Augmenting Cybersecurity Awareness at Critical Infrastructures in Developing Countries Through a Cybersecurity Governance Maturity Model

Hendrik Zwarts, Jaco Du Toit and Basie Von Solms
University of Johannesburg, South Africa

hzwarts@yahoo.com
jacod@akademia.ac.za
basievs@uj.ac.za

Abstract: As the utilization of cyber systems in the management and operation of critical infrastructures have grown, the cybersecurity threats to critical infrastructure sectors such as energy, healthcare, transportation and water simultaneously increased exponentially. Critical infrastructures in developing countries are particularly vulnerable to growing cybersecurity threats due to limited resources, inadequate cybersecurity policies and a general shortage of skilled cybersecurity specialists. Addressing these vulnerabilities is essential for developing countries to ensure the operational continuity, data protection and public safety associated with functioning critical infrastructures. An explorative literature review identified a number of aspects that can be used to counter the increasing cybersecurity threats to critical infrastructures in developing countries. Literature suggests that although there are defined norms and standards for critical infrastructures in developing countries, there is room for improvement in terms of the contribution that enhanced cybersecurity awareness can accomplish. A good cybersecurity awareness program must include sufficient training that is aligned with an organization's objectives, focus on raising cybersecurity awareness while performing normal duties whilst creating an interactive cybersecurity communication culture between all stakeholders. This paper presents research that is in progress to develop a functional cybersecurity governance maturity model aimed at capacitating role players responsible for the safeguarding of critical infrastructure systems in developing countries. The primary aim of the evolving Critical Infrastructure Cyber Governance Maturity Model (CICGM²) is to improve the cybersecurity governance of critical infrastructure systems in developing countries. The purpose of the article is to specifically describe how the CICGM² can be used to assess and determine the level of maturity of cybersecurity awareness programs at critical infrastructures in developing countries. The integration of recognized cybersecurity governance frameworks and established cybersecurity maturity models into the CICGM² presents unique opportunities to establish, measure and manage cybersecurity awareness initiatives at critical infrastructure systems in developing countries. This article contributes to the field of cybersecurity governance by offering a non-technical, scalable and adaptable CICGM² for key stakeholders at critical infrastructures in developing countries that can be used to determine the level of the cybersecurity awareness initiatives for the facilities that they are responsible for.

Keywords: Critical infrastructure, Cybersecurity, Awareness, Maturity model, Cybersecurity governance, CICGM²

1. Introduction

The European Union defines critical infrastructure (CI) as "an asset, a facility, equipment, a network or a system, or a part of an asset, a facility, equipment, a network or a system, which is necessary for the provision of an essential service" (European, 2022). It includes critical services which, if damaged or disrupted, would significantly impact the functioning of public services such as electricity and water provision, health care services and transport systems (Rajaonah, 2017). Critical Information Infrastructure (CII) refers to the computer systems and resources that underpin the core operations of Critical Infrastructure. The security of CII is a worldwide concern due to its essential role in the functioning of any nation's infrastructure. In addition to improving social connectivity and information exchange, the technological revolution has significantly improved organizational productivity (Prakasha, 2022).

The pivotal role of CIs make them targets for various criminal and terrorist organisations, but it is their increased interdependency - accelerated with the introduction of digital systems such as the Internet of Things (IoT) – that resulted in a much bigger cybersecurity threat (Urlainis, 2022). In recent years, the risk of cyberattacks on digital systems that manage and monitor CI has been steadily increasing. To mitigate this risk, greater emphasis should be placed on access control, personnel training, and managing insider threats. Nowadays many successful cyberattacks focus on exploiting vulnerabilities in human preparedness rather than targeting system or application-level weaknesses, often by targeting corporate personnel in CIs (Chowdhury et al., 2022).

The context of this article is an ongoing PhD study aimed at creating a Critical Infrastructure CICGM². The research problem of the study suggests that there are inadequate cybersecurity governance maturity models to assess the levels of cybersecurity governance measures in the critical infrastructure systems of developing

countries. This article itself focuses on the potential application of such a CICGM² to determine and improve the levels of the cybersecurity awareness capacity at CI facilities in developing countries.

