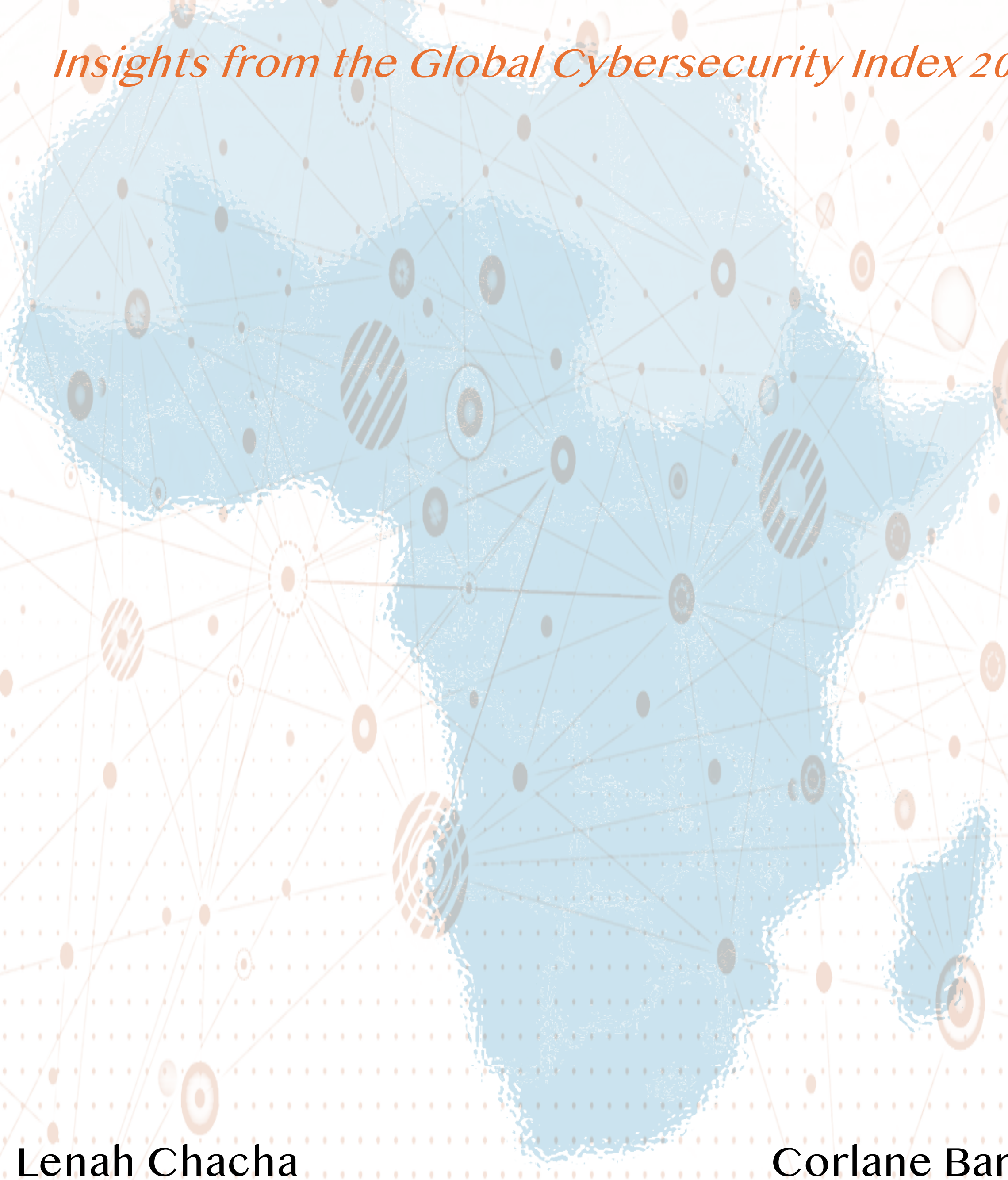
Mapping Africa's Cybersecurity Development

Insights from the Global Cybersecurity Index 2024



Lenah Chacha

Corlane Barclay

December 2024

Mapping Africa's Cybersecurity Development

Insights from the Global Cybersecurity Index 2024

ISBN 978-976-97440-1-1 (Electronic version)

Table of Contents

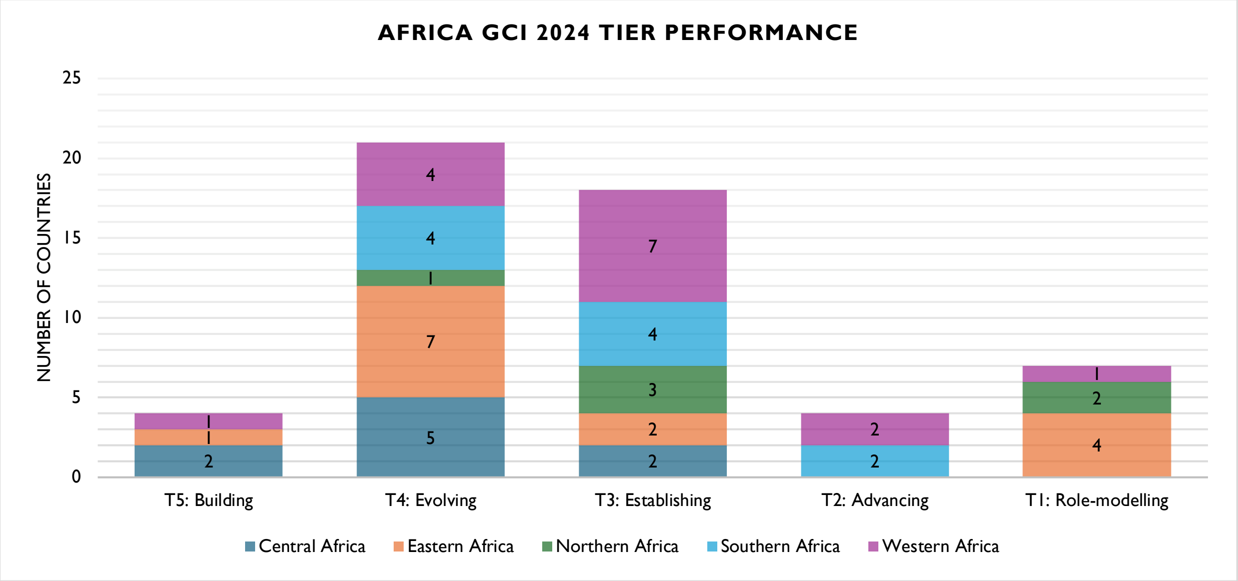
TABLE OF FIGURES

Report Abstract

The report provides a comprehensive review of cybersecurity commitments from Africa's national and regional perspectives. It analyses the recently released ITU Global Cybersecurity Index (GCI) 2024 report and its data, identifies major trends and provides insights for governments, policymakers and other stakeholders on how to adopt and effectively leverage good cybersecurity practices and measures, particularly as these countries embark on their digital development agenda.

The findings underline the urgent need to continue to tackle digital and cybersecurity capacity/capability divides among African countries as these economies grapple with rapidly escalating cybercrime and cyber threats, especially with the impact of artificial intelligence and other technological advances on cybercrime and threat models.

FIGURE 1: TIER PERFORMANCE BY REGIONS OF AFRICA



GCI 2024 Performance by Regions (Figure 1)

- Countries are predominantly at the Evolving and Establishing stages of leading and implementing government-led cybersecurity measures at the national level.
- Only Eastern, Northern and Western Africa have countries at the Role-modelling level of cybersecurity commitment. Eastern Africa leads with four countries, followed by Northern and Western Africa. The countries at this level are Egypt, Mauritius, Ghana, Tanzania, Kenya, Rwanda and Morocco.
- Two regions, Southern and Western Africa, account for the four countries at the Advancing level of cybersecurity commitment. These countries are Zambia, Benin, Togo and South Africa.
- Most countries in Central Africa are in the formative stages of cybersecurity development, demonstrating presence only at the Building, Evolving and Establishing stages.
- Only Central, Eastern, and Western Africa have at least one country at the Building level of cybersecurity commitment. These countries include Burundi, Guinea-Bissau, Central African Republic and Eritrea.

Progress in Cybersecurity

- Since the previous GCI edition, many countries in all regions, in particular, the current Establishing (T3) performers, experienced growth in the extent of their government-led actions to combat cybercrime and cybersecurity risks.
- Eswatini, Togo, and the Democratic Republic of Congo demonstrated the highest level of progress, with each country achieving between 51 and 62 points out of 100.
- Several countries experienced negative growth, including Tunisia, Guinea-Bissau and Nigeria. In some cases, this may be explained by factors, such as the availability and accessibility of relevant data to demonstrate cybersecurity commitments.

Role-modelling Activities

- Role-modelling actions in the continent are evident in all cybersecurity pillars. Some of these measures include bilateral agreements to build capacities in technical responses, parties and signatories to multilateral agreements, regional cybersecurity frameworks to support the development of national cybersecurity strategies, cybersecurity awareness programs targeting and empowering the youth, and the coming into effect of new and revised cybercrime, cybersecurity, privacy and data protection, and other related laws and frameworks.

Comparative Analysis of Africa and the Americas' GCI 2024 Performance

- Central Africa and the Caribbean reflect the lowest levels of cybersecurity commitment. A unified approach or similar tactics can be considered to address significant and comparable gaps.
- North America, comprising the USA and Canada, demonstrates the highest level of cybersecurity commitment on average, followed by Northern Africa.
- Latin America, Eastern, Northern, Southern and Western Africa demonstrate similarities in commitment trends across the cybersecurity pillars with relative strengths in legal, organisational and capacity development measures.

Policy Directions for Africa

- Tailored recommendations based on countries' tier performances are provided. These are centred on developing and strengthening cybercrime and cybersecurity regulatory frameworks, building capacities in cybersecurity to enable effective legal and enforcement responses to emerging risks, developing a strong cybersecurity workforce, and improving partnerships and cooperation at all levels, including increasing membership in regional and international cybersecurity treaties and agreements.
- Only 16 African countries, 29%, have ratified the Malabo Convention, and 13, or 24%, are signatories only. Despite the low participation, this represents a slightly higher percentage than participation in the Budapest Convention. This status calls for increased leveraging of multilateral cybersecurity cooperation to help boost information sharing and capacity building.
- Ensuring that cybersecurity becomes and remains a top priority is imperative for all countries in Africa, and in other regions, such as the Americas, as they navigate digital development and other national priorities.

