes and people—in a fashion that, when quantified, can indicate the cybersecurity maturity level of an organisation.

The core outcomes of the CRMM framework that we conceptualise in the article are the cybersecurity resilience quadrants (CRQs), which indicate an organisation's cybersecurity maturity level. These indicator quadrants, when analysed with reference to the relevant quantitative data, can reveal which controls and processes are under-achieving, or need to be fine-tuned, in order to achieve the expected maturity level. In this fashion, the CRMM framework can guide improvement across an organisation in a more consistent, coherent and measurable manner than is presently the case in most organisations' cyber risk treatments.

2. Research questions

In researching the necessary components for the CRMM conceptual framework, we were guided by several key questions, applicable in any organisation, which the framework would have to provide answers to. The overarching question was: What should be the structure, and key components, of a cybersecurity resilience maturity measurement framework?

We were guided, in our development of the CRMM structure and components, by our determination that the CRMM would, through its implementation by an organisation, need to answer the following questions for the organisation:

- What is the organisation's current stage in terms of cybersecurity resilience maturity?
- What is the organisation's desired next stage of maturity?
- What are the factors, causes or defects responsible for the current stage where the organisation is positioned?

- How does the organisation need to improve in order to achieve the next stage of maturity?
- In particular, what are the necessary security controls required for improvement?
- How can the organisation create momentum to ensure that its cybersecurity is consistently and constantly improved?

Guided by these questions, we sought to conceptualise quantifiable ways to measure, as accurately as possible, the variable factors that affect cybersecurity resilience. The conceptualised framework needed to accurately and consistently quantify the state of affairs with respect to an organisation's cybersecurity status at any given point in time, i.e., the degree to which the organisation's current practices and controls in place are appropriate to achieving improved cybersecurity resilience maturity.

The next section of this article provides background and underlying concepts, followed by a section on the phases of design, and refinement, of the CRMM. We then provide a detailed explanation of the CRMM framework, as conceptualised to date based on our research. After that, we provide a draft mathematical model developed for the framework, followed by conclusions.

This article provides the initial conceptual design for a CRMM framework. The detailed content of the framework, and its testing and refinement via data collection, will be presented in subsequent publications.

3. Background: The need for a cybersecurity resilience maturity measurement (CRMM) framework

Cyber attacks have become ubiquitous throughout society, drawing attention to the need to manage cyber risks (Hartwig & Wilkinson, 2014; HPE, 2016; Serianu, 2017a). Globally, advanced technologies have enabled malicious entities to commit cybercrime more easily than anticipated, while crippling cyber attacks are putting many organisations in disarray. The increase in data breaches is motivated by financial, political, revenge, espionage, identity theft and other motivations, resulting in long-term financial consequences, reputation and customer loss, loss of competitive advantage, and other liabilities (Marinos, 2013).

A significant cyber attack can result in loss of valuable assets, including personal data, commercial data, customers, intellectual property, and other assets (BIS, 2012). According to a 2016 Identity Theft Resource Centre (ITRC) report, 1,093 data breaches were documented in that year across five industries in the US (ITRC, 2016). Van Heerden, Von Solms and Vorster (2018) report on expert views that personal information disclosure and data breaches are among the top future threats for African countries. Van Heerden et al. (2018) quote one of their survey respondents as saying that corporations are "not always placing enough emphasis on securely storing and managing sensitive and private information", primarily due, according to the authors, "to the exploitation of unpatched systems and poorly secured systems holding Personal Identifiable Information (PII)" (p. 8).

Cyber risk management has emerged as a vital component of the corporate risk management portfolio, requiring effective steps to deal with and minimise risk exposure (ITU, 2017; NIST, 2017). As part of cybersecurity preparedness, an organisation's board and top management should be fully aware of cyber risk exposure and the degree of cybersecurity maturity needed to inform proportionate investment in cybersecurity. However, many organisations and institutions are not mindful of the cyber risks they face, due to lack of available scientific tools to quantify cyber risks and their severity. There is speculation about managing cyber risks, rather than deep understanding of the key drivers, variable factors, and effects that are relevant.

Cyber risks are top national priorities in many countries, as individuals, businesses, and governments increasingly face cyber attacks (Hartwig & Wilkinson, 2014). All countries need to increase their levels of cybersecurity resilience maturity, because the concentration of digital activities has incentivised cyber criminals to grow increasingly innovative, enabling them to persistently breach cybersecurity. Classes of cyber criminals have emerged with diversified interests and motivations, further complicating the threat landscape (Mbanaso, 2016). The effect of a single cyber attack, when it succeeds, may have debilitating effects of national magnitude, making it evident that cyber risk needs to be addressed at national levels. Cyber risk has prompted countries to devise a variety of approaches aimed at balancing the need to sustain the gains of the digital revolution with the need to combat the menace of cyber criminals (Powers, Fancher, & Silber, 2016), including: national cybersecurity strategies and policies, cybersecurity frameworks, cybersecurity agencies, and defence mechanisms. Increasing attention is being given to cybersecurity measurement frameworks and surveys, as a means to assess and advance maturity at country levels (see, for example, DTCC, 2014; ITU, 2015; 2017). However, because these approaches operate at national levels, they do not offer comprehensive solutions for application at the institutional level.

For example, Peter (2017) applies a Cyber Resilience Preparedness Index (CRPI) to 12 African economies,[1] where Egypt, Kenya, Nigeria, Tunisia, Morocco and South Africa show reasonable levels of preparedness with respect to their critical systems, industries, and classified documents. The five areas scrutinised in this 2017 Index are: (1) legislation, regulations, policies and articulation of a national cybersecurity strategy; (2) collaborations, cooperation and partnerships; (3) technical measures; (4) information-sharing mechanisms; and (5) capacity-building. This Peter (2017) CRPI framework operates at country level, drawing on three frameworks: the

[1] South Africa, Tunisia, Egypt, Kenya, Ghana, Morocco, Nigeria, Zimbabwe, Algeria, Libya, Angola, Sudan, listed here in order of Networked Readiness Index ranking.

DTCC (2014) cyber risk white paper; the ITU (2015) Global Cybersecurity Index and Cyber Wellness Profiles; and the Potomac Institute's Cyber Readiness Index (Hathaway, Demchak, Kerben, McArdle & Spidalieri, 2015). The Peter (2017) CRPI framework, like the three frameworks it draws on, "only measures the existence of each indicator in a country. Thus, the ranking is based on the existence, not the quality, extent or effectiveness, of the indicators for protecting each nation's cyber investments and critical infrastructure" (Peter, 2017, p. 50). These broad frameworks offer some limited perspective at country level, but do not assist organisations to adequately defend themselves against cybercrime.

In institutions of any kind, whether large corporate institutions, or small and medium-sized enterprises (SMEs), or governments, greater attention is needed to institutional-level cyber risk management. Yet too many of the current institutional-level cybersecurity frameworks (e.g., COBIT 5, NIST CSF) offer only broad guidelines for organisations to apply, rather than detailed, quantitative frameworks. Hence insufficient attention to cyber risk management is often present in organisational cybersecurity approaches.