This article is organised as follows: Section 2 reflects on the growing cybersecurity threat towards CIs in developing countries. Section 3 discusses the process that was followed to develop the CICGM². Section 4 briefly deliberates on the methodology that was followed for this article. Section 5 is a discussion on how the CICGM² could be utilised to improve cybersecurity awareness at CIs in developing countries and Section 6 provides the Conclusion.

2. The Growing Cybersecurity Threat Against Critical Infrastructures in Developing Countries

The Internet has grown and evolved considerably over the past few decades, profoundly changing how society, the economy and CIs function (Admass, 2024). Due to the critical role that CIs play in a country, CIs have always been targeted by various persons or organisations such as activists, rivals, terrorists and foreign countries. The introduction of cyberspace in the operation of CI added a new dimension to the threats CIs face as well as the adversaries targeting these facilities (Prakasha, 2022). Within the cybersecurity context the main attackers include nation-state actors, cybercriminals, state-sponsored attackers, terrorists, internal threat actors and hacktivists (Laubshtein, 2023). Research by the European Union Agency for Cybersecurity (ENISA) in 2023 proposes that these threat actors are motivated by financial gain, espionage, geopolitical disruptions, destruction of CIs and ideological beliefs.

Disabling or damaging CIs could potentially result in loss of life, economic instability and/or a compromise in national security. To prevent these consequences, CIs must be protected against all kinds of attacks – both physical as well as cyber (Sontan and Segun, 2024). Cyber threats against CIs evolved in recent decades with the increased introduction and utilisation of digital technologies (Sontan and Segun, 2024). This increase in cyber threats was exacerbated by society's – and CIs - increased dependence on ICT systems, the Internet and wireless networks (Admass, 2024). The cybersecurity threats to CIs are therefore increasing due to the growing number of connected devices. Unsurprisingly, there has been an increase in the occurrence of service disruption attacks, extortion and ransom demands at CIs (Laubshtein, 2023). As an example, cyberattacks on CIs in South Africa, a developing country, shows a rapid increase in the number of attacks as well as the diversity of targets since 2016. A single attack on Armscor in 2016 escalated to multiple attacks in 2021 where Transnet, the South African Space Agency, the Department of Justice and Constitutional Development, as well as the South African National School of Government was targeted (Oxford, 2022). Similar increases were observed in other developing countries such as Saudi Arabia and India (Lehto and Neittaanmaki, 2022).

The protection of CIs in developing countries is a serious challenge because of old CIs and insufficient capital investments to build new infrastructure. The main contributing factors that increase the cybersecurity threats to CIs in developing countries range from delayed digitalisation of CIs, the utilisation of ICT technologies that originate from developed countries, the cybersecurity risks associated with new ICTs and technologies are ignored or downplayed. The development of CIs are often sponsored by external entities that install their own ICTs in CIs and, therefore, have a certain amount of control over the functioning of the infrastructure process and/or facility of developing countries (Urlainis, 2022). The next section will briefly describe how the CICGM² was developed.

3. A cybersecurity Governance Maturity Model for Critical Infrastructures in Developing Countries

The process that was followed to develop the CICGM² for CIs in developing countries is described in detail in an article that will be presented at the 13th Computing Conference in London, United Kingdom in June 2025. A brief summary of this article contextualises the basis upon which this article was constructed (Zwarts et al., 2025).

As part of an ongoing PhD study a void was identified that suggests that there are inadequate cybersecurity governance maturity models to assess the levels of cybersecurity governance measures in the critical infrastructure systems of developing countries. The core proposition of the CICGM² was to create a model to evaluate cybersecurity governance maturity levels at CIs in developing countries The building blocks for the CICGM² were derived from recognised models and frameworks such as the Oxford's Cybersecurity Capacity Maturity Model for Nations (CMM), Centre for Internet Security's (CIS) Critical Security Controls Model, National Institute of Standards and Technology Cybersecurity Framework (NIST CSF), The ISO 27001 Framework and the Control Objectives for Information and Related Technology (COBIT) Governance Framework.