"Cybersecurity must remain a major concern for African nations as a matter of national sovereignty and economic prosperity" - President Faure Gnassingbé, Togo

Introduction

The recent global reports on ICT development[1] and e-government development[2] underline that Africa is experiencing continued growth in digital development. While disparities exist, many countries on the continent continue to make meaningful digital progress as a result of increased investments and prioritising certain SDGs in areas such as e-government services, digital identity systems, and mobile and internet connectivity. At the same time, there is an escalating wave of cybercrime across the continent, including ransomware, business email compromise, and other forms of online scams[3]. The financial impact of these cybercrimes and threats was estimated to be more than US$ 4 billion annually[4]. These conditions call for more comprehensive and proactive approaches to improve the security and resilience of national digital infrastructures, develop cyber capabilities and combat cybersecurity risks. As a result, increased attention to digital privacy and security at the national and regional levels is required to help foster socio-economic development and sovereignty.

The International Telecommunication Union (ITU) Global Cybersecurity Index (GCI) 2024 revealed that the global average country score is 65.7 out of 100, a 27% growth since the previous edition[5]. This indicates that, in general, countries are making progress in their cybersecurity actions and commitments. A closer look at the data shows that more than half of the African nations remain below the global average. This is despite significant advancements in government-led cybersecurity measures and activities across many African countries. This trend highlights the need for increased focus on addressing national privacy and cybersecurity risks to build trust in digital services. Additionally, it underscores that any digital development agenda must be accompanied by a commensurate commitment to a comprehensive cybersecurity development agenda.

Against this background, this report seeks to amplify the GCI 2024 data and implications. We undertake a review of the 54 countries within the continent of Africa[6] to gain deeper insights into the diverse cybersecurity efforts and the extent of cybersecurity commitments at the national and regional levels. A comparative analysis of Africa and the Americas is also undertaken, which reveals similar levels of cybersecurity commitment in several areas and reinforces the need for priority actions in Central Africa and the Caribbean, in particular.

Our analysis uncovers gaps and opportunities to enhance cybersecurity commitments, country cybersecurity postures, and maturity at both national and regional levels. These insights are expected to guide the implementation of measures and actions necessary to strengthen government-led cybersecurity initiatives, thereby improving or maintaining cybersecurity commitments.

[1] ICT Development Index, https://www.itu.int/itu-d/reports/statistics/idi2024/

[2] E-Government Development Index, https://publicadministration.un.org/egovkb/en-us/Reports/UN-E-Government-Survey-2024

[3] INTERPOL African Cyberthreat Assessment Report 2024

[4] INTERPOL Africa Cyberthreat Assessment Report 2021

[5] https://www.itu.int/en/ITU-D/Cybersecurity/Documents/GCIv5/2401416_1b_Global-Cybersecurity-Index-E.pdf

[6] The Sahrawi Arab Democratic Republic, an African Union member state, was not part of the GCI and is excluded for this reason.

A Summary of the GCI

The GCI is a cybersecurity-related composite index that measures the commitment of countries to cybersecurity across five cybersecurity pillars[7], namely:

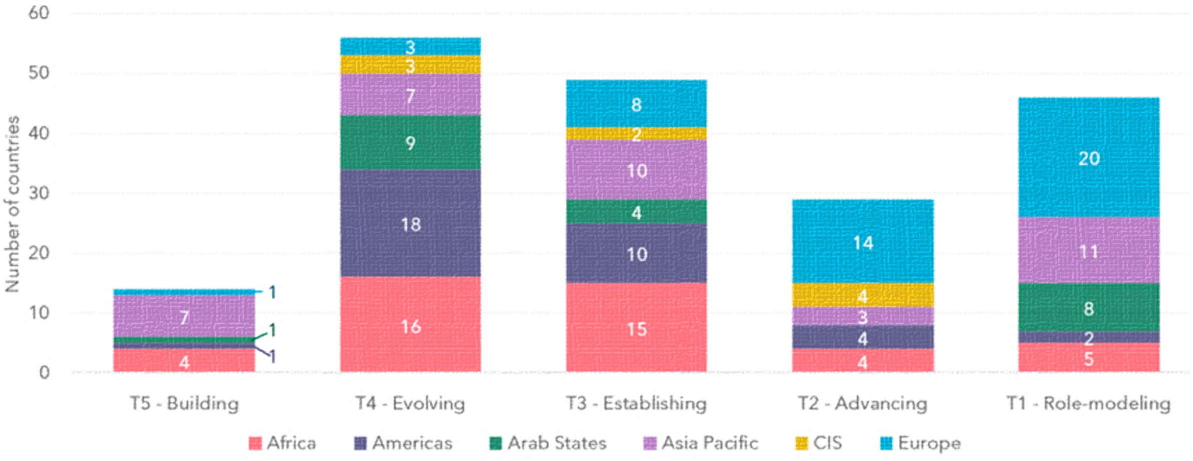
- **Legal**: Measures the laws and regulations on cybercrime and cybersecurity.
- **Technical**: Measures the implementation of technical capabilities through national and sector-specific agencies.
- **Organisational**: Measures national strategies, structures and institutions implementing cybersecurity.
- **Capacity Development**: Measures awareness campaigns, training, education and incentives for cybersecurity capacity development.
- **Cooperation**: Measures partnerships between agencies, firms and countries.

Therefore, cybersecurity commitments may be viewed as the totality of government-led actions and measures taken by a country to help combat cybercrime and manage cybersecurity risks within the framework of the five defined cybersecurity pillars.

A tiered model for measuring the level of cybersecurity commitment of countries was introduced in this fifth edition of the GCI. Each country's performance is measured across five tiers, with Tier 1 being the highest and Tier 5 being the lowest. The model is summarised as follows:

- Tier 1 (T1): Role-modelling - a country with 95 ≤ x ≤ 100 GCI score.
- Tier 2 (T2): Advancing - a country with 85 ≤ x < 95 GCI score.
- Tier 3 (T3): Establishing - a country with 55 ≤ x < 85 GCI score.
- Tier 4 (T4): Evolving - a country with 20 ≤ x < 55 GCI score.
- Tier 5 (T5): Building - a country with 0 ≤ x < 20 GCI score.

FIGURE 2: TIER PERFORMANCE BY GLOBAL REGION (GCI 2024)



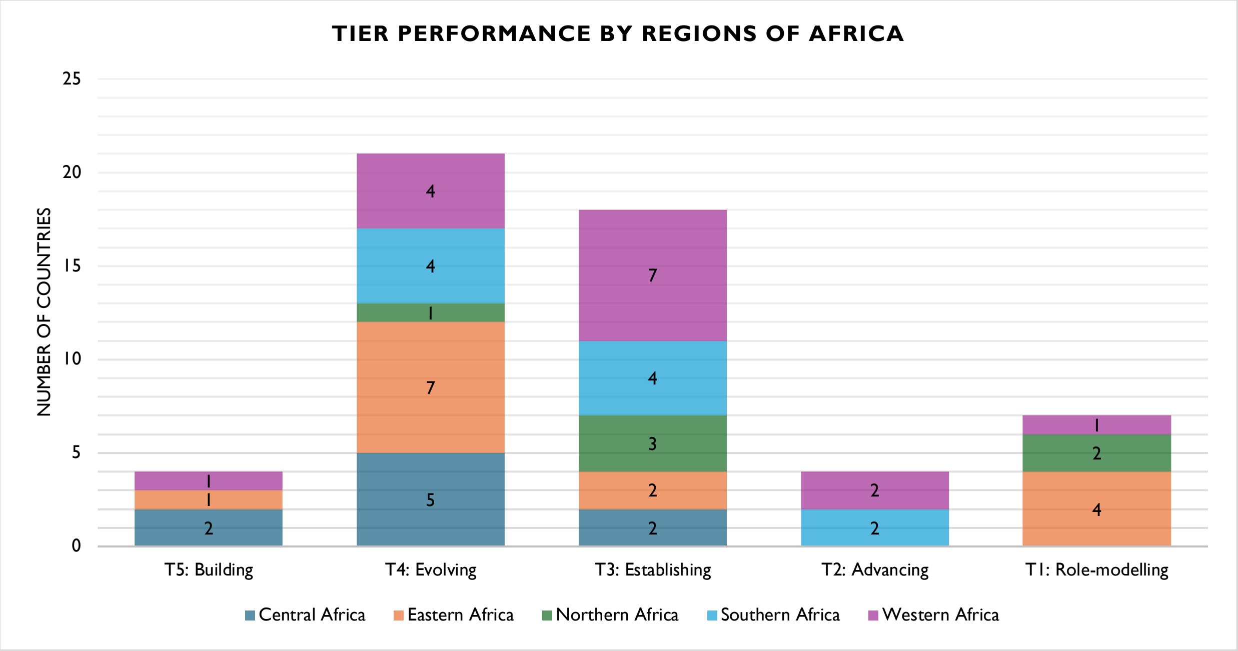
Source: ITU

[7] https://www.itu.int/en/ITU-D/Cybersecurity/Documents/GCIv5/2401416_1b_Global-Cybersecurity-Index-E.pdf

The tier performance across the six global regions (Figure 2), extracted from the GCI 2024 Report, highlights that the majority of global nations are at the Building, Evolving and Establishing stages of cybersecurity commitment while many countries in the Europe region are standouts in terms of relative commitment to cybersecurity. Africa has a presence in all stages, with most countries at the Evolving and Establishing stages[8].

We conduct a deeper examination of the performance of Africa[9] (Figure 3) by highlighting the tier performance of its five regions and 54 countries. The analysis highlights the disparities in the levels of cybersecurity commitments among countries and regions and the urgent need to prioritise greater cooperation as well as adopt more robust cybersecurity measures to combat risks and improve GCI scores.

FIGURE 3: TIER PERFORMANCE BY REGIONS OF AFRICA



Cybersecurity Commitment in Africa

The tier performance shows that Africa features varying levels of cybersecurity commitment, showcasing several leaders and many countries with growth potential, as illustrated in Figure 4. The regional classification of the African Union (AU)[10] is adopted while highlighting the difference in classification by the GCI.

T1 (Role-modelling): Seven countries, representing 13%, across three regions (Northern, Eastern and Western Africa) lead the continent in demonstrating a strong cybersecurity commitment to coordinated

[8] Adapted from C. Barclay, An Analysis of the GCI 2024: Progress, Challenges and Opportunities for the Caribbean, ISBN 978 976 97440 0 4

[9] Note: The Africa region in this report is distinct from the" Africa region" referred to in the GCI reports due to this report focusing on 54 countries in the continent.

[10] https://afripol.africa-union.org/member-states/

and government-driven actions across all five pillars and the majority of their indicators. These countries are Egypt, Mauritius, Ghana, Tanzania, Kenya, Rwanda and Morocco.

T2 (Advancing): Four countries, Zambia, Benin, Togo, and South Africa, representing 7.4%, demonstrate Advancing Levels of cybersecurity commitment by demonstrating strong commitments to coordinated and government-driven actions across the majority of pillars.