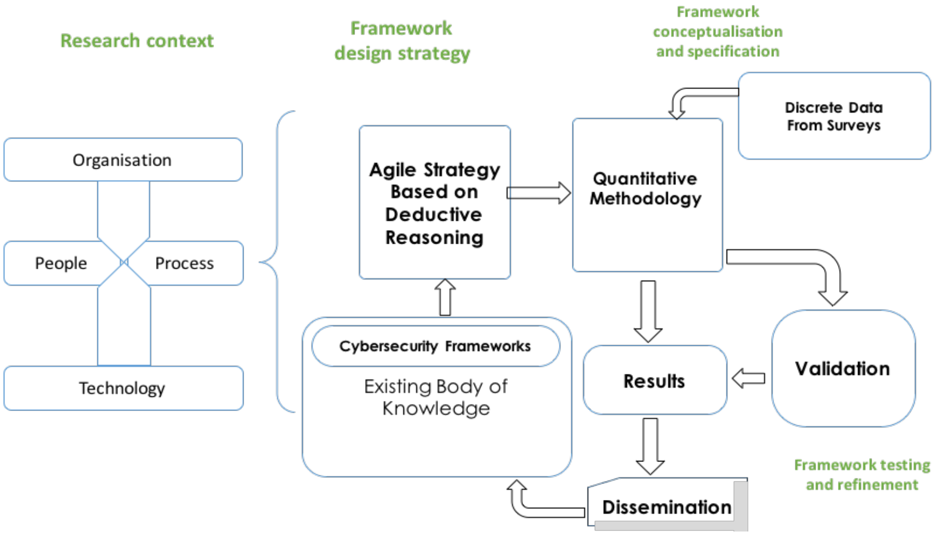
4. Research phases: Design and refinement of a CRMM framework

Cybersecurity can arguably no longer be viewed solely through the lenses of disciplines such as information systems or computer science, but should rather be understood as a multi-disciplinary domain spanning disciplines in both the sciences and humanities. At the same time, it is important, in both conceptual work and empirical work on cybersecurity matters, to adopt agile research strategies designed to enable researchers to continuously improve their frameworks (Dark, Bishop, Linger, & Goldrich, 2015).

We decided upon a quantitative approach for the conceptual framework we researched, on the grounds that a quantitative framework could generate replicable measurements able to establish the relationships between organisations' current cybersecurity practices and their targeted resilience maturity levels. Equally, it was clear to us that resilience should possess the characteristics of measurability, i.e., the resilience framework would need to be able to quantify the variable factors in numerical, logically computational form. This is in line with the dictates of quantitative empirical explorations, whose outputs must be computable, independent, numerical data that can be statistically analysed (Hassani et al., 2011; Salhin et al., 2016). Accordingly, the conceptual CRMM framework we set out in this article seeks to combine strengths found in various existing cybersecurity frameworks into a quantitative framework that can guide the design of instruments to allow logical computation of various effects or variables.

Figure 1 provides an illustration of the phases we decided would need to be followed in the design and refinement of a CRMM framework.

Figure 1: Design and refinement of a CRMM framework


Research context
Framework design strategy
Framework conceptualisation and specification
Organisation
People
Process
Technology
Agile Strategy Based on Deductive Reasoning
Quantitative Methodology
Discrete Data From Surveys
Cybersecurity Frameworks
Existing Body of Knowledge
Results
Validation
Dissemination
Framework testing and refinement

The discussion below provides detail on the steps taken to date, in terms of the phases outlined in Figure 1, for reference by any researchers wishing to follow similar phases in their own work on conceptualisation of quantitative measurement frameworks for application in organisational contexts. We cover only the first three phases—*research context*, *framework design strategy*, and *framework conceptualisation and specification*—as those are the phases we have completed and which produced the content for this article.

Phase 1: Research context

Contextually, the cybersecurity ecosystem should be observed through the variable factors that contribute to cybersecurity effects or risk. From a design perspective, the causal factors that affect cybersecurity can be viewed within the context of *organisation/enterprise*, *people, process*, and *technology* (ISF, 2016). These environments form the basis for comprehensive definition of causal factors and quantitative effects, as explained below:

- Organisation/enterprise: Corporate governance is key to effectiveness of operational cybersecurity aimed at minimising organisations' cyber risk exposure. In the organisational context, the executive management must set the policy direction and governance structure that provide assurance that cybersecurity actions are consistently and correctly executed.

- People: The people element seems often to be the weakest link, due to the inherent human fallibility (McAndrew, 2018; Sundström & Holmberg, 2008). Everyone with access to cyber infrastructure needs to be aware of their cybersecurity responsibilities, to have their effectiveness evaluated continually, and to be consistently managed.
- Process: Corporate processes, applications and data that support the operations and decision-making of cybersecurity must be assessed to assure effectiveness and consistency.
- Technology: This is concerned with assessment of physical and technical infrastructure, i.e., the network, hardware and software components required to support cybersecurity measures.

Phase 2: Framework design strategy

Events shaping cybersecurity risks are unpredictable and require continuous monitoring. Thus, we concluded that the philosophy and characteristics of agile strategy would need to be incorporated into the design of the CRMM framework. Various researchers (see Dark et al., 2015) have incorporated ideas and themes from agile strategy set out in the *Agile Strategy Manifesto* (Agile Helpline, 2011) into their work on the agile research process. Among the key characteristics of agile strategy is emphasis on an iterative or adaptive approach. We determined that the CRMM framework we conceptualised would need to be grounded in agile research strategy, i.e., it would need to be able to continually respond to the unpredictability of cybersecurity events and effects. Incorporating an agile approach into the framework would, we concluded, require inclusion of data analysis techniques that use deductive reasoning, in order to encourage agility based on reliable and objective data. Also required for the framework would be specification of regular, possibly annual or bi-annual, organisational application of the framework, in order to enhance agility.

Our framework design strategy also called for incorporation of relevant components from the existing body of knowledge with respect to cybersecurity frameworks and standards. As discussed in more detail in this article's section 5 below, it was decided that COBIT 5, CIS security controls, SoGP for IS, the ISO/IEC 27005, and NIST CSF should be examined, and selected components built into the design of the CRMM framework. For example, we built on the COBIT 5 achievement rating.

Phase 3: Framework conceptualisation and specification

Determining cybersecurity resilience maturity level requires measurement of events, and/or measurement of levels of occurrence of variable factors and effects. We determined that utilising relevant components from the five frameworks cited above and discussed in more detail below (hereafter referred to as the "combined core") would provide an appropriate foundation for a CRMM framework, noting that any identified gaps could be filled progressively as the framework is implemented and tested in actual organisations. Subsequent publications will report on the trial implementation of the framework in selected institutional settings, with the objective of testing the framework, and adapting it, if necessary, based on lessons learned.

We also concluded that cybersecurity resilience determinations would require that the framework, when applied, could generate discrete data with finite number values. This made the quantitative paradigm the necessary approach, since this would allow for numeric quantification of the resilience maturity values, and would allow for CRMM scores to be generated, disseminated, and compared, in a widely understandable fashion.

We also determined that the framework's data components would need to be selected from the five frameworks in such a way that they addressed the stated research problem as best as possible, and in a manner that could be validated. This meant that each data component chosen would have to be both relevant and quantifiable.