By integrating the core configurations of the models and frameworks mentioned above, the preliminary development elements of the proposed Critical Infrastructure Cyber Governance Maturity Model (CICGM²) were formulated. Figure 1 presents this holistic overview of the development elements (without necessarily including all the subcategories).

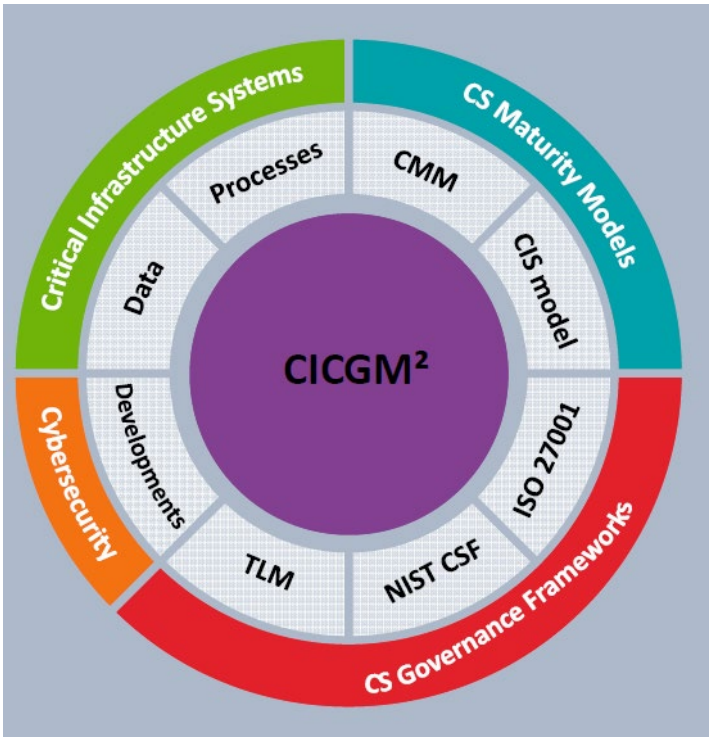

Figure 1: Design Elements of the CICGM² (Zwarts, Du Toit, Von Solms, 2025)

More research and development are still required to establish the maturity parameters and criteria for the CICGM². This parameters and criteria for cyber governance maturity levels must clearly outline the expectations for each level. To operationalize the CICGM² the cyber governance maturity levels are defined based on the following criteria:

- **Governance Level**: The level at which the Critical Infrastructure (CI) is governed. As illustrated in Figure 2, a CI can be managed at one of three levels: strategic, tactical, or operational. The governance level determines the specific cyber governance responsibilities for the CI.
- **Functions Performed**: The cybersecurity management or governance functions carried out within each CI can be categorized into six areas: govern, identify, protect, detect, respond, and recover.
- **Components Measured**: Nine key components of cyber governance have been identified for inclusion in the CICGM² framework. These components are policies, technology, cyber awareness, collaboration, risk management, legal considerations, stakeholders, work culture, and cybersecurity threats. Together, they encapsulate the core elements of effective cyber governance.

The resulting CICGM² is depicted in Figure 2 below. This design construct incorporates the capacity building maturity dimensions (2021), cyber governance processes ((NIST, 2024) (Kosutic, 2024) (Lanure et al., 2022)) and potential implementation levels ((Melaku, 2023) (Tatar et al., 2016)) discussed in this article.