T3 (Establishing): 18 countries, representing 33.3%, across the regions are at the Establishing level by demonstrating a basic cybersecurity commitment to government-driven actions across a moderate number of pillars or indicators. These include Uganda, Nigeria, Tunisia and Malawi.

T4 (Evolving): 21 countries, representing 38.9% across the regions are at the Evolving stage, demonstrating basic cybersecurity commitment to government-driven actions across at least one pillar, or several indicators or sub-indicators. These include Cabo Verde, Seychelles, Chad and Sudan.

T5 (Building): Four countries, Burundi, Guinea-Bissau, Central African Republic and Eritrea, representing 7.4%, are at the initial stage of cybersecurity development by demonstrating basic cybersecurity commitment to government-driven actions across at least one indicator or sub-indicator. Eritrea is positioned at the lowest rank. The T5 ranking may be explained by factors such as limited accessibility to relevant data in the case of Eritrea[11] or being marred by civil wars and political instability in the cases of the Central African Republic and Burundi.

FIGURE 4: GCI 2024 CONTINENT RANKING

Rank	Country	ITU Region	AU Region	Tier Performance
1	Egypt	Arab States	Northern Africa	T1: Role-modelling
1	Mauritius	Africa	Eastern Africa	T1: Role-modelling
3	Ghana	Africa	Western Africa	T1: Role-modelling
4	Tanzania	Africa	Eastern Africa	T1: Role-modelling
5	Kenya	Africa	Eastern Africa	T1: Role-modelling
6	Rwanda	Africa	Eastern Africa	T1: Role-modelling
7	Morocco	Arab States	Northern Africa	T1: Role-modelling
8	Zambia	Africa	Southern Africa	T2: Advancing
9	Benin	Africa	Western Africa	T2: Advancing
10	Togo	Africa	Western Africa	T2: Advancing
11	South Africa	Africa	Southern Africa	T2: Advancing
12	Uganda	Africa	Eastern Africa	T3: Establishing
13	Nigeria	Africa	Western Africa	T3: Establishing
14	Tunisia	Arab States	Northern Africa	T3: Establishing
15	Malawi	Africa	Southern Africa	T3: Establishing

[11] Adapted from C. Barclay, An Analysis of the GCI 2024: Progress, Challenges and Opportunities for the Caribbean, ISBN 978 976 97440 0 4

Rank	Country	ITU Region	AU Region	Tier Performance
16	Eswatini	Africa	Southern Africa	T3: Establishing
17	Côte d'Ivoire	Africa	Western Africa	T3: Establishing
18	Botswana	Africa	Southern Africa	T3: Establishing
19	Ethiopia	Africa	Eastern Africa	T3: Establishing
20	Burkina Faso	Africa	Western Africa	T3: Establishing
21	Libya	Arab States	Northern Africa	T3: Establishing
22	Senegal	Africa	Western Africa	T3: Establishing
23	Mozambique	Africa	Southern Africa	T3: Establishing
24	Algeria	Arab States	Northern Africa	T3: Establishing
25	Cameroon	Africa	Central Africa	T3: Establishing
26	Gambia	Africa	Western Africa	T3: Establishing
27	Democratic Republic of Congo	Africa	Central Africa	T3: Establishing
28	Sierra Leone	Africa	Western Africa	T3: Establishing
29	Guinea	Africa	Western Africa	T3: Establishing
30	Cabo Verde	Africa	Western Africa	T4: Evolving
31	Seychelles	Africa	Eastern Africa	T4: Evolving
32	Chad	Africa	Central Africa	T4: Evolving
33	Sudan	Arab States	Eastern Africa	T4: Evolving
34	Niger	Africa	Western Africa	T4: Evolving
35	Gabon	Africa	Central Africa	T4: Evolving
36	Zimbabwe	Africa	Southern Africa	T4: Evolving
37	Angola	Africa	Southern Africa	T4: Evolving
38	Mauritania	Arab States	Northern Africa	T4: Evolving
39	Comoros	Arab States	Eastern Africa	T4: Evolving
40	Somalia	Arab States	Eastern Africa	T4: Evolving
41	Namibia	Africa	Southern Africa	T4: Evolving
42	South Sudan	Africa	Eastern Africa	T4: Evolving
43	Madagascar	Africa	Eastern Africa	T4: Evolving
44	Djibouti	Arab States	Eastern Africa	T4: Evolving
45	Lesotho	Africa	Southern Africa	T4: Evolving
46	Mali	Africa	Western Africa	T4: Evolving
47	Congo Republic	Africa	Central Africa	T4: Evolving
48	Equatorial Guinea	Africa	Central Africa	T4: Evolving
49	Liberia	Africa	Western Africa	T4: Evolving
50	São Tomé and Príncipe	Africa	Central Africa	T4: Evolving

Rank	Country	ITU Region	AU Region	Tier Performance
51	Burundi	Africa	Central Africa	T5: Building
52	Guinea-Bissau	Africa	Western Africa	T5: Building
53	Central African Republic	Africa	Central Africa	T5: Building
54	Eritrea	Africa	Eastern Africa	T5: Building

State of Progress in Cybersecurity

Since the previous edition, Africa has experienced a significant shift in cybersecurity commitment. Across the continent, numerous countries have made considerable strides in implementing cybersecurity measures and initiatives, as illustrated in Figure 5. Many of these countries have made significant strides across various cybersecurity pillars. For instance, the Democratic Republic of Congo and South Africa have seen their most substantial improvements in organisational measures. Gabon, Cabo Verde, and Comoros have made advances in legal measures. Ethiopia has strengthened its cooperation measures, while Togo has made notable progress in capacity development measures.

General Observations

- Eswatini, Togo, and the Democratic Republic of Congo stand out in cybersecurity progress, displaying the highest growth rates on the continent.
- Countries showing the most significant improvements in the Establishing and Evolving tiers include Malawi, Eswatini, Ethiopia, Libya, Mozambique, Algeria, Gambia, Democratic Republic of Congo, Sierra Leone, Guinea, and Togo.
- A high percentage (over 70%) of the current Establishing performers have made substantial progress since the previous GCI edition. Countries include Algeria, the Democratic Republic of Congo, Eswatini, and Ethiopia.
- Countries that have made little to no progress or have remained low performers since 2021 include Zimbabwe, Chad, Sudan, São Tomé and Príncipe, the Central African Republic, and Eritrea.
- Several countries experienced a slight worsening in their scores, namely, Tunisia, Guinea-Bissau and Nigeria.
- Countries have also witnessed changes in their regional rankings. For example, many top performers have risen in the regional rankings and countries like Togo, Eswatini, and the Democratic Republic of Congo have seen substantial advances in regional standings.

Regional Insights

Central Africa: Notable progress is seen in many countries, particularly in the Democratic Republic of Congo, Gabon, Angola, Equatorial Guinea and Cameroon. Relatively moderate progress is seen in the Central African Republic and São Tomé and Príncipe.

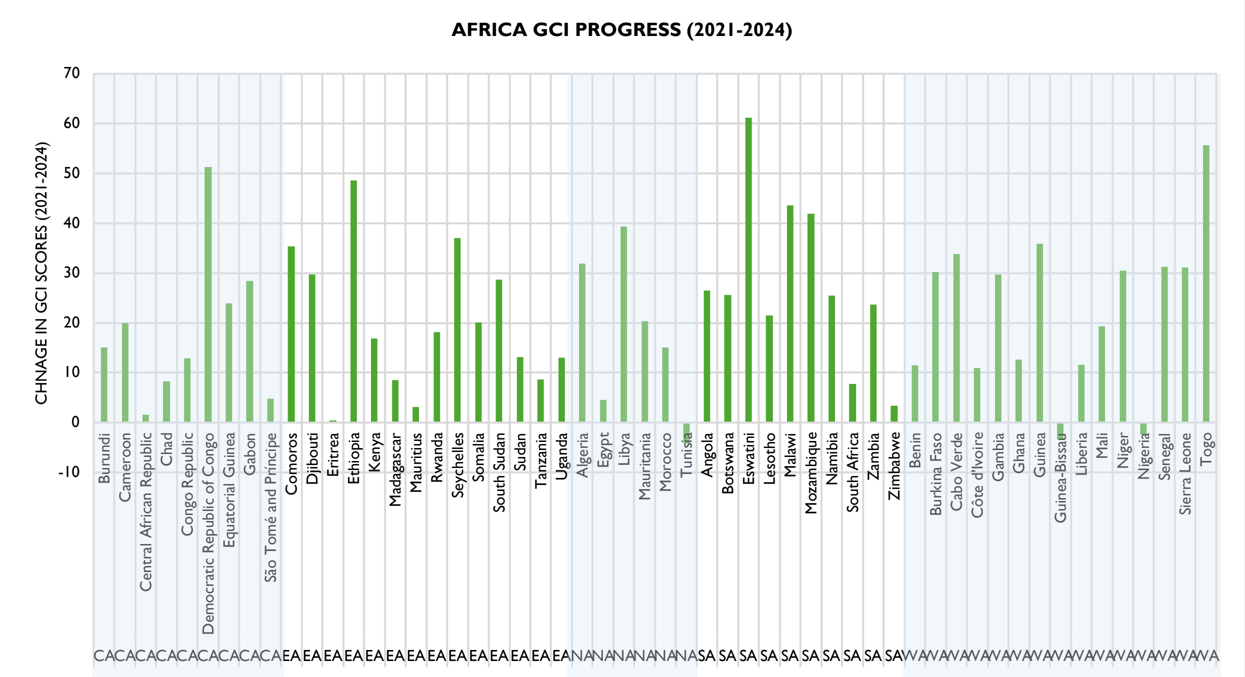
Eastern Africa: Countries such as Ethiopia, Seychelles and Comoros lead in the extent of progress in cybersecurity. The role-modelling countries such as Kenya experienced moderate growth.

Northern Africa: Algeria, Libya and Mauritania, in particular, show advances in cybersecurity. Legal, organisation and capacity development measures are some significant areas of growth for certain countries.

Southern Africa: Eswatini, Malawi and Mozambique show notable growth in the region.

Western Africa: Togo, Guinea and Cabo Verde experience the highest levels of progress in the region. Legal and capacity development measures are some notable areas of growth for certain countries.

FIGURE 5: AFRICA'S PROGRESS IN CYBERSECURITY COMMITMENTS



Although some progress may be explained by the change in the methodology adopted by ITU, a significant portion of each country's progress can be traced to coordinated measures and interventions by its national government to improve national cybersecurity capabilities. For example, Togo has adopted a cooperative model approach to support their national efforts in mitigating cybersecurity risks[12]. The Cyber Defense Africa SAS (CDA) established through Public-private partnerships (PPPs) and the African Cybersecurity Centre are notable outcomes of such a strategy[13]. Togo's progress in overall GCI score, and particularly in capacity development and cooperation measures, is therefore unsurprising.