As a first step, COBIT 5, CIS security controls, SoGP for IS, and ISO/IEC 27005 would need to be examined and selected components mapped to the five functional pillars of the NIST CSF, thereby adapting the existing CSF, which is a guiding framework, to make it part of a quantifiable framework. As a second step, components of the combined core of the adapted NIST CSF would need to be examined to decide which should be selected and which should be deselected, based on clear reasons. As a third step, the full set of selected components would need to be used to craft a cybersecurity resilience maturity survey instrument. The survey instrument would need to use defined metrics for the combined core—an example of which is set out in Figure 3 below using the "protect" functional pillar of the NIST CSF.

We determined that the process of gathering relevant quantitative data in an established systematic way, for each of the components of the combined core, will be critical to the quality of the survey data, including the integrity, accuracy and reliability of the data. The result produced via a framework grounded in quantitative data needs to be quantifiable, objective, and consisting of numerical datasets that can be computationally and statistically analysed. Accordingly, our conceptualisation of the CRMM framework had to include provision for a computational mechanism based on computational mathematics, data structures, and algorithms. When developed as a software artefact, this computational mechanism would have to have the capability to process the data inputs and present the cybersecurity resilience quadrant (CRQ) indicator as an output. A brief outline of the key elements conceptualised for the mathematical model to be applied to the survey data is presented in this article's section 7.

(The full set of specific data collection components required for this third phase (framework conceptualisation and specification), and a discussion of the fourth phase (framework testing and refinement, as shown in Figure 1) will be published separately from this initial conceptual article.)

5. More detail on phase 3: Framework conceptualisation and specification

A range of frameworks and standards deal with cybersecurity from similar but distinct philosophical stances, each providing guidelines, principles, procedures, standards and best practices for effectively managing cybersecurity risks in organisations. These frameworks provide sequences of activities that can contextually manage cyber risk in a systematic fashion. Among these frameworks are the main foundation for our framework, the NIST cybersecurity framework (NIST CSF) (NIST, 2014), and four other influential frameworks in the field, namely, in chronological order of publication: version 5 of the control objectives for information and related technology (COBIT 5) (ISACA, 2012); the Centre for Internet Security (CIS) security controls (CIS, 2016); the standard of good practice for information security (SoGP for IS) (ISF, 2018); and the ISO information security risk management (ISO/IEC 27005) standard (ISO/IEC, n.d.). All five of these frameworks are applicable at organisational level.

Building on these five frameworks, the framework we devised focuses on the measurement of cybersecurity effectiveness at institutional level; in other words, creating a framework to measure actual resilience, rather than simply providing guidance. The sub-sections that follow introduce the five frameworks we drew on.

Control objectives for information and related technology (COBIT 5)

The control objectives for information and related technology (COBIT) framework has been developed by the Information Systems Audit and Control Association (ISACA), and the latest version, COBIT 5, is formulated using five principles and seven enablers. The principles are: meeting stakeholders' needs; covering the enterprise end-to-end; applying a single integrated framework; enabling a holistic approach; and separating governance from management. The enablers are: processes; organisational structures; culture, ethics and behaviour; principles, policies and frameworks; information; services, infrastructure and applications; and people, skills and competencies (ISACA, 2012). COBIT 5 is a comprehensive framework for the treatment of information technology governance and management, and includes but is not specific to cybersecurity matters. We determined that COBIT 5's principles and enablers can be accommodated within a framework grounded in NIST CSF.

Centre for Internet Security (CIS) security controls

The Centre for Internet Security provides a set of 20 security controls that establish a critical set of actions specific to handling aspects of cybersecurity threats in a wide range of sectors. These controls represent a collection of best practices, including six basic controls (including inventory and control of hardware assets; inventory and control of software assets; and continuous vulnerability management); 10 foundational controls (including email and web browser protections; malware defences; and data recovery capabilities) and four organisational controls (including security awareness and training; application software security; and penetration tests and red team exercises) (CIS, 2018). The CIS controls are specific to cybersecurity and contributed to our establishment of the building blocks for cybersecurity resilience.

Standard of good practice for information security (SoGP for IS)

The Information Security Forum (ISF) has formulated a standard of good practice for information security (SoGP for IS) to support organisations in addressing information security concerns based on six elements: technology, process, people, compliance, risk, and governance (ISF, 2018). The SoGP for IS also provides principles with respect to security governance, security requirements, control frameworks, and security monitoring and improvements. Furthermore, it addresses emerging concerns such as: threat intelligence; cyber attack protection and industrial control systems; enhancement of risk assessment approaches; security architecture; and enterprise mobility management. The SoGP for IS adds complementary dimensions to COBIT 5 and the CIS security controls.

ISO information security risk management standard (ISO /IEC 27005)

The International Organisation for Standardisation (ISO) and the International Electrotechnical Commission (IEC) provide a suite of information security standards, known as ISO/IEC 27005, which offer guidelines on information security risk management (ISO/IEC, n.d.). In particular, ISO/IEC 27005 is a risk-based approach to the treatment of cybersecurity: first, by establishing the cybersecurity context including the scope and the methods (either qualitative or quantitative); and second, by taking cognizance of the organisation's defined risk tolerance or appetite. It considers assets, threats, existing controls, and vulnerabilities as the basis for determining the probability of incident occurrences and anticipated level of risk. This standard is explicit with respect to risk management.

The NIST cybersecurity framework (NIST CSF)

The NIST cybersecurity framework (NIST CSF) provides three main components: (1) *framework core*, (2) *implementation tiers*, and (3) *framework profile* (NIST, 2018). The framework core primarily consists of a set of five cybersecurity functional categories (with subcategories) as essential activities for effective cybersecurity risk management. The five functions—*identify*, *protect*, *detect*, *respond*, and *recover*—define characteristics of security controls and activities that are implementable (NIST, 2018). The implementation tiers enable organisations to foster understanding of the cybersecurity treatment approach and the context upon which control measures can apply (Barrett et al., 2017). The framework profile provides the guidance for implementing the framework, and for tracking the organisation's requirements for improving its cybersecurity resilience posture.

The NIST CSF provides four implementation tiers—(1) *partial*, (2) *risk-informed*, (3) *risk-informed and repeatable*, and (4) *adaptive*—as the basis for choosing a target maturity profile, and for evaluation of progress (Almuhammadi & Alsaleh, 2017). According to NIST, the four tiers do not represent maturity, but rather the basis to support how organisations can view their maturity level. In other words, the tiers are meant to help inform top management's view of cybersecurity and its determination of the phases of action necessary to achieve a particular maturity target. NIST's notions of *current profile* and *target profile* are meant to address identified gaps consistently, but do not provide scientific or empirical ways to quantify cybersecurity resilience maturity.

In the African context, the NIST CSF is broadly followed by consultancy Serianu in construction of its Africa Cyber Security Framework, which includes four domains (Serianu, 2017a, p. 78). Domain 1 is *cybersecurity risk management (anticipate risks)*; domain 2 is *cybersecurity vulnerability management (detect vulnerabilities)*; domain 3 is *cybersecurity incident management (respond to incidents)*; and domain 4 is *cybersecurity visibility management (contain)* (Serianu, 2017a, p. 78). Serianu has also set out an Africa Cyber Security Maturity Framework, with five levels of cyber maturity: level 1 (*ignorant)*, level 2 (*informed*), level 3 (*engaged*), level 4 (*intelligent*), and level 5 (*excellent*) (Serianu, 2017a, p. 9).