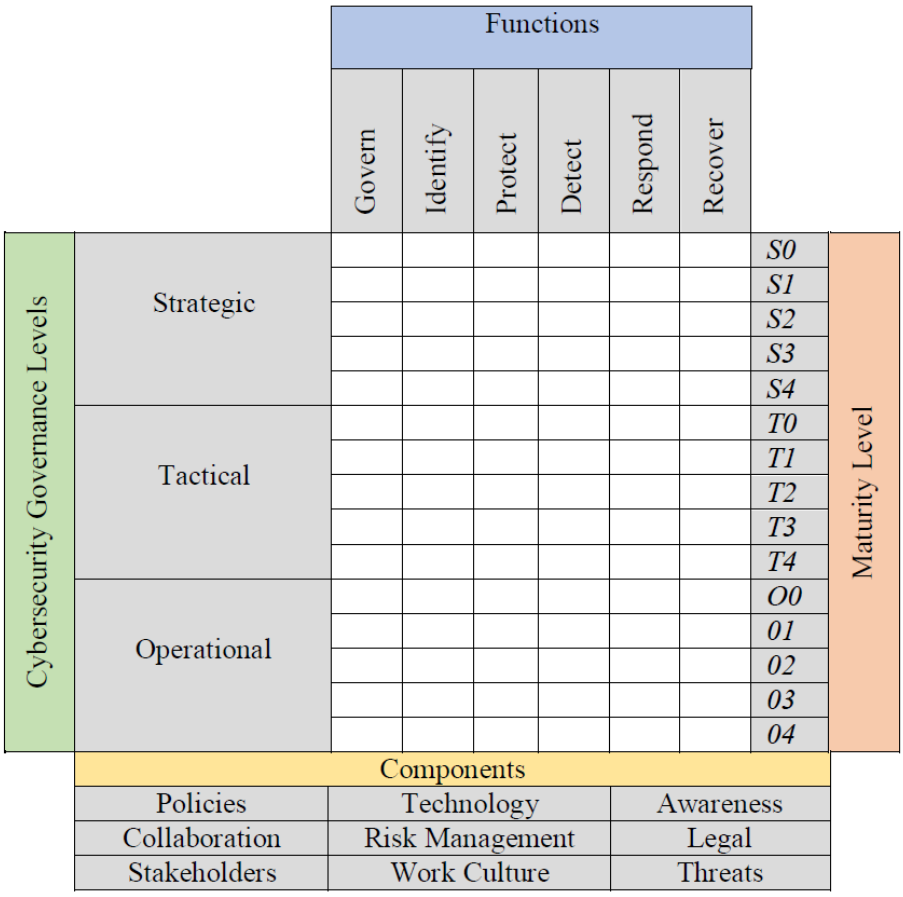

Figure2: Design Construct for the CICGM² (Zwarts, Du Toit, Von Solms, 2025)

The next section will look at the research methodology that was used to compose this article.

4. Research Methodology

The research methodology of the PhD study to development the CICGM² consists of a literature review on all the aspects of cybersecurity in critical infrastructures, cybersecurity governance frameworks, and cybersecurity maturity models. The building blocks identified in the literature review was used to construct the CICGM². The third phase will employ a qualitative approach, using purposive sampling to gather data from industry experts to refine the final CICGM². This paper concentrates on the Cybersecurity Awareness and capacity building of the CICGM².

Based on the design construct of the CICGM² this article conducted a literature review on cybersecurity awareness and capacity building. The objective was to identify cybersecurity awareness requirements necessary to measure and develop this capacity in CIs in developing countries. Due to the intended implementation area the identified requirements are specifically on a non-technical level. The next section is a discussion on the possible application of the CICGM² to improve cybersecurity awareness at critical infrastructures in developing countries.

5. Application of the CICGM² to Measuring and Improving Cybersecurity Awareness Capacities Critical Infrastructures in Developing Countries

The question is, how can the CICGM² be applied to improve the cybersecurity awareness at CIs in developing countries? The importance of cybersecurity awareness has increased over the last two decades as governments, businesses and individuals' day-to-day activities around the world become more and more digitalised. The challenge for developing countries is that these countries often lack the organizational, technological and human resources to secure their online activities. These cybersecurity capacity shortages increased considerably with the introduction of IT and OT devices in CIs (Veale and Brown, 2020).?

