The Development of Critical Infrastructure Regulation in the Republic of South Africa[1]

Tibor Polonyi[2], Endre Szűcs[3]

Abstract:

The critical infrastructure regulation of the Republic of South Africa has undergone a significant transformation, from the introduction of the National Key Point Act (NKPA) in 1980 to the enactment of the Critical Infrastructure Protection Act (CIPA) in 2019. Over the course of nearly 40 years, the political and social changes within the country, alongside global developments affecting critical infrastructures, have clearly driven the regulatory environment in a positive direction. In this study, the CMMI (Capability Maturity Model Integration) theoretical framework is applied to examine, in a practical manner, the main characteristics of both pieces of legislation, as well as the critical events that occurred during the period between them. The analysis focused on four protective dimensions — risk management, responsibility, oversight, and incident management — to determine the maturity level of the relevant processes. The results demonstrate a clear paradigm shift: the previous ad hoc, single-decision-maker approach has been replaced by a transparent, shared-responsibility model supported by a well-organised institutional framework. The underlying philosophy has moved from static protection to maintaining service continuity. The technically narrow, physical-security-only approach has been superseded by a risk assessment-based framework that applies international standards, raising the process maturity from the initial ad hoc level to an organisationally defined and managed level.

Keywords:
Risk Management; Maturity Model; Resilience; Service Continuity; CIPA; Republic of South Africa.

[1] DOI: 10.12700/jceeas.2026.6.3.543

[2] PhD-student, Óbuda University, Doctoral School of Safety and Security Sciences, Budapest, Hungary; ORCID: 0009-0007-6724-8106; polonyi@dsc.hu.
[3] Co-Author, University Lecturer, Óbuda University, Donát Bánki Faculty of Mechanical and Safety Engineering, Budapest, Hungary; ORCID: 0000-0003-2818-262X; szucs.endre@bgk.uni-obuda.hu.

Introduction

Critical infrastructure (hereinafter CI) refers to the assets, systems, networks, and services that are essential for the functioning of society and the economy. Any disruption, reduction in efficiency, or complete failure of these systems has serious consequences for society and poses a threat to national security and stability.

From an international perspective, EU regulation provides useful reference point. EU Directive 2022/2557 defines critical entities as organisations whose disruption would affect the whole of society and its economic functioning. Similarly, EU Directive 2022/2555, known as NIS2, recognises the systemic importance of networks and information systems that serve these critical entities. (Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on Measures for a High Common Level of Cybersecurity across the Union, Amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and Repealing Directive (EU) 2016/1148 (NIS 2 Directive) (Text with EEA Relevance), 2022)

Although the legal language of the Republic of South Africa differs, the main directions and meaning are essentially the same. The National Key Point Act 102 of 1980 (hereinafter NKPA) focused primarily on the physical protection of designated strategic assets, while the Critical Infrastructure Protection Act 8 of 2019 (hereinafter CIPA) introduced a risk-based approach and institutional oversight. (Critical Infrastructure Protection Act 8 of 2019 (*Critical Infrastructure Protection Act 8 of 2019 (English / isiXhosa) | South African Government*, n.d.)

The political and social changes that took place in the Republic of South Africa revealed the extent to which critical infrastructures are vulnerable. Following the fall of the Apartheid regime, neglected or poorly managed development projects and organisational shortcomings further deepened the crisis in supply systems. For this reason, it is important to examine scientifically the processes and circumstances that led to the development of the new regulation.

The aim of this article is to carry out a comparative analysis of the NKPA and CIPA regulations by determining maturity levels, thereby contributing to a deeper understanding of the South African reforms.

Methodology

To objectively evaluate South African critical infrastructure regulation, the CMMI (Capability Maturity Model Integration) framework was applied. Although CMMI was originally developed for auditing software development processes, its adaptability makes it suitable for measuring the process maturity of complex protective systems. The fundamental premise of the methodology is that the effectiveness of a national security strategy depends not only on the content of legislative requirements, but also on the predictability, repeatability, and manageability of the underlying processes. The model distinguishes five incremental maturity levels. Level 1 is the ad hoc level, where processes are unpredictable and essentially reactive. At Level 2 (Managed), individual processes are planned and controlled, while at Level 3 (Defined), processes are standardised at

the organisational level and are clear and proactive. Level 4 (Quantitatively Managed) features controlled processes with built-in measurement points, and at the highest Level 5 (Optimising), the focus shifts to continuous improvement and innovation. (*CMMI Institute - CMMI Levels of Capability and Performance*, n.d.) The general CMMI model is illustrated in Figure 1.