Analysis

In as much as these frameworks and standards provide ways to treat cybersecurity risks, they do not provide means to *measure* actual cybersecurity resilience. Nonetheless, we found that many of the elements of these five frameworks and standards could be used as building blocks for the CRMM framework we propose.

6. Conceptualisation of a CRMM framework

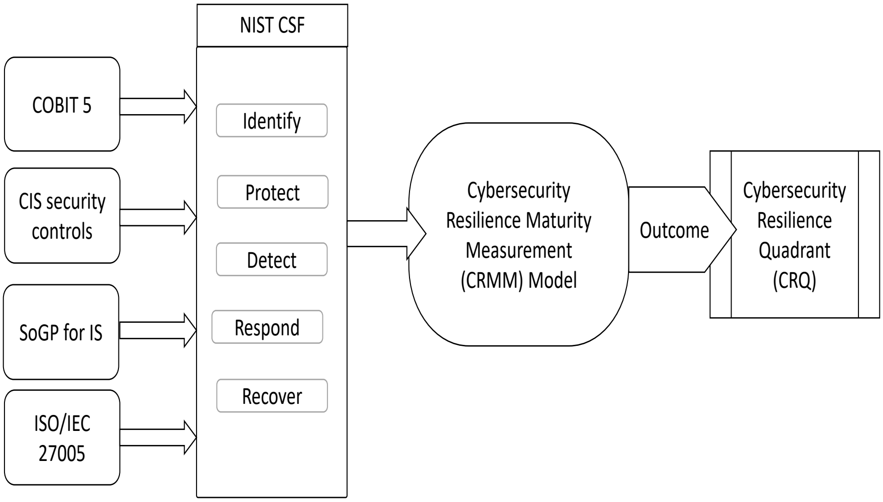
As explained above, our objective in conceptualising—and, at a later stage, piloting and refining—a CRMM framework is to enable quantitative measurement of cybersecurity resilience maturity, i.e., ascertaining the resilience posture of an organisation. This we consider necessary in order to ensure that an organisation's underperforming controls can easily be identified, prioritised, consistently managed, and improved upon. Due to cyberspace's continuously shifting threat environment, effective organisational operation in cyberspace requires a way of formally evaluating and measuring the cybersecurity resilience maturity level of an organisation, based on a comprehensive and actionable set of quantifiable effects and metrics. Such cybersecurity metrics can then be the basis for balanced understanding of cybersecurity resilience at the necessary level of granularity. Understanding cybersecurity resilience maturity requires analysis of actual organisational practice; hence the need for a suitable framework to quantify current practice against established baseline security controls and global best practices.

Accordingly, we have conceptualised our CRMM framework as a predictive tool that can provide quantification of various cybersecurity operational activities, can highlight areas that are under-performing, and can indicate the actions necessary to effect changes necessary to improve cybersecurity functions.

The CRMM framework we have conceptualised adapts the aforementioned NIST CSF five functional pillars—identify, protect, detect, respond, recover—and their respective subcategories, by mapping and integrating selected framework elements from COBIT 5, CIS controls, SoGP for IS, and ISO/IEC 27005 into the NIST

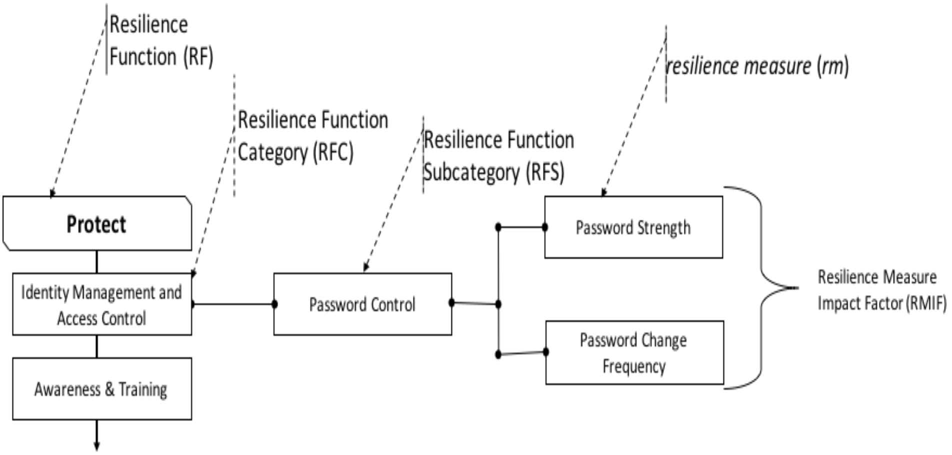
CSF. The result is the aforementioned *combined core* for the CRMM framework, which is aimed at ensuring that the framework is robust. The combined core, and the elements flowing from it, are illustrated below in Figure 2.

Figure 2: Combined core, and elements flowing from it, in proposed CRMM framework



Flowing from the conceptual design in Figure 2 above, Figure 3 below presents a magnified view of the structural organisation of one of the components of the framework and its categories and subcategories, using the "protect" functional pillar as the specific framework component. (This initial representation will be further refined, and applied with respect to all five NIST CSF functional pillars, at the next stage of our research endeavour.)

Figure 3: Example of draft CRMM functional pillar: "Protect"


Resilience Function (RF)
Resilience Function Category (RFC)
Resilience Function Subcategory (RFS)
resilience measure (rm)
Protect
Identity Management and Access Control
Awareness & Training
Password Control
Password Strength
Password Change Frequency
Resilience Measure Impact Factor (RMIF)

As depicted in Figure 3 for a single function ("protect"), a computational mathematical model design will be applied to each of the five functional pillars, with each of the five adapted NIST CSF functional pillars denoted as resilience functions (RFs), and with each RF underpinned by a resilience function category (RFC) and a resilience function subcategory (RFS). Additionally, for each RFS, a resilience measure (*rm*), and a resilience measure impact factor (RMIF), will be assigned.

7. Mathematical model for CRMM framework

The following are the elements we have initially developed for a mathematical model corresponding to the CRMM conceptual framework outlined above:

- Definition 1: Cybersecurity resilience function index (CRFI) is the sum total quantification of the resilience functions (or the sum of RFs) (explained in more detail below);
- Definition 2: Resilience function factor (RFF) defines the summation of resilience function categories (or RFCs) under a particular function;
- Definition 3: Resilience category factor (RCF) defines the summation of resilience function subcategory activities (or sum of RFSs) under a subcategory;
- Definition 4: Resilience function subcategory (RFS) factor is the sum total quantification of resilience measure impact factors (RMIFs);
- Definition 5: Resilience measure impact factor (RMIF) is the summation of resilience measures (*rm*s) for a specific subcategory; and
- Definition 6: Resilience measure (*rm*) is the unit quantification that measures a precise control (or depicting current practice) (explained in more detail below).

In the sections that follow, we provide the conceptual assumptions that underpin the construction of the mathematical model.