E-GOVERNMENT AND CYBERSECURITY COMMITMENTS

Digital transformation, particularly in the public sector, is a top priority for many African countries, and cybersecurity plays a crucial role in this process. To this end, we examine the relationship between the

[12] https://www.cda.tg/

[13] https://www.un.org/africarenewal/magazine/september-2022/togo-and-un-sign-mou-establish-african-cybersecurity-centre

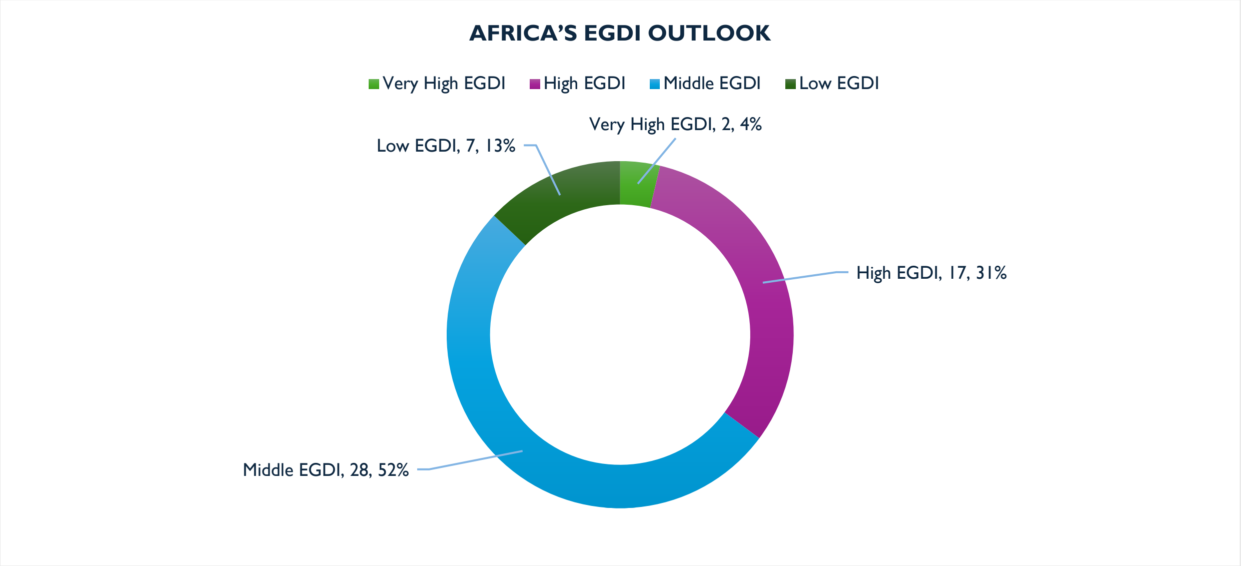
development of national e-government initiatives and the commitment to cybersecurity using EGDI 2024 and GCI 2024 data, as illustrated in Figure 7. This investigation helps illuminate how robust cybersecurity measures support and enhance the effectiveness of e-government services and platforms, ensuring the protection of digital infrastructure and data.

The E-Government Development Index (EGDI) measures the progress of e-government development at the national level[14]. According to the United Nations (UN) E-Government Survey 2024, the EGDI is a composite measure which consists of three normalised indices: the Telecommunications Infrastructure Index (TII), the Human Capital Index (HCI), and the Online Service Index (OSI). They further state that the EGDI serves as a benchmarking and development tool for advancing digital transformation, allowing national and local governments to learn from each other, identify areas of strength and challenges in e-government, and shape their policies and strategies for future improvement.

The model is summarised as follows:

- Very high EGDI: above 0.75
- High EGDI: ranging from 0.50 to 0.75
- Middle EGDI: ranging from 0.25 to 0.50
- Low EGDI: ranging from 0 to 0.25

FIGURE 6: AFRICA'S EGDI OUTLOOK



Summary of the UN E-Government Survey 2024

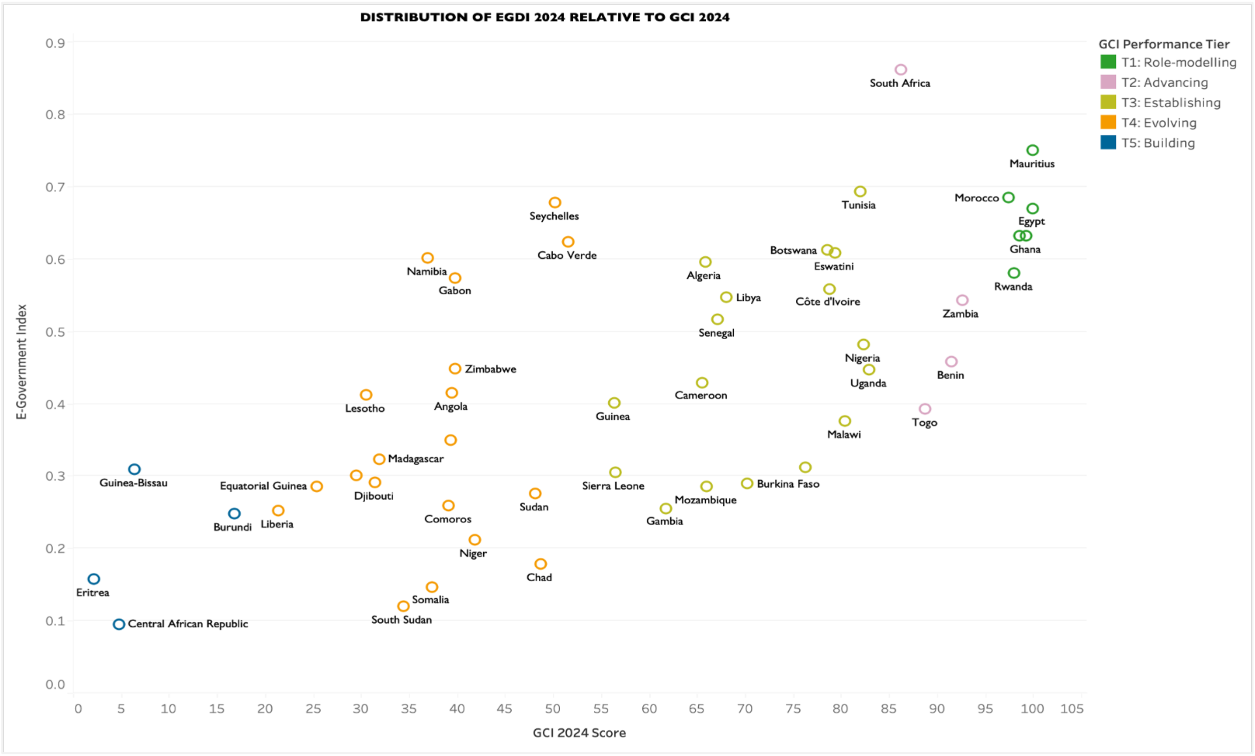
The EGDI report is summarised, highlighting key points concerning Africa.

- The global average value of EGDI, as a proxy for measuring the digital divide, has improved substantially over the past two years, with the proportion of the world population lagging in digital government development decreasing from 45.0% in 2022 to 22.4% in 2024.

[14] https://publicadministration.un.org/egovkb/en-us/Reports/UN-E-Government-Survey-2024

- Africa has made some progress but remains below the global average, with a regional average value of 0.4227 compared to the global average EGDI of 0.6382. This suggests that African countries are facing digital inequities and exclusion.
- Significant disparities persist in digital infrastructure, connectivity, digital skills, and e-government readiness within the region. Two countries, or 4%, have a very high EGDI, 17 countries, or 31 %, are in the high EGDI group, 28 countries, or 52%, are in the middle EGDI group, and seven countries, or 13%, fall into the low EGDI group (Figure 6).
- With respective EGDI values of 0.8616 and 0.7506, South Africa and Mauritius are the first African countries to join the very high EGDI group.
- The Survey predicts that, even with the most optimistic projections, Africa will not close the digital gap with other regions by 2030. Thus, there is an urgent need for accelerated efforts and innovative solutions to address the digital divide.

FIGURE 7: DISTRIBUTION OF EGDI 2024 RELATIVE TO GCI 2024



AFRICA'S EGDI AND GCI RELATIONSHIP

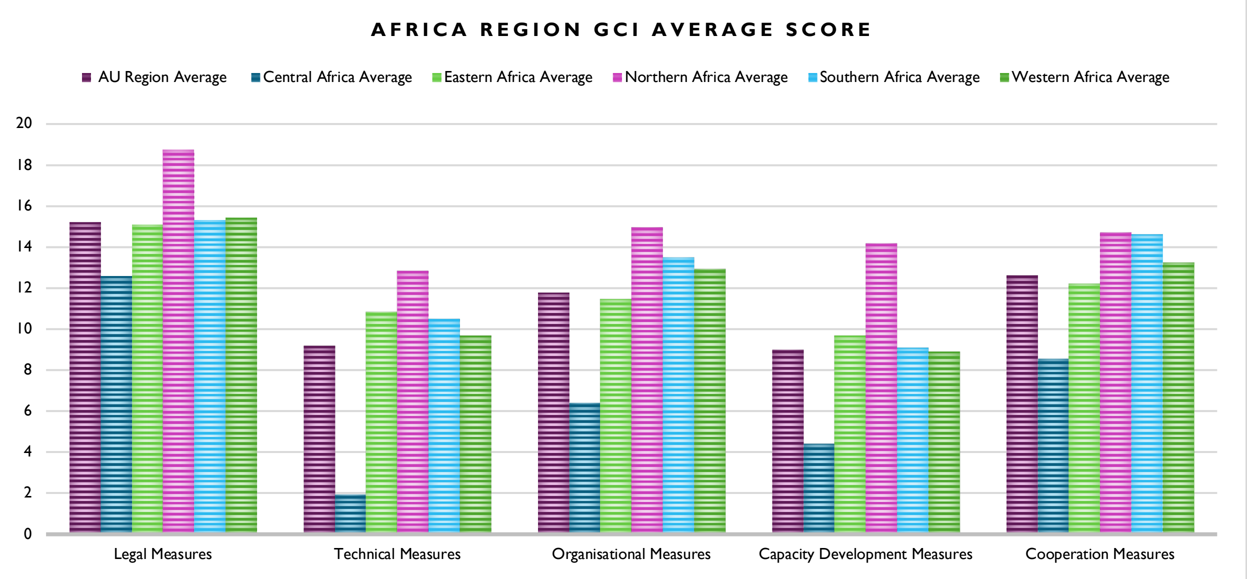
- A comparative analysis of the two indices reveals a correlation between the EGDI rankings and the GCI performance tiers. Several countries that perform well on the EGDI tend to also rank high in the GCI index, as illustrated in Figure 7. Conversely, countries with the lowest EGDI values occupy the lower tiers in the current GCI edition. This trend underscores the interconnectedness of digital government development and commitment to cybersecurity, highlighting the importance of strengthening both indices to achieve a more secure digital development.
- All Role-modelling countries are within the high to very high EGDI groups, while all countries at the Building stage are within the low to middle EGDI groups.