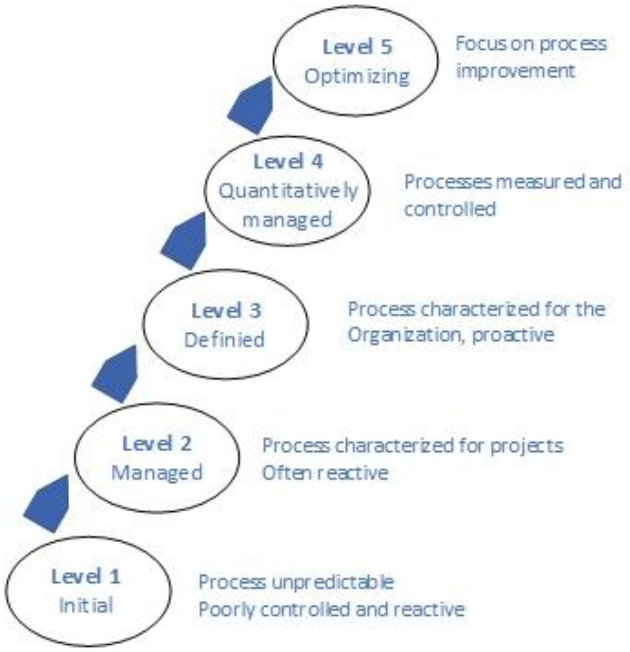


Figure 1: The five-level CMMI general model (Al-Sai et al., 2019), own compilation, 2026).

Using this theoretical framework in practice, the maturity of the NKPA and CIPA regulations was examined and compared across four protective dimensions. To identify the maturity levels, the following areas were selected as the main subjects of investigation: risk management methodology, delegation of responsibilities, system-level oversight (audit), and incident management in crisis situations.

Application and Results

Historical Context and Regulatory Background

The first critical infrastructure regulation was introduced in the Republic of South Africa in 1980. The National Key Point Act 102 of 1980 established the designation of critical infrastructures, placing related responsibilities under the authority of the Chief of Police department through single-person decision-making. The designated critical infrastructures, or „key points" as the legislation called them, were treated in isolation, with focus exclusively on the security of each individual site. The Act declared centralised ministerial authority and a protection-centred approach (defence-based logic), while granting the Minister broad discretionary powers. Additionally, it was characterised by a primacy of secrecy and a non-transparent structure. Ministerial decisions and designations were not made public and were not subject to transparent oversight. The system was entirely built on location-based identification, with the physical location of

a given infrastructure serving as the key point. It did not categorise critical entities by risk, and the concept of resilience was entirely absent.

The system's oversight was essentially determined by designations and ministerial authority, neither of which was publicly accessible; transparency and openness were absent from the system. Both accountability and transparency were lacking: the legislation did not include any reporting obligation to the legislature and, furthermore, it criminalised the disclosure of information. (*National Key Points Act 102 of 1980 | South African Government*, n.d.)

In practice, this meant, for example, that in the energy sector the primary principle was compliance with security requirements, while ports and logistical infrastructures were mainly governed by secrecy rules. This approach clearly stands in contrast to modern resilience development: it does not address hybrid or cyber threats, vulnerabilities in supply chains, or the recommendations of modern global infrastructure protection frameworks.

Significant changes took place in the country after the fall of the Apartheid regime. In 1996, a new Constitution was adopted, laying entirely new foundations for the country's political system. The new Constitution established, among other things, new legal frameworks, transparency, and the right of access to information; however, the NKPA remained in force. (*The Constitution of the Republic of South Africa | South African Government*, n.d.)

The period from 1996 to 2019 was characterised by political change, while infrastructure reform did not take place. Yet a number of global developments during this time led other countries to fundamentally reconsider their approaches to critical infrastructure. Most significantly, the terrorist attacks of 11 September 2001 gave rise to specific demands and concrete measures focused on the protection of technologies and installations. In this international context, one of the first pieces of legislation was EU Directive 2008/114/EC on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection. (Council Directive 2008/114/EC of 8 December 2008 on the Identification and Designation of European Critical Infrastructures and the Assessment of the Need to Improve Their Protection (Text with EEA Relevance), 2008)

In the meantime, the widespread adoption of digitalisation, the rapid growth of telecommunications and information technology, and the related internet-based services — particularly in the telecommunications and banking sectors — drew attention to the growing threat of cybercrime.