Cybersecurity resilience function index (CRFI)

The CRFI is the weighted summation of the quantification of the five functional pillars controls—identify, protect, detect, respond, recover—based on the contributing elements of the RFs. The weighted elements are grounded in the assumptions of what we determined to be percentage weights of the risk-contributing function factors (RCFFs) of the core functions, as shown in Table 1.

Table 1: Weightings of risk-contributing function factors (RCFFs)

	Function	Abbrev-iation	Description	Weight (%)	w_f
1	Identify	*idf*	identify factor effect	20%	0.20
2	Protect	*prf*	protect factor effect	25%	0.25
3	Detect	*def*	detect factor effect	20%	0.20
4	Respond	*ref*	respond factor effect	20%	0.20
5	Recover	*rcf*	recover factor effect	15%	0.15
	Total		total factor effect	100%	1

The rationale for the weights assigned to the risk-contributing function factors (RCFFs) in Table 1 is that function pillars will have varying effects on cybersecurity resilience. We argue that among the five functions (based on an average weighting of 20% for each), *protect* controls should be the highest priority, and thus should have a higher weighting, of 25%, because it serves as the most critical resilience factor effect. We based this weighting on the view that an organisation must put greatest emphasis on prevention. We determined that *recover* controls should be lower priority, with a marginally lower weighting of 15%, making it the least critical effect factor, as it is a result of actions taken in terms of the other four functional pillars.

Resilience measure (rm)

Based on our scrutiny of the existing frameworks outlined above, we decided that one of the foundational units of measure for all higher-level metrics in the design of the CRMM mathematical model should be the resilience measure (*rm*). This *rm* is the controlling effect that measures the actual cybersecurity practice against the baseline security controls and best practices. For this measure, we adapted the COBIT 5 *achievement* rating, to produce the *rm* formulated as a quantifiable weight, as depicted in Table 2. The COBIT 5 achievement rating is a standard derived from a rating scale defined in ISO/IEC 15504, which is mostly used in process assessment modelling. It is used here because the CRMM framework is an assessment model, and the COBIT 5 achievement rating is a known and accepted standard in process modelling.

Table 2: Weightings of resilience measure (*rm*)

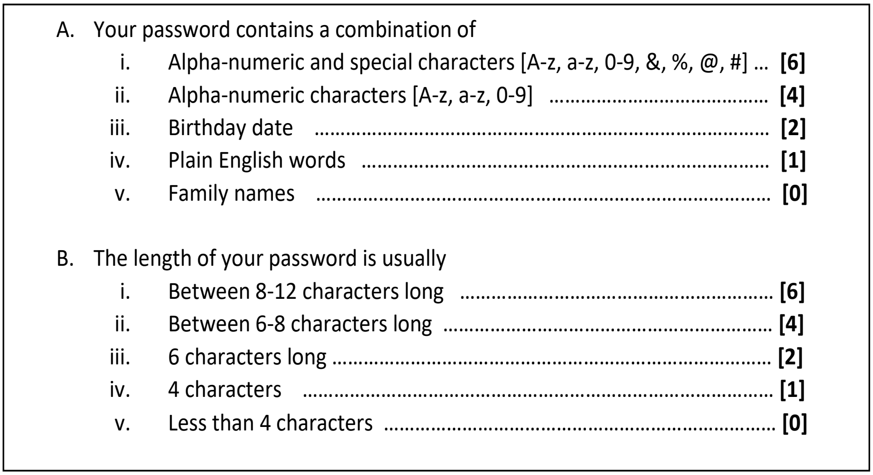
	***rm* level**	**Weight**	**Note**
1	not achieved	0	no controls in place, or very poor controls
2	loosely achieved	1	few controls in place, or incoherent controls
3	partially achieved	2	some controls in place, but not consistently and structurally organised; many, and/or important, elements missing
4	largely achieved	4	controls structurally implemented, but not consistent; only a few, and/or only minor, elements missing
5	fully achieved	6	baseline security; the best practice value

The resilience measure (*rm*) is the smallest unit of analysis for which data can be collected and can be specific to any particular types of resilience being measured in our framework—for example, password strength, as discussed below in relation to Figure 4 on "password regime". We built our conceptual design of *rm* through application of the SMART (*specific*, *measurable*, *actionable*, *relevant*, *timely*) construct derived from the field of strategic management. SMART is largely used in improvement and performance schemes in order to make goals achievable (Cheng et al., 2014; MindTools, 2018). We used SMART to clarify and conceptually position *rm* in a way that is focused, strategic and significant, and in a manner that increases chances of achieving certain defined objectives, as follows:

- Specific: The *rm* control is focused on a specific unit of effect measurement, and not a by-product or result of another component.
- Measurable: The *rm* control has quantifiable effect, i.e., it is accurate and complete by itself.
- Actionable. The *rm* control can be improved upon, i.e., it is easy to understand the particular corrective action required.
- Relevant: The *rm* control has measurable resilience effect, and is important to achieve the overall cybersecurity goal.
- Timely: The *rm* control is easily accessible when required.

To show how *rm* weight could be calculated in terms of the framework, Figure 4 provides a sample proposed instrument, which could be entitled "password regime".

Figure 4: Draft sample *rm* instrument: Password regime



A. Your password contains a combination of

i. Alpha-numeric and special characters [A-z, a-z, 0-9, &, %, @, #] ... **[6]**
ii. Alpha-numeric characters [A-z, a-z, 0-9] .... **[4]**
iii. Birthday date .... **[2]**
iv. Plain English words .... **[1]**
v. Family names .... **[0]**

B. The length of your password is usually

i. Between 8-12 characters long .... **[6]**
ii. Between 6-8 characters long .... **[4]**
iii. 6 characters long .... **[2]**
iv. 4 characters .... **[1]**
v. Less than 4 characters .... **[0]**

The draft instrument provided in Figure 4 would aim to test users' compliance level, and knowledge, quantitatively. In respect of statement A, a user who uses *alpha-numeric and special (or weird) characters* would have more resilience against password attacks than a user who uses *family names*. In respect of statement B, a user who has a password length of *8-12 characters* would have a higher resilience measure than a user with a password length of *4 characters*.

Drawing on the assignment of numeric values in Figure 4 and Table 2, enforcement and practice for the strongest password regime (i.e., A=6, B=6) would be quantified as *rm* level 5 (fully achieved). Thus, theoretically, it can be argued that the construction of weighted scales for the quantification of granular controls can provide adequate validity in terms of summation of baseline security controls and best practices for cybersecurity resilience.

An important note to add in this context is that a user may be aware of password best practice but still fail to comply. Users' resistance to change, or human weakness, can be a major factor in cybersecurity, and identification and quantification of such weaknesses can show an organisation more precisely what the strengths and weaknesses are, as the foundation for deciding how to address these.

Based on the foregoing, CRMM could be expressed mathematically to enable the development of a suitable data structure, algorithms, and computational logic for the various *rm* effects which, when summated, would produce a result that indicates an organisational cybersecurity resilience function index (CRFI) as a cybersecurity resilience quadrant (CRQ) indicator. The mathematical formulation would be as follows:

To sum the contributing effect of *rm* for one sub-category, it can be expressed as follows:

$$RMIF \;=\sum_{i=1}^{n} rm_i \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \, equation\,(1)$$

Where i = 1 to n, and n is the number of resilience effects under consideration.