- There is a broad distribution of countries within the low to middle EGDI groups demonstrating disparate GCI tier performances. For example, Benin and Togo are Advancing performers, Zimbabwe, Angola, and Comoros are Evolving performers, Nigeria, Mozambique and Gambia are at the Establishing stage, and Eritrea and the Central African Republic are at the Building level.
- Cabo Verde, Seychelles, Namibia, and Gabon have high EGDI rankings but show significantly lower cybersecurity commitments, as observed in the GCI 2024. This can pose a significant risk to these countries in terms of increased vulnerabilities to cyberattacks, compromised critical information infrastructure and issues with public trust regarding the use of e-government services.
- Countries such as Burkina Faso, Gambia, Malawi, and Togo exhibit disproportionate cybersecurity commitments and EGDI values. While this demonstrates efforts to improve government-led cybersecurity actions, certain other challenges are likely to exist, such as inefficient public services, the underutilisation of digital services, and underused capacity in cybersecurity.
- The analysis underscores that efforts to address the digital divide and improve the efficiencies in e-government services must be accompanied by sound cybersecurity measures.

REGIONAL CYBERSECURITY OUTLOOK

The regional cybersecurity outlook reveals varied levels of cybersecurity development across different African regions. Northern Africa leads in cybersecurity commitment, while Central Africa lags behind all other regions, as illustrated in Figure 8 and Figure 9. Notably, similar patterns of government-led cybersecurity activities are evident in Eastern, Southern, and Western Africa. Regional data highlight that, although gaps exist in all cybersecurity pillars, technical and capacity development measures require further priority. Enhanced collaboration and sharing of best practices within and across regions could elevate the national and regional cybersecurity profiles across the continent.

FIGURE 8: REGIONAL GCI 2024 AVERAGE PILLAR PERFORMANCE



Legal Measures: The legal measures pillar is the strongest performing pillar across all regions, which is consistent with global trends. Northern Africa leads with the highest regional average score, while Central Africa occupies the lowest position. However, the variation in legal measures among regions is relatively small.

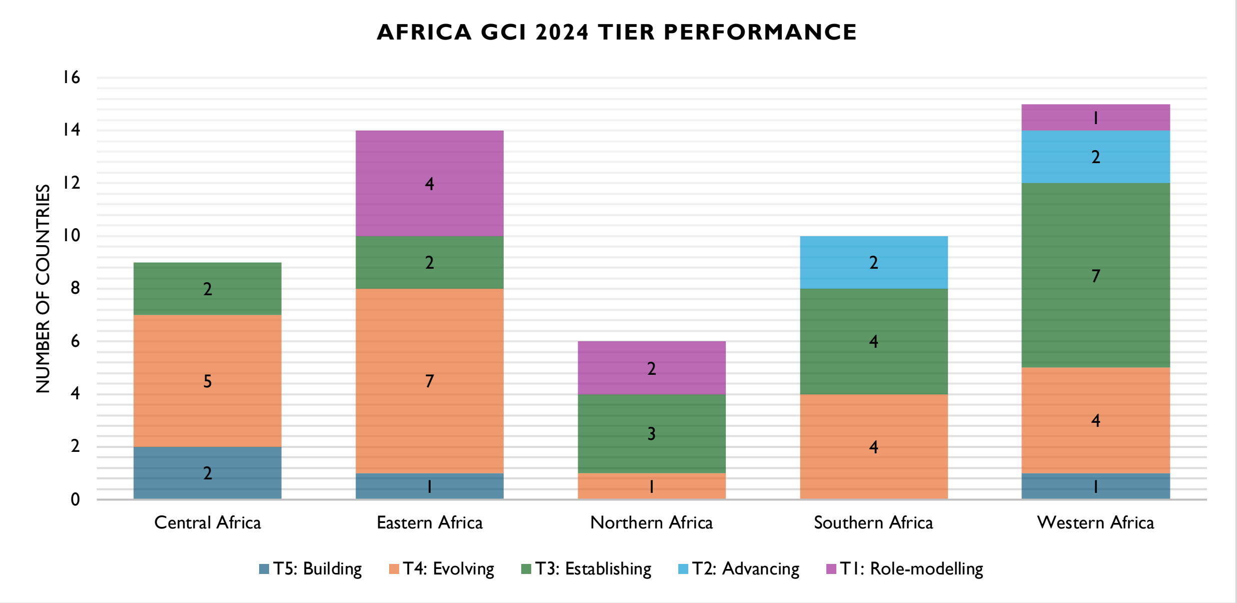
Technical Measures: Northern Africa excels in technical measures, but regional scores vary widely. Central Africa scores particularly low, and most regions fall below the mid-range (< 10/20). This disparity underscores differences in technical response capabilities and commitments across regions. Development and support from regional CIRTs in incident response capabilities is one approach, especially where there may be limited resource availability at the national level.

Organisational Measures: African countries perform relatively well in organisational measures generally, especially when compared to technical measures, with Northern Africa being a notable exception as a consistent performer in both pillars. The average scores for organisational measures indicate that most regions have relatively more standard cybersecurity measures, such as frameworks and strategies in place.

Capacity Development Measures: Capacity development measures are generally limited across the continent, with only Northern Africa exceeding the mid-range (>10/20). This highlights the need for greater investment in capacity-building initiatives such as targeted awareness campaigns and cybersecurity curricula at all education levels, as well as increased education and training for cybersecurity professionals and research and development.

Cooperation Measures: Cooperation measures are fairly consistent across regions, with Central Africa being the only exception, falling below the mid-range (< 10/20). This signifies the need for increased efforts to foster national, regional and international collaboration in cybersecurity, such as membership in cybersecurity treaties and leveraging information sharing and capacity building opportunities across key sectors.

FIGURE 9: GCI 2024 REGIONAL PERFORMANCE



Central Africa

Central Africa reflects performance levels at the earliest stages of cybersecurity commitments, categorised as Building, Evolving, and Establishing tiers, with the majority of these countries at the Evolving level demonstrating basic cybersecurity commitment in at least one pillar or several indicators. Only two countries show government-driven actions in a moderate number of pillars or indicators. The current trend calls for urgent actions to enhance efforts across all cybersecurity pillars to propel these countries to more advanced levels of cybersecurity commitments.

Central Africa				
T5: Building	**T4: Evolving**	**T3: Establishing**	**T2: Advancing**	**T1: Role-modelling**
Burundi	Chad	Cameroon		
Central African Republic	Congo Republic	Democratic Republic of Congo		
	Equatorial Guinea			
	Gabon			
	São Tomé and Príncipe			

Eastern Africa

Eastern Africa exhibits diverse levels of cybersecurity commitment with a notable presence at the "Role-modelling" level. The current status shows that while some countries like Kenya, Mauritius, Rwanda, and Tanzania are role models in cybersecurity, others are in the initial building and evolving stages. This suggests a need for varied approaches tailored to address each country's specific gaps while leveraging any cooperation measures within the region to better enable more advanced nations to support those in earlier stages.

Eastern Africa				
T5: Building	**T4: Evolving**	**T3: Establishing**	**T2: Advancing**	**T1: Role-modelling**
Eritrea	Comoros	Ethiopia		Kenya
	Djibouti	Uganda		Mauritius
	Madagascar			Rwanda
	Seychelles			Tanzania
	Somalia			
	South Sudan			
	Sudan			

Northern Africa

Northern Africa features prominently in the Establishing and Role-modelling levels of cybersecurity commitment as well as having a single country at the Evolving stage. The data highlight that while Egypt leads as a role model in cybersecurity, countries like Mauritania, Algeria, Libya, Tunisia, and Morocco are at different stages of implementing certain cybersecurity measures. The region exhibits a strong potential for growth and improvement, and therefore, Initiatives to help advance countries' cybersecurity profiles are needed in most countries despite cybersecurity leadership in a few.

Northern Africa				
T5: Building	**T4: Evolving**	**T3: Establishing**	**T2: Advancing**	**T1: Role-modelling**
	Mauritania	Algeria		Egypt
		Libya		Morocco
		Tunisia		

SOUTHERN AFRICA

Southern Africa exhibits a range of cybersecurity commitment levels among its countries. South Africa and Zambia are the highest performers at the Advancing level while a fairly balanced spread is seen at the Evolving and Establishing levels. This highlights significant potential for growth and development, with opportunities to enhance government-led cybersecurity initiatives and capacity building across the region.

Southern Africa				
T5: Building	**T4: Evolving**	**T3: Establishing**	**T2: Advancing**	**T1: Role-modelling**
	Angola	Botswana	South Africa	
	Lesotho	Eswatini	Zambia	
	Namibia	Malawi		
	Zimbabwe	Mozambique		

WESTERN AFRICA

Western Africa displays a diverse range of cybersecurity commitment levels among its countries showing a presence at all levels. Ghana leads as a role model in cybersecurity, while countries such as Benin and Togo are advancing, and others are in various stages of building and evolving their cybersecurity frameworks. The region showcases a significant potential for growth and development in cybersecurity, with opportunities to enhance government-led cybersecurity initiatives and capacity building in the region.

Western Africa				
T5: Building	**T4: Evolving**	**T3: Establishing**	**T2: Advancing**	**T1: Role-modelling**
Guinea-Bissau	Cabo Verde	Burkina Faso	Benin	Ghana
	Liberia	Côte d'Ivoire	Togo	
	Mali	Gambia		
	Niger	Guinea		
		Nigeria		
		Senegal		
		Sierra Leone		

Role-modelling Practices and Insights from Africa

Overview

Given the disparity in national cybersecurity commitments, learning from others is a practical strategy to help advance government-led cybersecurity initiatives. We examine some good cybersecurity practices that have been adopted by African countries, particularly during the GCI 2024 review period. Others can adopt similar initiatives as they seek to improve performance in the cybersecurity pillars. The perspective of role-modelling is adapted to consider not only countries within that tier but also the identification of specific measures adopted that may mitigate cybersecurity risks and address the cybersecurity challenge[15]. A non-exhaustive list of activities and illustrations are discussed herein.