In the Republic of South Africa, a major power outage was recorded during 2007–2008, as documented in ESKOM's reports — a further warning sign that the existing regulation needed to be revised. This „ugly fact" highlighted that the NKPA was not capable of addressing supply chain vulnerabilities. (*ESKOM 2003-2012 - Heritage*, 2021)

In 2016, at the Warsaw Summit, NATO set out baseline requirements for national resilience and the protection of critical infrastructures. (North Atlantic Treaty Organization [NATO], 2016)

Finally, in 2019, after a lengthy consultation process, the Critical Infrastructure Protection Act (CIPA) was adopted, fundamentally transforming critical infrastructure regulation within the country. (Critical Infrastructure Protection Act 8 of 2019 (*Critical Infrastructure Protection Act 8 of 2019 (English / isiXhosa) | South African Government*, n.d.) CIPA represented a major change in the protection of critical infrastructures. The most important shift was that it moved away from the exclusively site-based protection of the NKPA, placing the focus on function instead. Secrecy was replaced by transparency and the use of a defined framework, as well as a risk management system. The key element of the new regulation is the Council, which acts as an expert advisory body supporting the designation of critical infrastructures and the functioning of their risk management.

The new regulation places critical infrastructures within a structured framework, provides definitions for their identification, and establishes a transparent system. Critical infrastructure is approached from the perspective of service continuity, recognising that the functioning of modern society is based on interconnected, networked systems. This type of interdependency is illustrated in Figure 2.

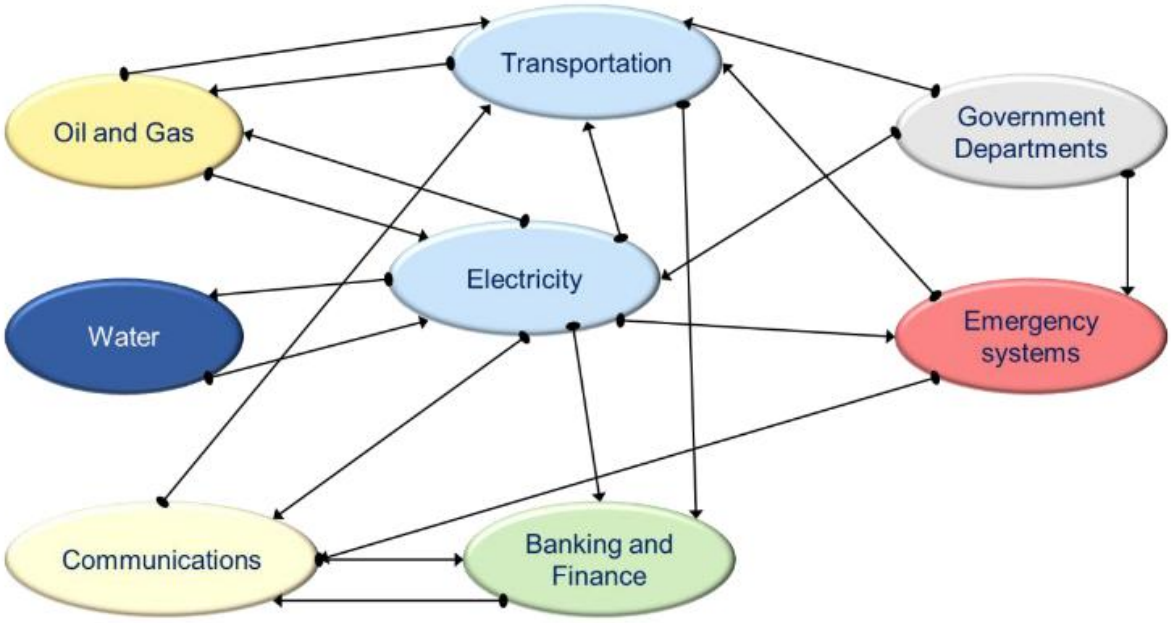


Figure 2.: Example of CI interdependence (Gonçalves & Serfontein, 2022).

In his publication, Goncalves illustrates this mutual dependency by noting that, for example, electricity is required for the operation of railways and transport, which in turn carries the energy sources (e.g. coal) needed for electricity generation. (Gonçalves & Serfontein, 2022) Critical infrastructure is no longer limited to a single key point, building, or facility; it may also encompass an entire supply chain or digital network.

The primary task of the Critical Infrastructure Council is, as an expert body, to ensure that decisions affecting critical infrastructures are made on a professional rather than a political basis. At the same time, the Council's role has grown in importance with regard to the designation of infrastructures and the maintenance of security standards. Single-

person decision-making has clearly been replaced by a collective, professionally grounded approach. Thanks to the Council's work, transparency prevails over secrecy.