To normalise the result for the resilience function subcategory, it is necessary to divide the resilience measure impact factor (RMIF) by *N*, so that equation (1) becomes: [2]

$$RMIF \;=\sum_{i=1}^{N} \frac{rm_i}{N} \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \, equation\,(2)$$

Similarly, it follows from the above equations that the contributing effect of the resilience category factor (RCF) for all subcategories can be expressed as follows:

$$RCF = \sum_{i=1}^{n} (RMIF)_i \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \, equation\,(3)$$

Where i = 1 to n, and n is the number of RMIF.

To normalise the above equation, it is necessary to divide RCF by *N*, so that equation (3) becomes:

$$RCF = \sum\nolimits_{i=1}^{N} \frac{(RMIF)_i}{N} \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \, equation\,(4)$$

Following from equation 4, the contributing effect of the resilience function factor (RFF) for all categories can be expressed as follows:

$$RFF = \sum\nolimits_{i=1}^{n} (RCF)_i \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \, equation\,(5)$$

Where i = 1 to n, and n is the number of RCF.

To normalise this equation, it is necessary to divide RCF by *N*, so that equation (5) becomes:

$$RFF = \sum\nolimits_{i=1}^{N} \frac{(RCF)_i}{N} \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \, equation\,(6)$$

[2] *n* is capitalised as *N* to show the distinction between the normalised and the standard values.

Now, the cybersecurity resilience function index (CRFI) is the next level equation needed to calculate the contributing effect of all resilience functions. Noting that each function has a specific contributing weight factor (see Table 1), the cybersecurity resilience function index (CRFI) can be expressed generically as follows:

$$CRFI = \sum_{i=1}^{N} (RFF)_i \times w_i \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \, equation\ (7)$$

Where i = 1 to N, and N is the number of RFF, but in this case N is 5, and w_i *is the weight factor of each function (see Table 1).*

So far, we have shown the accumulation of the various contributing function factors from subcategories to function categories, and then the functions. Therefore, based on the previously assigned weights (see Table 1), the function weight factors can be applied to specific functions, and the cyber resilience function index (CRFI) can now be expressed as follows:

$$CRFI = \left(RFF_{idf} \times w_{idf}\right) + \left(RFF_{prf} \times w_{prf}\right) + \left(\mathrm{RFF}_{def} \times w_{def}\ \right) + \left(\mathrm{RFF}_{ref} \times w_{ref}\right) + \left(RFF_{rcf} \times w_{rcf}\right) \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots..\, equation\ (8)$$

Since the values of function weight factors are known, derived from Table 1, we can substitute the values into equation 8. Thus, CRFI can be expressed as follows:

$$CRFI = 0.2(RFF\_idf) + 0.25(RFF\_prf) + 0.2(RFF\_def) + 0.2(RFF\_ref) + 0.15(RFF\_rcf) \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \, equation\ (9)$$

Where $CRFI_0$ *is the optimised cybersecurity resilience function index and should have a value* between *0 and 1 then:*

$$CRFI_o = \frac{CRFI}{100} \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \, equation\ (10)$$

From the foregoing, the cyber resilience quadrant (CRQ) can be created based on the following definitions assigned:
Quadrant I: “Initial” is the range 0.0 – 0.25
Quadrant II: “Defined” is the range 0.26 – 0.5
Quadrant III: “Managed” is the range 0.51 – 0.75
Quadrant IV: “Optimised” is the range 0.76 – 1.0

These formulations show how cybersecurity resilience maturity can be quantified mathematically. From the relevant CRQ, the degree of cybersecurity resilience of an organisation can be gauged—depicting the current practices and the degree of applicable baseline security controls, with the maturity level falling in one of the quadrants, I through IV.

The underlying logic is the quantification and aggregation of the effect of five functions—identify, protect, detect, respond, and recover functions—and their subcategories. In the subcategories, the resilience measure (*rm*), which is the smallest unit quantified, helps to measure the unique effects of each particular resilience indicator. The summation of the effects in a cluster of functions, including their subcategories, is then aggregated in the computation of the CRFI, leading to the generation of the CRQs. The numerical ranges assigned to each of the four possible CRQs (i.e., the four possible maturity quadrants) ensure that the cumulative resulting effect lies between 0 and 1, therefore generating four usable quadrants.

8. The cybersecurity resilience quadrants (CRQs)

The conceptual design of the cybersecurity resilience quadrants (CRQs) aims to provide a single view of an organisation's maturity level, i.e., its degree of cybersecurity resilience. The resulting $CRFI_o$ value is a pre-defined functional performance indicator that indicates in which of the four quadrants the organisation lies with respect to cybersecurity resilience maturity.

Thus, within our proposed CRMM framework, the CRQs represents the intersections of risk and resilience, as illustrated in Figure 5 on the next page. In order to formulate the CRQs, we adapted the capability maturity model integration (CMMI) developed by the Software Engineering Institute, Carnegie Mellon University (CMMI Institute, n.d.; Nath, 2018). The CMMI, which is globally recognised as a process improvement framework, has five levels (*initial, managed, defined, quantitatively managed, optimising).* We adapted four of the five CMMI levels to conceptualise the CRQs for our CRMM framework.

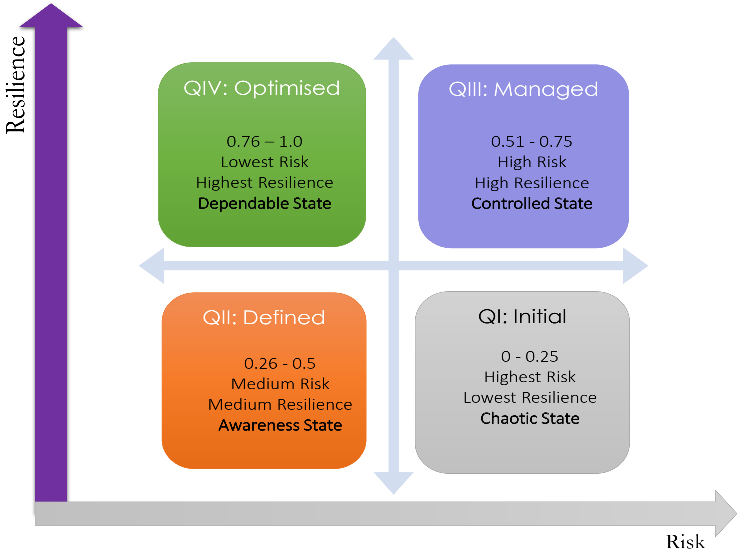
The explanations for each of the four CRQs are as follows:

- Initial: This CRQ describes a maturity level characterised by a high-risk environment with few, or ad hoc and chaotic, security controls. The organisation typically is not a stable environment, i.e., there is an absence of top management leadership and an absence of prioritisation of cyber risk as part of corporate risk management. This quadrant indicates highest risk and lowest resilience.
- Defined: This CRQ describes a maturity status that is characterised by a medium-risk environment with basic security controls in place. There is recognition of cyber risk, and the organisation is making efforts to ensure that security controls are standardised by policy, standards, procedures and governance functions. This quadrant indicates medium risk and medium resilience.
- Managed: This CRQ describes a maturity status that is well categorised and understood, and is described in standards, procedures, tools, and corporate governance practices. A critical distinction between *defined* and *managed* is the wider scope, in this quadrant, of the cybersecurity standards, policies and procedures across the organisation. Security controls are consistently planned, managed, performed, measured, and controlled. Relevant stakeholders are

aware of the cybersecurity responsibility imposed on them by virtue of their corporate responsibility. This quadrant indicates high risk but also high resilience. Risk is potentially high, but because the risk is understood and prioritised, it is managed vigorously and consistently.