Cybersecurity awareness capacity building has evolved to the point where cybersecurity frameworks include much more than the traditional technical aspects of cybersecurity. Digitalisation and social media uptake in almost all aspects of modern-day living necessitated a paradigm shift with regards to cybersecurity capacity building to include aspects such as cybersecurity strategy and policy, awareness, legal and regulatory structures, threat response etc. (Dutton et al., 2019).

Humans are still one of the main security vulnerabilities in the protection of CIs. Insufficient cybersecurity awareness training of employees is a key factor behind many successful cyberattacks at CIs. As social engineering techniques continue to evolve, attackers frequently target employees to gain access to sensitive information. To address this threat, cybersecurity awareness training initiatives have been prioritised at both government and corporate environments. Therefore, human alertness is a crucial component of cybersecurity for CIs (Chowdhury et al., 2022).

There are a number of models and frameworks that include cybersecurity awareness elements such as the Cybersecurity Capacity Maturity Model for Nations (CMM), Global Forum on Cyber Expertise's (GFCE) agenda for cyber capacity building, Association of Southeast Asian Nations (ASEAN) Cyber Capacity Programme (ACCP) and the Cyber Security Body of Knowledge (CyBOK) to name a few. By integrating the concepts of these models the following list of elements constitute issues that should be included in an elementary cybersecurity awareness program (Zwarts et al., 2022):

- The basic concepts of cybersecurity
- The concept of cyberspace
- The dependencies between cybersecurity and the main security domains
- The areas that fall under cybersecurity
- Different frameworks that identify cybersecurity risks
- Elements that can be targeted in an ICT system
- The correlation between human behaviour and cybersecurity risks
- The threats and threat agents that exist within the cybersecurity environment

One of the main reasons why there is a need for a CICGM² is that humans play a significant role in an organization's security and their behaviour is influenced by their perception of risk - perceptions that can and should be changed. As the cyber threat to CIs is constantly evolving and changing, cybersecurity awareness and skills among all CI employees also need to change accordingly (Spremić and Šimunic, 2018). The CICGM² provides a tool to measure and manage the level of cybersecurity awareness capacity within CIs.

he CICGM² proposes an alternative solution to improving cybersecurity awareness capacity building by introducing a maturity model that focuses specifically on improving the governance of cybersecurity related aspects of CI systems in developing countries. CICGM² is a maturity model that contains various cyber governance aspects – including aspects of cybersecurity awareness and capacity building. The following section will describe how the cybersecurity awareness section of the CICGM² was developed and how it can be utilized to measure and manage the level of cybersecurity awareness capacity within the CIs in developing countries.

As indicated in previous paragraphs insufficient cybersecurity awareness capacities coupled to evolving social engineering techniques is a major threat to the information systems of CIs. To contextualise this section, a brief synopsis of social engineering will ensure a common point of departure.

According to Hijji and Alam (2021) social engineering (SE) is a method commonly used by hackers and cybercriminals to build strategies aimed at misleading persons into permitting them access to a system illegally or even legally? Their primary aim is to get access to computer networks, sensitive data and information by circumventing all technologies and firewalls (Hijji and Alam, 2021). If the objective of the social engineering attacks relates to money threat actors commonly employ phishing techniques in ransomware attacks to introduce malicious code into a victim's computer or network system. This code encrypts the system, rendering the data inaccessible to the victim. The attacker then demands a monetary payment in exchange for the decryption key needed to restore access to the compromised files and data (Hijji and Alam, 2021).

Measuring and improving the cybersecurity awareness capacity of employees at CIs in developing countries could be a challenge if there are no clear progression and/or maturity structures in place. A study conducted in 2022 which investigated the resilience of CIs in developing countries found that the economic growth, measured in terms of a country's Gross Domestic Product (GDP), is directly affected by the critical infrastructure of the

country. In developing countries, the number one CI that is targeted, is infrastructure in the energy sector such as power plants (Khan Babar and Ali, 2022).