Legal Measures

- **Cybercrime and Cybersecurity Legislation and Regional Model Laws**. More countries have implemented new and revised laws which are closely aligned with multilateral cybercrime and cybersecurity conventions. These include South Africa's Cybercrimes Act, where several sections came into effect in 2021[16], and the recent amendment of Nigeria's Cybercrime (Prohibition, Prevention, etc) Act[17].
- **Modern Data Protection and Privacy Frameworks**. Countries have implemented new and updated data protection laws that contemplate current good practices and standards, such as requirements for data breach notifications, data protection impact assessments, and data protection officers. Examples include Tanzania's Personal Data Protection Act, 2022, which came into effect in 2023[18], South Africa's Protection of Personal Information Act, which came into operation in 2021 after a one-year grace period[19], Botswana's Data Protection Act, 2018, which came into effect on October 15, 2021[20], Gabon's Law No. 025/2023 amending Law No. 001/2011 on the protection of personal data[21], and Rwanda's Law No. 058/2021 Relating to the Protection of Personal Data and Privacy which came into effect in 2021[22].
- **National Critical Infrastructure Protection**. The region has seen progress in the development and implementation of national critical infrastructure policies, laws and regulations. These frameworks take into account designating and defining national critical information infrastructure, the legal framework for the protection and continued resilience of critical infrastructure, and the assignment of a responsible entity to enforce the law, among other connected matters. Several existing cybercrime laws contemplate some of these issues, and notable recent laws include South Africa's Critical Infrastructure Protection Act, Gabon's Law No. 027/2023 Regulating Cybersecurity and the Fight against Cybercrime[23], and Kenya's Computer Misuse and Cybercrimes (Critical Information Infrastructure and Cybercrime Management) Regulations, 2023[24].
- **Digital ID Systems and Frameworks**. There is a move towards the harmonisation of digital ID systems, policy, legislative, and regulatory frameworks to support the current and emerging

[15] Adapted from C. Barclay, An Analysis of the GCI 2024: Progress, Challenges and Opportunities for the Caribbean, ISBN 978 976 97440 0 4
[16] https://cybercrimesact.co.za/
[17] https://cert.gov.ng/ngcert/resources/CyberCrime__Prohibition_Prevention_etc__Act__2024.pdf
[18] https://www.pdpc.go.tz/media/media/THE_PERSONAL_DATA_PROTECTION_ACT.pdf
[19] https://popia.co.za/
[20] https://www.bocra.org.bw/sites/default/files/documents/32%20Act%2010-08-2018-Data%20Protection.pdf
[21] https://journal-officiel.ga/20089-166-pr-/
[22] https://rwandalii.org/akn/rw/act/law/2021/58/eng@2021-10-15
[23] https://journal-officiel.ga/20091-168-pr-/
[24] https://nc4.go.ke/storage/2023/08/COMPUTER-MISUSE-AND-CYBERCRIMES-GENERAL-REGULATIONS-.pdf

digital ID ecosystems as well as data privacy and security concerns. For instance, the AU Interoperability Framework for Digital ID, introduced in 2022, seeks to enable all African citizens to easily and securely access public and private services conveniently by defining common requirements, minimum standards, governance mechanisms, and alignment among legal frameworks[25]. At the national level, countries are at various stages of implementing, refining and harmonising national digital ID systems and frameworks.

- **Regulatory Impact Assessments**. To promote evidence-based policymaking, more countries are conducting regulatory impact assessments (RIAs) to help ensure the effective implementation of laws relating to cybercrime and cybersecurity and that their subsidiary laws meet desired objectives. Undoubtedly, adopting a sound RIA framework can significantly improve the understanding of the potential impact of regulatory actions within the cybersecurity ecosystem. For example, Kenya performed an RIA on the Computer Misuse and Cybercrimes (Critical Information Infrastructure and Cybercrime Management) Regulations, 2023, to assess whether the "regulation is welfare-enhancing from the societal viewpoint, in that, the benefits will surpass costs"[26] and found that both public and private actors stand to benefit meaningfully from the implementation of such legally binding instruments.

TECHNICAL MEASURES

- **The Creation and Strengthening of National and Sectoral Incident Response Capabilities.**
    - The role of the Communications Authority of Kenya (CA) was enhanced to include the establishment and operation of the Cyber Security Operations Centre (CSOC) for the ICT and Telcom Sector following the enactment of the Computer Misuse and Cybercrime (Critical Information Infrastructure and Cybercrime Management) Regulations in 2024[27].
    - Sectoral CERTs have increased their influence and presence in their countries by promoting awareness, capacity-building initiatives, and fostering information sharing among their constituents. These efforts are evident in several countries, such as Egypt, Ghana, Kenya, Tanzania, Mauritius, and Morocco.
- **Conducting Cybersecurity Drills**. Leading and participating in cybersecurity drills are an important aspect of bolstering continuity and resilience, identifying vulnerabilities, building capacity and fostering cooperation. The Africa Computer Emergency Response Team (AfricaCERT) plays an integral role through its annual cyber drill to test the capability of CERTs in Africa[28]. Countries also lead regular national cybersecurity exercises to help strengthen capacity and promote awareness.
- **Developing and Strengthening National Frameworks to Support the Adoption of Cybersecurity Standards.**
    - Regional working groups have been increasingly active in developing cybersecurity frameworks to support the development of technical capabilities. For example, in 2023, East African Communications Organisations (EACO), developed several minimum standards and guidelines, such as the establishment of the Regional Strategy for

[25] https://au.int/sites/default/files/documents/43393-doc-AU_Interoperability_framework_for_D_ID_English.pdf
[26] https://nc4.go.ke/storage/2023/09/Regulatory-Impact-Statement.pdf
[27] https://ke-cirt.go.ke/
[28] https://www.africacert.org/wp-content/uploads/2022/10/Press-release-2nd-Africa-CYBER-DRILL-Stay-on-Alert.pdf

Establishing and Operationalising of Computer Incident Response Teams (CIRTS/CERTS)[29] and the Guidelines for the Management of Critical Infrastructure[30].

- **Developing National Threat Intelligence Networks**. Beyond sharing information and incidents among national and sectoral CERT constituents, threat intelligence networks can offer valuable insights regarding ongoing activities at the national level. Tanzania has implemented one such initiative through the deployment of honeypots to monitor and analyse cyber threats[31]. Additionally, academic institutions and private sector companies in Tanzania are increasingly adopting honeypots as part of their cybersecurity strategies to better understand and mitigate cyber threats.

Organisational Measures

- **The Adoption of National and Regional Cybersecurity Strategies.**
  - The ECOWAS Regional Cybersecurity and Cybercrime Strategy and regional policy on CII[32] was developed in response to the ongoing digital transformation in West Africa. It provides a framework for Member States to consider in their national strategies and implement in their action plans to enhance cybersecurity and combat cybercrime.
  - Several countries have launched new or updated strategies. Earlier this year, Ghana launched its new policy and strategy aimed at addressing increasing cybersecurity threats arising from the nation's rapid digital transformation[33]. Morocco adopted a new national cybersecurity strategy in 2022, tackling strengthening cybersecurity measures and protecting national security[34]. Rwanda updated its national cybersecurity strategy (2024-2029), emphasising the promotion of cyber resilience and trust, building a cybersecurity industry, and enhancing cooperation and collaboration [35] . Senegal developed a new national cybersecurity strategy in 2022, promoting cybersecurity awareness and protecting national information infrastructure[36]. Uganda launched its national cybersecurity strategy in 2022, aimed at improving cybersecurity readiness and protecting national information infrastructure [37] . Eswatini also launched its 5-year national cybersecurity strategy in 2022[38].
  - Some common characteristics of a sound national cybersecurity framework include implementable actions to support specific goals, robust performance monitoring and reporting, clear accountabilities, adequate resource allocation and assignment, active committee participation and engagement, and an inclusive and participatory approach throughout the strategy lifecycle.

[29] https://eaco.int/admin/docs/reports/Regional%20Strategy_25EACO%20Congress.pdf

[30] https://eaco.int/admin/docs/reports/Guidelines1%20critical%20infrastructure_%2025EACO%20CONGRESS.pdf

[31] https://www.tzcert.go.tz/security-releases/honeypot-reports

[32] https://dig.watch/resource/ecowas-regional-critical-infrastructure-protection-policy

[33] https://www.csa.gov.gh/ghana-launches-national-cybersecurity-policy-and-strategy.php

[34] https://www.dgssi.gov.ma/sites/default/files/legislative/brochure/2022-10/presentation_note_of_the_law_n_deg_05-20_on_cybersecurity_-_english_version.pdf

[35] https://cyber.gov.rw/index.php?eID=dumpFile&t=f&f=427&token=6375c4cab9b091a9747cd9f07f8dc616ba825245

[36] https://www.itu.int/en/ITU-D/Cybersecurity/Documents/National_Strategies_Repository/SNC2022-Senegal-NCS-Jan-2018_eng.pdf

[37] https://ict.go.ug/wp-content/uploads/2023/01/National-Cybersecurity-Strategy-UG.pdf

[38] https://www.esccom.org.sz/publications/reports/docs/Eswatini_National_Cybersecurity_Strategy_2022-2027.pdf

- **The Development of Child Online Protection Frameworks and Strategies.**
    - The AU Child Online Safety and Empowerment Policy (2024)[39] provides a framework for implementing children's rights in the digital environment. It supports Member States in maximising the benefits of children's use of Information and Communication Technologies (ICTs) while prioritising the best interests of the child and minimising risks.
    - Côte d'Ivoire developed its national child protection strategy 2024-2028 to strengthen positive community practices in child protection and safeguarding against all forms of violence[40]. The process was supported by an inclusive and participatory approach that included a series of validation activities by key stakeholders.
    - In response to research amplifying the dangers of children on the internet, Ghana published a comprehensive National Child Online Protection Framework[41]. The framework seeks to ensure the effective operation of child protection mechanisms and safeguarding policies while respecting children's rights in digital settings. A consultative approach was adopted to create a flexible and adaptive agenda based on good standards.
- **The Establishment of National Institutions to Support Cybersecurity Governance.**
    - In 2021, Ghana established the Cyber Security Authority (CSA) to regulate cybersecurity activities and promote the development of cyber security. The CSA also has a Child Online Protection Unit, which is mandated to handle all online child-related issues.
    - National Cybersecurity Risk Management Frameworks typically contemplate tailored cybersecurity metrics, audit requirements, and related matters. These frameworks provide the benefits of improved risk management, accountability, transparency, and enhanced cybersecurity posture at the organisational and national levels. Several countries, particularly T1 performers, have existing policy and regulatory frameworks that impose certain obligations on government agencies to help ensure the continuity and resilience of key national assets.