- Optimised: This CRQ describes a maturity status that is effectively agile and continually improved, based on a quantitative understanding of the common cyber risk factors. There is full commitment of top management, and full understanding of organisational risk exposure. The significance of effective cybersecurity governance, and of stakeholders' roles and responsibilities, are well understood, resulting in a cycle of persistent improvement and continual revision in order to respond to changing business objectives and the changing threat environment. This quadrant indicates the lowest risk and highest resilience.

Figure 5: Cybersecurity resilience quadrants (CRQs)



9. Conclusion and future work

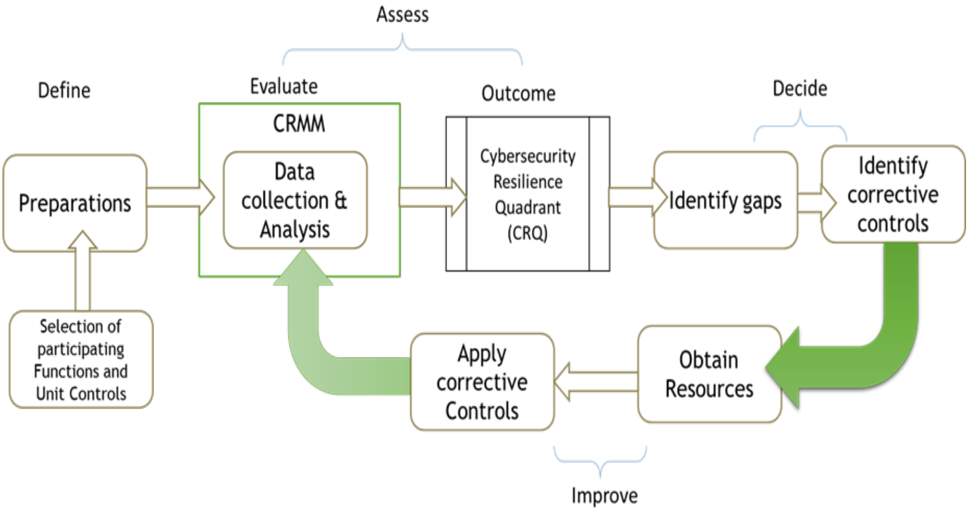
The CRMM framework we have outlined in this article conceptualises mechanisms to address cybersecurity risk management gaps. It incorporates a mathematical model designed to quantify the cybersecurity effects and variables which, if correctly addressed, can lead to improved performance of an organisation's cybersecurity. The CRMM and its CRQs provide a framework for developing, improving, and sustaining cybersecurity resilience by determining the extent to which the organisation's current actions on cybersecurity governance are working, the extent to which the organisation is improving, and the extent to which the organisation needs greater continuous improvement. Our CRMM framework offers a rigorous yardstick, a performance-rating technique, which allows comparison between an organisation's current cybersecurity performance against known best practice, and between current performance and the organisation's previous, or desired future, performance.

While there are robust cybersecurity frameworks that prescribe the essential toolkits to manage cybersecurity risk, determining the current state of cybersecurity resilience remains an imprecise practice. This gap makes it difficult for an organisation to ascertain its current status, and to identify a visible path for improvement. As an organisation advances its cybersecurity preparedness, it is expected to establish a maturity level whereby it detects areas needing enhancement, and knows how to correct negative effects by drilling down to under-performing areas. The CRMM and the CRQs are conceptualised with the aim of providing a clear single view of an organisation's cybersecurity resilience maturity, in a way that can direct the organisation to consistently and continuously better its performance. To earn an optimised CRQ rating in our framework, i.e., to achieve an optimised level of cybersecurity resilience maturity, an organisation will have to exhibit a deep understanding of, and commitment to, improving cybersecurity resilience based on statistical and quantitative methods. Conversely, an organisation found to be in one of the other three quadrants will receive an indication of the elements that the organisation requires, by way of continuous improvement, in order to advance to a higher level of cybersecurity resilience maturity, i.e., to a better CRQ.

The CRMM approach can create value for an organisation by establishing the specific gaps and priorities in its cybersecurity. Applying the CRMM framework will provide a status report on which of the four quadrants the organisation falls into, which controls are underperforming, which quadrant the organisation should move to next, and how it can move to that next quadrant, all the while building greater organisational precision in measuring resilience levels.

The conceptual design we have presented in this article is a first step towards greater precision in measuring cybersecurity resilience maturity. The next step in this research will be to move from the conceptual framework to actual testing and refinement, via pilot implementation. Pilot implementation will initially require four steps, as set out in Figure 6: (1) *define* (first, by selecting relevant functions and unit controls); (2) *assess* (evaluate the current state of pilot organisations' resilience through pilot quantitative surveys generating CRQ outcomes); (3) *decide* (decide on corrective controls); and then (4) *improve* (pilot application – apply prioritised controls to enhance resilience).

Figure 6: CRMM framework testing and refinement


Assess
Define
Evaluate
CRMM
Outcome
Decide
Preparations
Data collection & Analysis
Cybersecurity Resilience Quadrant (CRQ)
Identify gaps
Identify corrective controls
Selection of participating Functions and Unit Controls
Apply corrective Controls
Obtain Resources
Improve

We are also developing a software application to support framework testing and refinement. Using the software, organisations will be able input their relevant data and compute their CRQ and deduce appropriate remedial actions, if applicable. Our subsequent publications will, among other things, focus on the detailed computational design, algorithms, and data structures for the CRMM software tool.

References

Agile Helpline. (2011). Agile strategy manifesto. Retrieved from http://www.agilehelpline.com/2011/04/agile-strategy-manifesto.html

Almuhammadi, S., & Alsaleh, M. (2017). Information security maturity model for NIST cyber security framework. *Computer Science & Information Technology (CS & IT)*, *7*(3) 51–62. https://doi.org/10.5121/csit.2017.70305

Barrett, M., Marron, J., Yan Pillitteri, V., Boyens, J., Witte, G., & Feldman, L. (2017). *The cybersecurity framework: Implementation guidance for federal agencies*. Draft NISTIR 8170. US Department of Communication. Retrieved from https://csrc.nist.gov/csrc/media/publications/nistir/8170/draft/documents/nistir8170-draft.pdf

Center for Internet Security (CIS). (2018). CIS controls version 7. Retrieved from https://learn.cisecurity.org/20-controls-download

Cheng, Y., Deng, J., Li, J., Deloach, S. A., Singhal, A., & Ou, X. (2014). Metrics of security. In A. Kott, C. Wang, & R. F. Erbacher (Eds.), *Cyber defense and situational awareness* (pp. 263–295). Cham: Springer. https://doi.org/10.1007/978-3-319-11391-3_13