For example, as part of her cyber governance responsibility a national manager of a power station in a developing country wants to improve the facility's cybersecurity awareness capacity by determining the CI's maturity level in terms of identifying cyberattacks through social engineering - the risk that was explained above. The CICGM² will initially assist the manager by providing a detailed assessment of the current state of affairs at the CI in terms of its cybersecurity awareness capacity level. The CICGM² model will then highlight the criteria or indicators for the different cyber governance maturity levels in terms of the employees' cybersecurity awareness capacities. These capacities will assist in identifying social engineering and other attacks on a *Strategic Governance Level* (the level of the CI in the example). The CICGM² will provide specific indicators under maturity levels ranging from *S0 to S4* under the *Identify Function* linked to the *Awareness Component* as indicated in Figure 3.

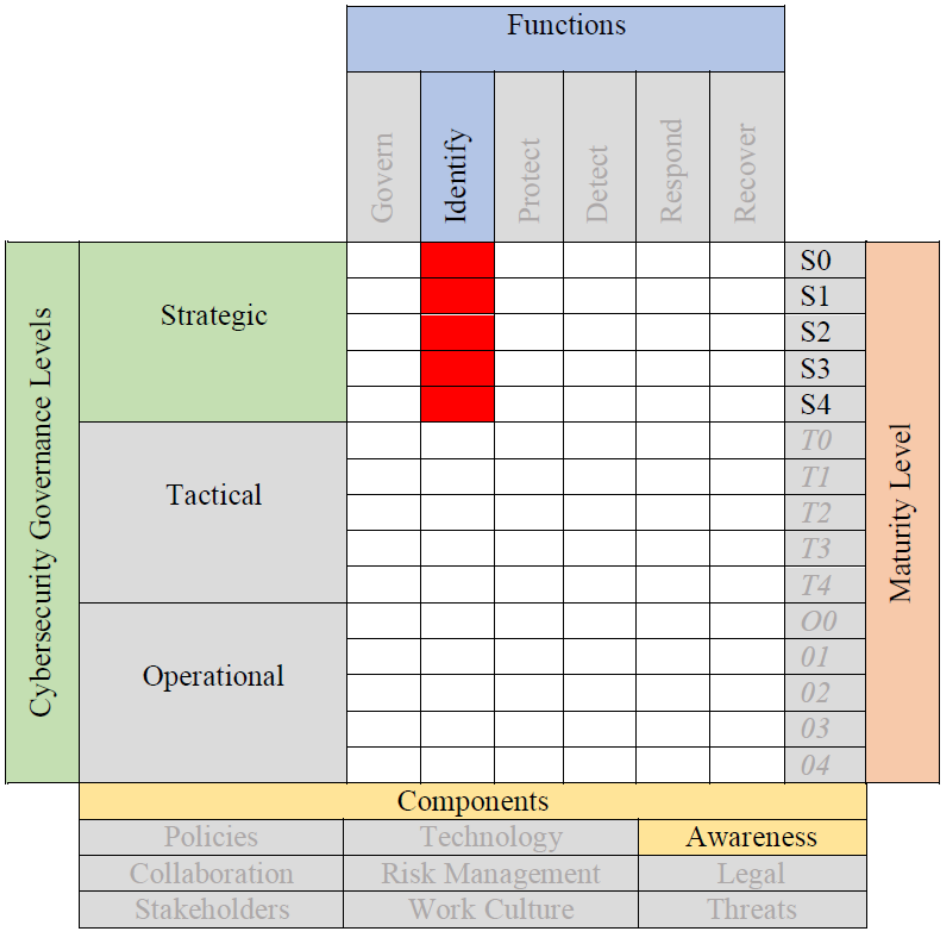

Figure 3: Measuring CIs Cyber Governance Maturity in Terms of Cybersecurity Awareness (Author)

If we zoom into the specific criteria for the cyber governance maturity levels for cybersecurity awareness of a CI on a *Strategic Level* the indicators could be as depicted in Figure 4 below.