Capacity Development Measures

- **Cybersecurity Awareness Activities Targeting Diverse Groups.**
    - National Cybersecurity Awareness Month (NCAM) initiatives in countries such as Ghana[42] and South Africa[43] adopt a multi-faceted approach to delivering cybersecurity education and awareness to diverse target groups.
    - Egypt launched awareness initiatives to address current and emerging threats. For example, campaigns are on popular social media channels to address issues like social media hacking[44] on WhatsApp, LinkedIn, and Instagram platforms. Additionally, awareness campaigns focused on topics like Artificial Intelligence (AI), online extortion, and sextortion are delivered.
    - Sierra Leone implemented an initiative to safeguard children online by promoting youth advocacy and empowerment[45]. They have organised competitions where students

[39] https://au.int/en/documents/20240521/african-union-child-online-safety-and-empowerment-policy
[40] https://www.faapa.info/blog/le-document-de-la-politique-nationale-de-protection-de-lenfant-valide/
[41] https://www.csa.gov.gh/resources/National%20COP%20Framework.pdf
[42] https://ncsam.csa.gov.gh/index.php
[43] https://www.education.gov.za/ArchivedDocuments/ArchivedArticles/Cybersecurity-Awareness-Month-1023.aspx
[44] https://egcert.eg/publications/page/2/
[45] https://grassrootsjusticenetwork.org/connect/organization/young-africans-community-empowerment-initiative-sierra-leone-yacei-sl/

discuss pressing issues on national television, such as cyberbullying and social media safety. This strategy engages students directly, enhancing their understanding and ability to address current online safety concerns effectively. This initiative not only raises awareness but also empowers students to become advocates for online safety, fostering a safer digital environment for everyone.

- **Training of Law Enforcement, Judiciary and Cybersecurity Professionals.**
    - In 2023, over 150 judges from Ghana, Malawi and Zambia were trained by the Commonwealth Secretariat's Cyber Unit in handling cybercrime cases[46].
    - Joint initiatives of the European Union (EU) and Council of Europe (COE) such as the CyberSouth+ project, aimed at strengthening criminal justice capacities with a focus on enhanced cooperation on cybercrime and disclosure of electronic evidence. It combines regional and country-specific actions that are tailored to the needs and capacities of project countries such as Algeria, Egypt, Libya, Morocco, and Tunisia[47].
    - Another joint project of the EU and COE is the GLACY-e (Global Action on Cybercrime Enhanced), which was launched in December 2023[48]. The project is aimed at strengthening the capacities of countries in Africa, Asia-Pacific, and Latin America (and the Caribbean) to apply cybercrime and electronic evidence laws and foster international cooperation. Regarding Africa, Ghana, Senegal, and Mauritius serve as "hubs and multipliers" for sharing tools, best practices, and experiences.
- **Research and Development Initiatives.**
    - The launch of a cyber hub in Nigeria to help build the cybersecurity capacity of youths and engender a more comprehensive cybersecurity ecosystem. This was established by a partnership between the American Business Council (ABC), the University of Lagos and private sector stakeholders[49]. A similar approach is seen in Benin with the BjWhiteHat Community[50], which aims to identify and build talent to meet market demand.
    - The Republic of Togo and the United Nations Economic Commission for Africa (UNECA) signed a memorandum of understanding (MoU) to collaborate to establish the ACCRC to promote cybersecurity and combat cybercrime. The Centre will provide technical expertise and research capabilities to promote cybersecurity within the region[51].
    - Continuing activities and outputs from research institutions such as the African Centre for Security (ACS)[52] as well as the establishment of the African Centre for Coordination and Research (ACCRC) as a regional hub[53].
- **Government Incentives.** There are several examples of the use of incentives to support development and growth in the national cybersecurity industry and ecosystem.
    - Egypt's Ministry of Communications and Information Technology (MCIT) launched several initiatives, such as the AI Capacity Building Initiative, Digital Egypt Pioneers Initiative, Basic Digital Skills Development Programs, and Programs for Government Employees[54]. These projects aim to develop specific and relevant capabilities among

[46] https://thecommonwealth.org/news/commonwealth-workshops-train-150-african-judges-handling-cybercrime-cases
[47] https://www.coe.int/en/web/cybercrime/cybersouthplus
[48] /https://rm.coe.int/3399-glacy-e-summary-vfinal-en/1680ae1cba
[49] https://vmtnews.ng/cybersecurity-american-business-council-stakeholders-unveil-cyber-hub/
[50] https://bjwhitehats.bj/
[51] https://www.un.org/africarenewal/magazine/september-2022/togo-and-un-sign-mou-establish-african-cybersecurity-centre
[52] https://africensec.africa/
[53] https://accrc.africa/en/home
[54] https://mcit.gov.eg/en/Human_Capacity/MCIT

diverse stakeholder groups, including students, youth, young professionals and government employees.

- Countries have proposed diverse incentives to accelerate national cybersecurity capacity in their national strategic framework. For example, Eswatini discussed projects stemming from funding and incentive programs for national enterprises providing Cybersecurity solutions[55], while Rwanda identified national research grants, incentives for the research and production of innovative cybersecurity patents, and support to international research ventures[56].

Cooperation Measures

- **Regional and International Cyber Treaties.** Several countries are members of any three major treaties in force and pertinent to the continent: the African Union Convention on Cyber Security and Personal Data Protection (Malabo Convention), the Convention on Cybercrime (Budapest Convention), and the Arab Convention on Combatting Technology Offences (Arab Convention). Morocco is a party to all three treaties, while Côte d'Ivoire, Ghana, and Senegal are parties to the Malabo and Budapest treaties. Several countries have acceded to the Budapest Convention in the last year, including Cameroon, Côte d'Ivoire, Sierra Leone, and Tunisia acceded to the Budapest Convention. At the same time, eight countries including Kenya, Malawi, and Mozambique have been invited to accede[57].
- **Regional Law Enforcement's Partnerships**. AFRIPOL and INTERPOL's continuing collaboration efforts aimed at enhancing cybercrime capacity building and cyber resilience in Africa include several milestones, such as the establishment of the AFRIPOL data centre and forensic databases, the inauguration of the Criminal Intelligence Analysis Unit (CIA), and the launch of the AFRIPOL Bootcamp on Cybercrime investigation[58].
- **Regional Responses to Combatting Cybercrime**. OCWAR-C, the West African Response on Cybersecurity and Fight against Cybercrime[59] is part of the priorities of cooperation between the European Union, the ECOWAS Commission and its Member States under the Regional Indicative Program of the 11th European Development Fund and is aimed at enhancing cybersecurity and combatting cybercrime in the member states of the Commission of the Economic Community of West African States (ECOWAS).
- **Regional Information Sharing Platforms and Frameworks**. Regional intergovernmental entities, such as the EAC, Southern African Development Community (SADC), and ECOWAS have been engaged in a number of initiatives to foster increased collaboration among member countries, especially as they work towards achieving the mandate of the African Continental Free Trade Area (AfCFTA). An example is the EAC Community Data Protection Knowledge Exchange[60], which seeks to enhance collaboration and knowledge sharing among data protection regulatory authorities in East Africa. One key outcome of this initiative is the EAC Data Governance Policy Framework, which is to harmonise the region's approach to data

[55] https://www.esccom.org.sz/publications/reports/docs/Eswatini_National_Cybersecurity_Strategy_2022-2027.pdf
[56] https://cyber.gov.rw/index.php?eID=dumpFile&t=f&f=427&token=6375c4cab9b091a9747cd9f07f8dc616ba825245
[57] https://www.coe.int/en/web/cybercrime/news
[58] INTERPOL African Cyberthreat Assessment Report 2024
[59]https://www.ocwarc.eu/#:~:text=OCWAR%2DC%2C%20the%20%C2%ABWest,West%20African%20States%20(ECOWAS).
[60] https://d4dhub.eu/news/strengthening-data-protection-across-east-africa-a-knowledge-exchange-between-data-protection-authorities

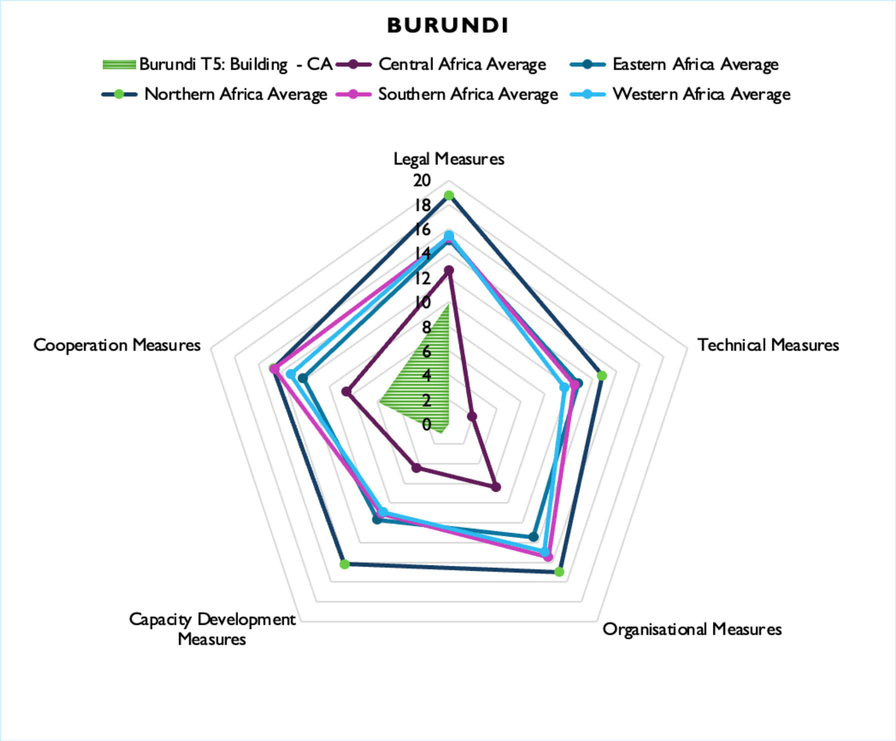
management by fostering the adoption of common standards for data protection, privacy, and security among Partner states[61].

Country Cybersecurity Profile by Region

The analysis assesses each country's GCI score against the average scores of the African regions and the continent. Organised by region, the country performance analysis is designed to help inform government policies by identifying each country's relative advantage and recommending priority actions across cybersecurity pillars to enhance commitments to cybersecurity[62]. Relative strength is based on the performance of the country relative to the average scores for each pillar for all regions. Therefore, strong country performance is based on the cybersecurity commitment level of each country when compared to the highest average regional score of a cybersecurity pillar. This approach enables benchmarking against peers rather than solely the country itself, providing valuable insights into potential cybersecurity actions for governments that may be prioritised. Priority actions are based on the identification of any gaps in GCI performance with respect to each pillar. To that end, even a role-modelling country may have gaps despite performing above the highest average regional score of a cybersecurity pillar. Role-modelling countries are also given general guidance focused on maintaining position and prioritising a risk-based approach to growth and innovation across the cybersecurity pillars.