The significance of transparency lies in the fact that it makes the use of public resources verifiable, renders the system auditable, and allows for the detection of corruption. This greatly increases public trust and enables broad, objective communication with society.

A significant innovation in the regulation is that it includes the owners of privately held critical infrastructure elements in the protection process, requiring security audits and the preparation of protection plans, the costs of which are borne by the owners. Protection is a shared interest and responsibility, with the state providing expert guidance on addressing threats.

With regard to critical infrastructures, cyber threats are now just as relevant as physical ones. Since computer networks were barely a consideration when the NKPA was drafted in 1980, the interconnected computing systems that now underpin infrastructure operations have become critically important. The new regulation creates the opportunity for protection against modern technological threats by ensuring the security of data and control systems. (*Critical Infrastructure Protection Act 8 of 2019 (English / isiXhosa) | South African Government*, n.d.)

Maturity Analysis Based on the CMMI Model

By comparing the frameworks established by the NKPA and CIPA, the model was used to examine and identify the maturity levels represented by each regulation. During the development of the CMMI model, four areas of critical infrastructure protection were examined, and the model was assembled on the basis of this analysis. The examination began with the identification of the analytical dimensions — defining those areas whose analysis would allow the maturity model to be constructed. Four areas were focused on: risk management, responsibility, oversight, and incident management.

The first area examined is the methodology of risk management as addressed by the regulation. The key question is the basis on which threats are identified and infrastructures are classified — whether such decisions are subjective and made by a single person, or whether they follow some transparent system. On this basis, the NKPA was characterised by ad hoc decision-making (Level 1), while CIPA clearly applies standardised methods, using risk assessment and objective indicators for classification, such as the extent and impact of economic damage and the probability of an incident occurring for a given infrastructure element. In the case of CIPA, this approach corresponds to Level 3 of the maturity model.

Regarding responsibility, the NKPA contains no provision that defines how tasks and responsibilities are allocated or delegated for individual critical infrastructure elements. In contrast, CIPA clearly involves the owners of privately held infrastructure elements in the protection process, delegates the task of developing protection plans, defines obligations, and establishes the foundations of process management. From the perspective of the model, this represents one of the most significant advances: organisational-level regulation and oversight are achieved, which is an element of

process management at Levels 2 and 3. Under the NKPA, responsibility was limited to the local, site-level organisations (e.g. on-site security), and was not defined at the system level.

From the perspective of oversight, the CIPA framework sets out audits and reporting obligations, ensuring continuous control over infrastructure protection. This feedback mechanism is one of the most important elements at Level 3 and provides the foundation for progression in the development phase. The NKPA, by contrast, concentrated solely on protection and contained none of the elements required for oversight. Inspections themselves were classified, and owners were unable to prepare for them in advance.

In terms of incident management, the NKPA focused exclusively on protection and provided no guidance on the restoration of operations. Since it concentrated only on prevention, incident management — what to do during an attack and how to restore the service — was entirely dependent on the preparedness of local personnel. CIPA clearly points towards proactive planning: the mandatory preparation and practice of emergency plans ensures that critical infrastructure services can be maintained, and that recovery does not need to start from scratch in the event of an attack. The process is therefore defined and proactive, which corresponds to Level 3 in the case of CIPA. A comprehensive comparison of the analysis results and maturity levels is presented in Figure 3.

Dimension	NKPA - Level 1	CIPA - Level 3
Risk management	Ad-hoc, one-man-based decision by the minister, classified,	Well definied and standardized, based on objective economical and social indicators
Responsibility	Isolated, localized, locally managed	Involve the private ownership, delegating obligations
Oversight, Audit	Secret, unknown methodology, lack of control and transparency	Legally regulated, mandatory audits and reporting systems
Incident management	Reactive, phisycal protection in focus, lack of recovery policies	Maintaining continuity, proactive emergency plans

Figure 3.: Comparison table of NKPA and CIPA process maturity along CMMI dimensions (own compilation, 2026).

Based on the results, the CIPA regulation is clearly two maturity levels above the NKPA. Further efforts are needed for critical infrastructure regulation to advance to Level 4. In practice, however, the theoretical Level 3 has not yet been fully achieved, as operational implementation still faces challenges. The frameworks established by CIPA are forward-looking in this regard: maintaining resilience and service continuity is a key element in addressing both physical and cyber threats. In order to progress to the quantitatively managed level of the maturity model, additional data-driven measurement processes need to be introduced into South African critical infrastructure regulation.