CMMI Institute. (n.d.). Introducing CMMI V2.0. Retrieved from https://cmmiinstitute.com/capability-maturity-model-integration

Dark, M., Bishop, M., Linger, R., & Goldrich, L. (2015). Realism in teaching cybersecurity research: The agile research process. In M. Bishop M., N. Miloslavskaya, & M. Theocharidou (Eds.), *Information security education across the curriculum*. Proceedings of the 9th IFIP WG 11.8 World Conference on Security Education (WISE 9), Hamburg, May. Cham: Springer. https://doi.org/10.1007/978-3-319-18500-2_1

Department for Business, Innovation and Skills (BIS). (2012). *Cyber risk management – A board level responsibility*. London: UK Government. Retrieved from https://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/12-1119-cyber-risk-management-board-responsibility.pdf

Depository Trust and Clearing House (DTCC). (2014, October). *Cyber risk – A global systemic threat: A white paper to the industry on systemic risk*. Retrieved from http://www.dtcc.com/~/media/Files/Downloads/issues/risk/cyber-risk.pdf

Federal Republic of Nigeria. (2015). Cybercrime Act. Retrieved from http://www.nigerianlawguru.com/legislations/STATUTES/CYBERCRIME%20ACT%202015.pdf

Hartwig, R. P., & Wilkinson, C. (2014). *Cyber risks: The growing threat.* Insurance Information Institute. Retrieved from https://www.iii.org/sites/default/files/docs/pdf/paper_cyberrisk_2014.pdf

Hassani, H., et al. (2011). Research methods in computer science. *Methodological Innovations Online*, *11*(1), 1–16. https://doi.org/10.13140/RG.2.2.25912.55043

Hathaway, M., Demchak, C., Kerben, J., McArdle, J., & Spidalieri, F. (2015). *Cyber readiness index 2.0: A plan for cyber readiness: A baseline and an index*. Arlington, VA: Potomac Institute for Policy Studies. Retrieved from http://www.potomacinstitute.org/images/CRIndex2.0.pdf

Hewlett Packard Enterprise (HPE). (2016). *HPE cyber risk report 2016*. Retrieved from http://techbeacon.com/sites/default/files/gated_asset/hpe-cyber-risk-report-2016.pdf

Identity Theft Resource Center (ITRC). (2016). *ITRC data breach reports: 2016 end of year report*. Retrieved from https://www.idtheftcenter.org/images/breach/2016/DataBreachReport_2016.pdf

International Organisation for Standardisation & International Electrotechnical Commission (ISO/IEC). (n.d.). ISO/IEC 27000 family - Information security management systems. Retrieved from https://www.iso.org/isoiec-27001-information-security.html

Information Security Forum (ISF). (2018). *The standard of good practice for information security 2018*. Retrieved from https://www.securityforum.org/tool/the-isf-standard-good-practice-information-security-2018/

Information Systems Audit and Control Association (ISACA). (2012). COBIT 5 introduction. Retrieved from https://www.isaca.org/COBIT/Documents/An-Introduction.pdf

International Telecommunication Union (ITU). (2015). Global cybersecurity index and cyberwellness profiles. Retrieved from https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-SECU-2015-PDF-E.pdf

ITU. (2017). *Global cybersecurity index 2017*. Retrieved from https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-R1-PDF-E.pdf

Marinos, L. (2013). *ENISA threat landscape 2013: Overview of current and emerging cyber-threats*. European Union Agency for Network and Information Security. https://doi.org/10.2788/14231

Mbanaso, U. M. (2016). Cyber warfare: African research must address emerging reality. *The African Journal of Information and Communication (AJIC), 18,* 157–164. https://doi.org/10.23962/10539/21789

Mbanaso, U. M., & Dandaura, E. S. (2015). The cyberspace: Redefining a new world. *IOSR Journal of Computer Engineering*, *17*(3), 17–24. doi: 10.9790/0661-17361724

McAndrew, T. (2018, January 28). Human phish-bait: Why people are the weakest link in our cyber defence. *Washington Times*.

MindTools. (2018). SMART. Retrieved from https://www.mindtools.com/pages/article/smart-goals.htm

Minister of Justice and Correctional Services. (2018). Cybercrimes Bill. Pretoria: Government of South Africa. Retrieved from https://www.ellipsis.co.za/wp-content/uploads/2018/03/181023Clean_Cybercrimes_Bil.pdf

Nath, S. (2018). Building capability with CMMI. *ISACA Journal*. Retrieved from https://www.isaca.org/Knowledge-Center/Blog/Lists/Posts/Post.aspx?ID=667

National Institute of Standards and Technology (NIST). (2014). *Framework for improving critical infrastructure cybersecurity*. https://doi.org/10.1109/JPROC.2011.2165269

NIST. (2018). *Framework for improving critical infrastructure cybersecurity*. v1.1 Draft. https://doi.org/10.1109/JPROC.2011.2165269

Powers, E. W., Fancher, J. D., & Silber, J. (2016). *Beneath the surface of a cyberattack: A deeper look at business impacts*. Deloitte. https://doi.org/10.1007/978-1-4302-1115-0_14

Salhin, A., Kyiu, A., Taheri, B., Porter, C., Valantasis-Kanellos, N., & König, C. (2016). Quantitative data gathering methods and techniques. In A. Paterson et al. (Eds.), *Research methods for accounting and finance*. https://doi.org/10.23912/978-1-910158-88-3-3226

Serianu. (2017a). *Africa cyber security report 2017: Demystifying Africa's cyber security poverty line*. Retrieved from www.serianu.com/downloads/AfricaCyberSecurityReport2017.pdf

Serianu. (2017b). *Kenya cyber security report 2017: Demystifying Africa's cyber security poverty line*. Retrieved from www.serianu.com/downloads/KenyaCyberSecurityReport2017.pdf

Serianu. (2017c). *Nigeria cyber security report 2017: Demystifying Africa's cyber security poverty line*. Retrieved from www.serianu.com/downloads/NigeriaCyberSecurityReport2017.pdf

Serianu. (2017d). *Tanzania cyber security report 2017: Demystifying Africa's cyber security poverty line*. Retrieved from www.serianu.com/downloads/TanzaniaCyberSecurityReport2017.pdf

Serianu. (2017e). *Uganda cyber security report 2017: Demystifying Africa's cyber security poverty line*. Retrieved from htwww.serianu.com/downloads/UgandaCyberSecurityReport2017.pdf

Sundström, M., & Holmberg, R. (2008). The weakest link human behaviour and the corruption of information security management in organisations – An analytical framework. In International Institute of Informatics and Systemics (Ed.), *IMSCI '08: 2nd International Multi-Conference on Society, Cybernetics and Informatics*, Vol. III Proceedings (pp. 94-99). Retrieved from http://portal.research.lu.se/ws/files/5974349/1543150.pdf

Van Heerden, R., Von Solms, S., & Vorster, J. (2018). Major security incidents since 2014: An African perspective. In IEEE (Ed.), *2018 IST-Africa Week Conference (IST-Africa).* Retrieved from https://ieeexplore.ieee.org/document/8417326