Function: Identify			
Cybersecurity Governance Level: Strategic	Is there a cybersecurity awareness program at the CI? Do employees know the procedure to report any cybersecurity related issues? Is cybersecurity awareness training part of new employees' induction?	S0	Maturity Level
	Have employees in critical positions undergone CI-specific cybersecurity awareness training? Have external service providers undergone CI-specific cybersecurity awareness training?	S1	
	Are there continuous awareness campaigns on evolving cyber threats, potential cyberattacks, and system vulnerabilities? Are cybersecurity breaches at other CIs communicated to create awareness?	S2	
	Have the cybersecurity awareness of employees been tested?	S3	
	Is cybersecurity awareness capacity building prioritised in the Strategic Plan of the CI?	S4	
Component: Awareness			

Figure 4: Criteria for cybersecurity awareness maturity levels of a CI on Strategic Level (Author)

The indicators or criteria listed in Figure 4 provide indicators to guide the manager on the process to improve or upgrade the CI's cybersecurity awareness component to the next maturity level. If all the requirements of a specific maturity level are not reached, it follows that the CI's cyber governance maturity level for that specific function and component stays on the lower level.

In practise a CI can meet cybersecurity awareness capacity criteria in different maturity levels, but in order to progress from a lower level to the next level, all the criteria for the lower maturity level must be met. We can refer to this as a sequential progression system and the maturity criteria for the CICGM² is specifically designed in such a way that the lowest maturity levels start with the most basic requirements for a specific function that must be performed in terms of a specific component. It follows that higher levels of maturity include more complex and detailed indicators. As the CI progress from one level to another in various components, the cybersecurity governance of the CI automatically matures or improves. This is why the CICGM² is ideal for CIs in developing countries since it capacitates managers on different levels by dismembering and presenting cybersecurity governance aspects in a non-technical and easy-to-understand style. The end result is a more competent workforce as well as a more cyber secure CI facility.

6. Conclusion

The primary goal of CICGM² is to enhance cyber governance in CI within developing countries. By incorporating cyber governance maturity level standards across different governance levels, linked to specific functions and governance components, the model aims to provide CI stakeholders with clear expectations, indicators, and methodologies to advance from one maturity level to the next (De Bruin, 2018). Currently, CICGM²'s distinct focus on cyber governance maturity sets it apart from other existing models. However, a comprehensive comparison with other cybersecurity governance frameworks will only be feasible once the CICGM² has been fully developed and tested. Since the CICGM² is still in development, its cyber governance maturity level standards have not yet been finalized. A critical evaluation will only be possible after the release of the final draft version. At that point, industry experts will be engaged to assess the CICGM² in a real-world environment.

References

enisa Threat Landscape 2023. Attiki Greece: European Union Agency For Cybersecurity.

Admass, W. S., Munaye, Y.Y., Diro, A.A. 2024. Cyber Security: State Of The Art, Challenges And Future Directions. *Cyber Security And Applications,* 2**,** 100031-100031.

Ccm 2021. Cybersecurity Capacity Maturity Model For Nations 2021 Edition. United Kingdom: The Global Cyber Security Capacity Centre.

Chowdhury, N., Nystad, E., Reegård, K. & Gkioulos, V. 2022. Cybersecurity Training In Norwegian Critical Infrastructure Companies. *International Journal Of Safety And Security Engineering,* 12**,** 299-310.

Cis. 2021. *Critical Security Controls* [Online]. Center For Internet Security. Available: Https://Learn.Cisecurity.Org/Cis-Controls-V8-Guide-Pdf [Accessed May 23 2024].

De Bruin, R. 2018. *A Maturity Framework For Cybersecurity Governance.* Phd Of Science, University Of Johannesburg.

Dutton, W., Creese, S., Shillair, R. & Bada, M. 2019. Cybersecurity Capacity: Does It Matter? *Journal Of Information Policy,* Volume 9.

European, U. 2022. European Union Directive 2022/2557. *In:* Union, T. E. (Ed.). The European Union.

Hijji, M. & Alam, G. 2021. A Multivocal Literature Review On Growing Social Engineering Based Cyber-Attacks/Threats During The Covid-19 Pandemic: Challenges And Prospective Solutions. *Ieee Access,* 9**,** 7152-7169.