Conclusion

South African critical infrastructure regulation has undergone a clear and significant development over the past nearly 40 years. The introduction of CIPA marked a paradigm shift, replacing the previous location-based protective focus with a service continuity perspective. The new regulation successfully broke with the ad hoc, law-enforcement-oriented, and opaque logic of the NKPA, and defined a management-oriented, proactive resilience framework that aligns with the modern EU protective directives (CER, NIS2). CIPA established the regulatory framework for the service continuity-based operation of critical infrastructures. The risk-based approach to critical infrastructures, their classification, the preparation of security plans, and their continuous auditing all enable process improvement and the correction of non-conformities.

The research also highlighted that the theoretical Level 3 maturity has not yet been fully achieved in operational practice: the development and quality of infrastructures still face challenges (e.g. the electricity grid). In practice, this presents significant implementation and funding tasks that remain to be resolved.

This structured process system provides a stable foundation for the South African regulatory framework to develop further in the future. In order for the protective system to reach Level 4 as defined by CMMI (Quantitatively Managed), future research should focus on how quantifiable measurement processes, performance indicators, and monitoring systems — whose introduction and operation are essential for achieving the highest level of resilience — can be developed and implemented.

Conflict of Interest

The authors hereby declare that they have no financial interest in this manuscript.

Notes on Contributors

Tibor Polonyi is a Ph.D. student at the Doctoral School of Security Sciences at Óbuda University, as well as a business and security technology specialist. His professional experience includes serving as Business Development Director at DSC Hungária Kft., where he specializes in physical security, security system design, CCTV, and project management.

Dr. Endre Szűcs is an assistant professor at the Institute of Mechanical Engineering, Security Sciences, and Cyber Defense at the Donát Bánki Faculty of Mechanical and Safety Engineering at Óbuda University, as well as a thesis advisor at the Doctoral School of Security Sciences. He is a mechanical engineer, engineering educator, and certified safety engineer, and holds a Ph.D. in military sciences (2006, Miklós Zrínyi National Defense University). Research areas: The application of renewable energy sources in security technology, the history of security technology, and military and security systems.

References

Al-Sai, Z., Abdullah, R., & Husin, H. (2019). *A Review on Big Data Maturity Models* (p. 161). https://doi.org/10.1109/JEEIT.2019.8717398

CMMI Institute—CMMI Levels of Capability and Performance. (n.d.). Retrieved April 19, 2026 from https://cmmiinstitute.com/learning/appraisals/levels

Council Directive 2008/114/EC of 8 December 2008 on the Identification and Designation of European Critical Infrastructures and the Assessment of the Need to Improve Their Protection (Text with EEA Relevance), CONSIL, 345 OJ L (2008). Retrieved April 19, 2026 from http://data.europa.eu/eli/dir/2008/114/oj

Critical Infrastructure Protection Act 8 of 2019 (English / isiXhosa) | South African Government. (n.d.). Retrieved April 19, 2026 from https://www.gov.za/documents/acts/critical-infrastructure-protection-act-8-2019-english-isixhosa-28-nov-2019

Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on Measures for a High Common Level of Cybersecurity across the Union, Amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and Repealing Directive (EU) 2016/1148 (NIS 2 Directive) (Text with EEA Relevance), EP, CONSIL, 333 OJ L (2022). Retrieved April 19, 2026 from http://data.europa.eu/eli/dir/2022/2555/oj

ESKOM 2003-2012—Heritage. (2021, November 2). Retrieved April 19, 2026 from https://www.eskom.co.za/heritage/history-in-decades/eskom-2003-2012/

Gonçalves, D. P., & Serfontein, C. J. (2022). *Systemic approaches to critical infrastructure risk and security capabilities*. Retrieved April 19, 2026 from http://hdl.handle.net/10204/12557

National Key Points Act 102 of 1980 | South African Government. (n.d.). Retrieved April 19, 2026 from https://www.gov.za/documents/national-key-points-act-24-mar-2015-1016

The Constitution of the Republic of South Africa | South African Government. (n.d.). R Retrieved April 19, 2026 from https://www.gov.za/documents/constitution/constitution-republic-south-africa-04-feb-1997

North Atlantic Treaty Organization. (2016. July 9.) *Warsaw Summit Communiqué*. [Press Release] NATO. Retrieved April 19, 2026 from https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2016/07/09/warsaw-summit-communique

Figures

1. Figure: The five-level CMMI general model (Al-Sai et al., 2019), own compilation, 2026)
2. Figure: Example of CI interdependence (Gonçalves & Serfontein, 2022)
3. Figure: Comparison table of NKPA and CIPA process maturity along CMMI dimensions (own compilation, 2026)