Khan Babar, A. H. & Ali, Y. 2022. Framework Construction For Augmentation Of Resilience In Critical Infrastructure: Developing Countries A Case In Point. *Technology In Society,* 68.

Kosutic, D. 2021. *What Is Iso 27001? A Beginner's Guide* [Online]. Available: Https://Advisera.Com/27001academy/What-Is-Iso-27001/ [Accessed May 05 2024].

Kosutic, D. 2024. *16 Steps For The Implementation Iso 27001* [Online]. Available: Https://Advisera.Com/27001academy/Iso-27001-Risk-Assessment-Treatment-Management/#Section1 [Accessed May 05 2024].

Lanure, M. A., Maulana, F. & Lubis, M. 2022. Assessment Of It Maturity Level And Roadmap Preparation For Improving Governance Based On Cobit 5 (Case Study: Xyz Company). *2022 1st International Conference On Information System & Information Technology (Icisit).*

Laubshtein, Y. 2023. Protecting Water And Sanitation Infrastructure From Cyberthreats: A Cybersecurity Study For Latin America And The Caribbean. Inter-American Development Bank.

Lehto, M. & Neittaanmaki, P. 2022. *Cyber-Attacks Against Critical Infrastructure*, Springer.

Melaku, H. M. 2023. A Dynamic And Adaptive Cybersecurity Governance Framework. *Journal Of Cybersecurity And Privacy,* 3**,** 327-350.

Nist 2024. The Nist Cybersecurity Framework (Csf) 2.0. National Institute Of Standards And Technology.

Oxford, T. 2022. Keeping The Country's Lights On. *The Public Technologist.* South Africa: Itweb.

Prakasha, K. 2022. Critical Information Infrastructure Protection Vulnerabilities, Threats And Challenges: A Critical Review. *Manipal Journal Of Science And Technology,* 7**,** 13.

Rabii, A., Assoul, S., Ouazzani, T., Khadija, R. 2020. Information And Cyber Security Maturity Models: A Systematic Literature Review. *Information & Computer Security,* 28**,** 627-644.

Rajaonah, B. 2017. A View Of Trust And Information System Security Under The Perspective Of Critical Infrastructure Protection. *Ingenierie Des Systemes D'information,* 22**,** 109-133.

Sontan, A. D. & Segun, S. V. 2024. Emerging Trends In Cybersecurity For Critical Infrastructure Protection: A Comprehensive Review. *Computer Science & It Research Journal,* 5**,** 576-593.

Spremić, M. & Šimunic, A. 2018. Cyber Security Challenges In Digital Economy. *Proceedings Of The World Congress On Engineering,* 1.

Tatar, U., Karabacak, B. & Gheorghe, A. 2016. An Assessment Model To Improve National Cyber Security Governance. *Proceedings Of The 11th International Conference On Cyber Warfare And Security, Iccws 2016***,** 312-319.

Tvaronavičienė, M., Plėta, T. & Della Casa, S. 2021. Cyber Security Management Model For Critical Infrastructure Protection. *International Scientific Conference "Contemporary Issues In Business, Management And Economics Engineering 2021".*

Urlainis, A., Ornai, D., Robert, L., Vilnay, O., Shohet, I.M. 2022. Loss And Damage Assessment In Critical Infrastructures Due To Extreme Events. *Safety Science,* 147**,** 105587-105587.

Veale, M. & Brown, I. 2020. Cybersecurity. *Internet Policy Review,* 9.

Zwarts, H., Du Toit, J. & Von Solms, B. A Cyber-Diplomacy And Cybersecurity Awareness Framework (Cdaf) For Developing Countries. 21st European Conference On Cyber Warfare And Security, 2022 University Of Chester. Academic Conferences International Limited, 469.

Zwarts, H., Du Toit, J. & Von Solms, B. 2025. Towards A Cybersecurity Governance Maturity Model For Critical Infrastructures In Developing Countries. *13th Computing Conference 2025.* London.