Central Africa

Burundi



GCI 2024
AFRICA REGION
CONTINENT OUTLOOK
CA: Central Africa Region

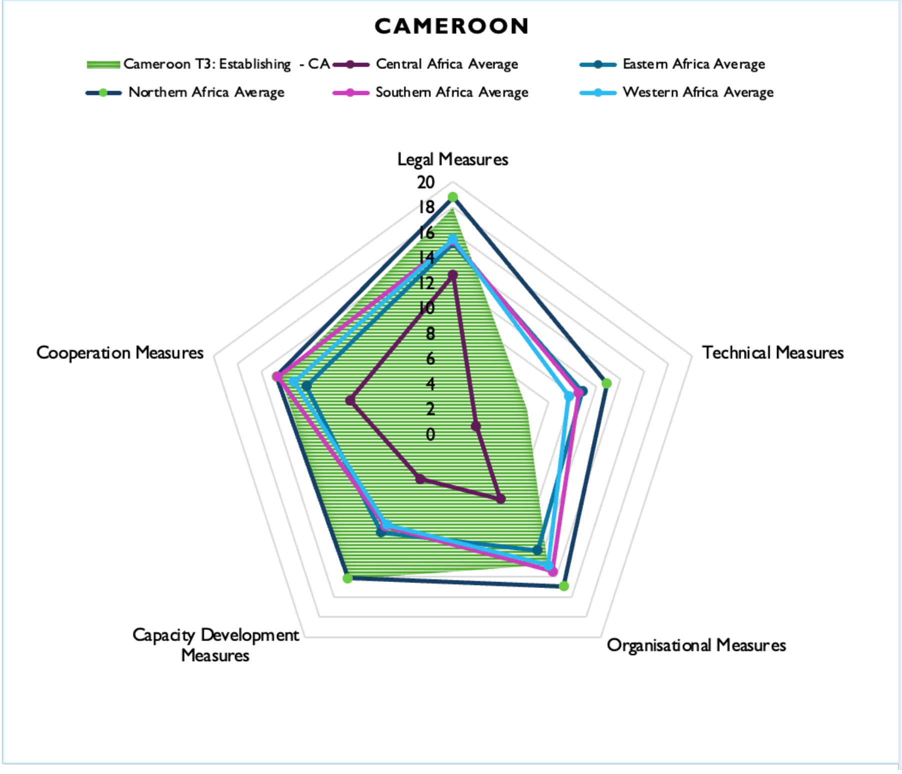
Pillar(s) of Relative Strength
None

Area(s) for Priority Action
Legal Measures
Technical Measures
Organisational Measures
Capacity Development Measures
Cooperation Measures

[61] https://www.eac.int/press-releases/3195-eac-set-to-advance-data-governance-and-protection-with-development-of-a-regional-policy-framework

[62] Adapted from C. Barclay, An Analysis of the GCI 2024: Progress, Challenges and Opportunities for the Caribbean, ISBN 978 976 97440 0 4

CAMEROON

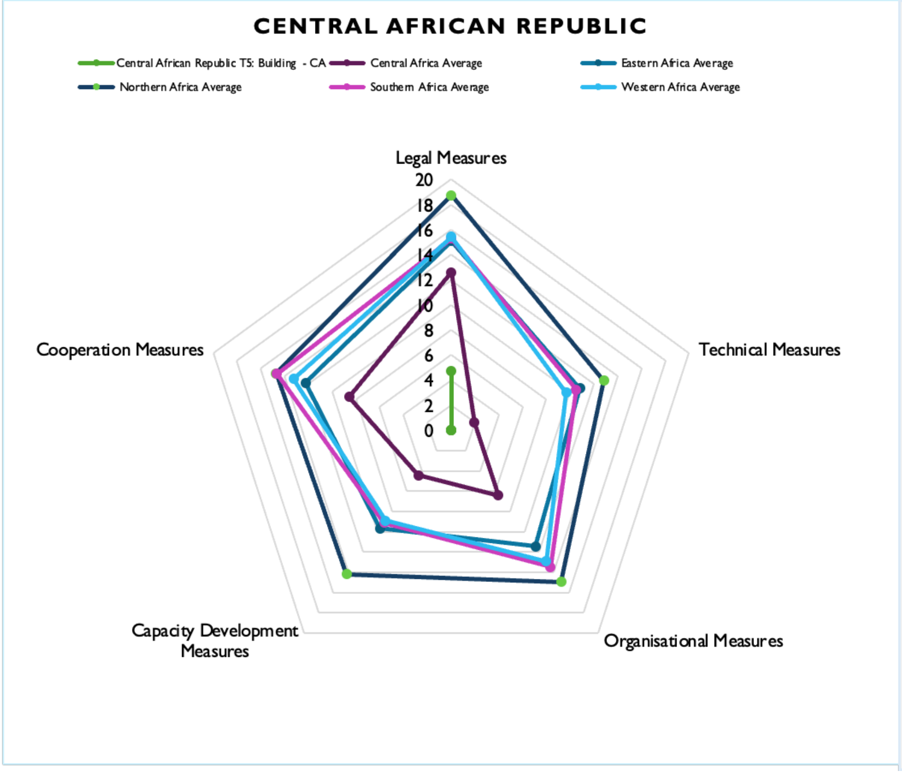


GCI 2024
AFRICA REGION
CONTINENT OUTLOOK
CA: Central Africa Region

Pillar(s) of Relative Strength
None

Area(s) for Priority Action
Legal Measures
Technical Measures
Organisational Measures
Capacity Development Measures
Cooperation Measures

CENTRAL AFRICAN REPUBLIC

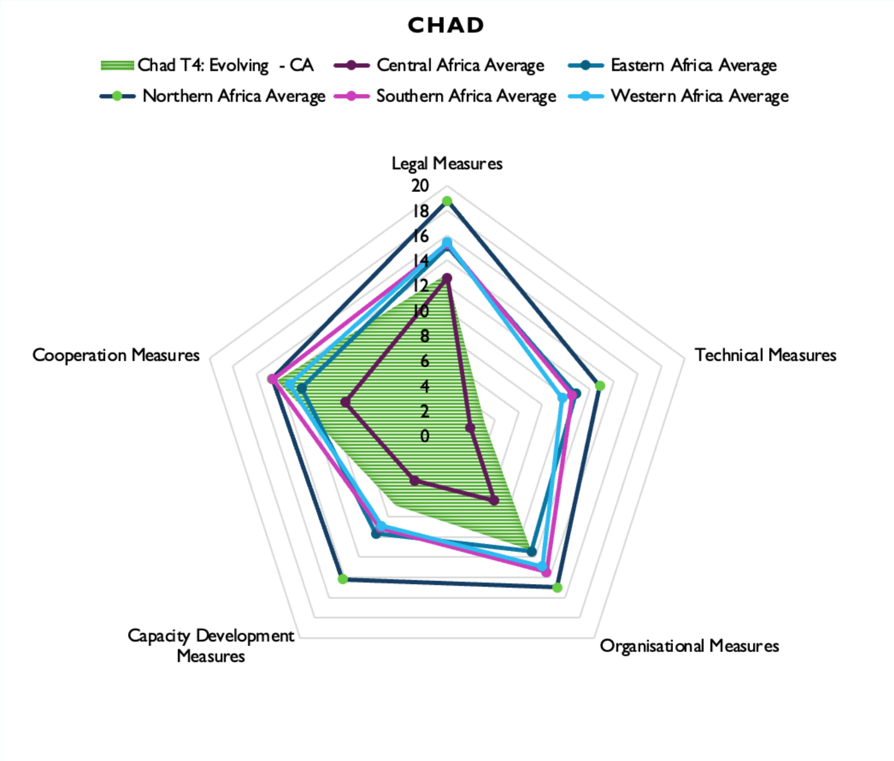


GCI 2024
AFRICA REGION
CONTINENT OUTLOOK
CA: Central Africa Region

Pillar(s) of Relative Strength
None

Area(s) for Priority Action
Legal Measures
Technical Measures
Organisational Measures
Capacity Development Measures
Cooperation Measures

Chad

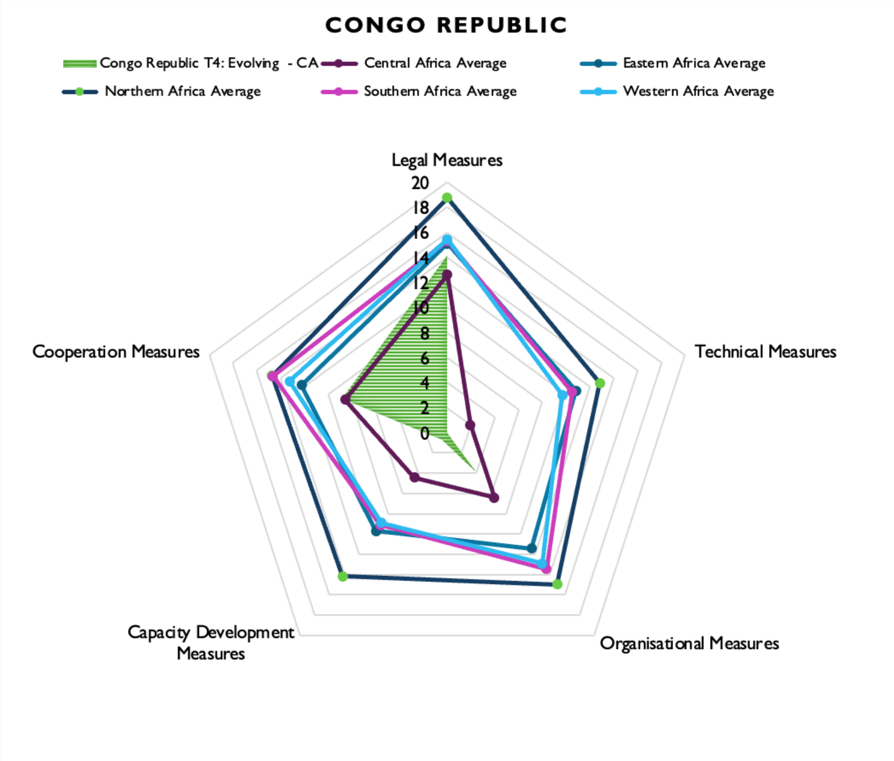


GCI 2024
AFRICA REGION
CONTINENT OUTLOOK
CA: Central Africa Region

Pillar(s) of Relative Strength
None

Area(s) for Priority Action
Legal Measures
Technical Measures
Organisational Measures
Capacity Development Measures
Cooperation Measures

Congo Republic

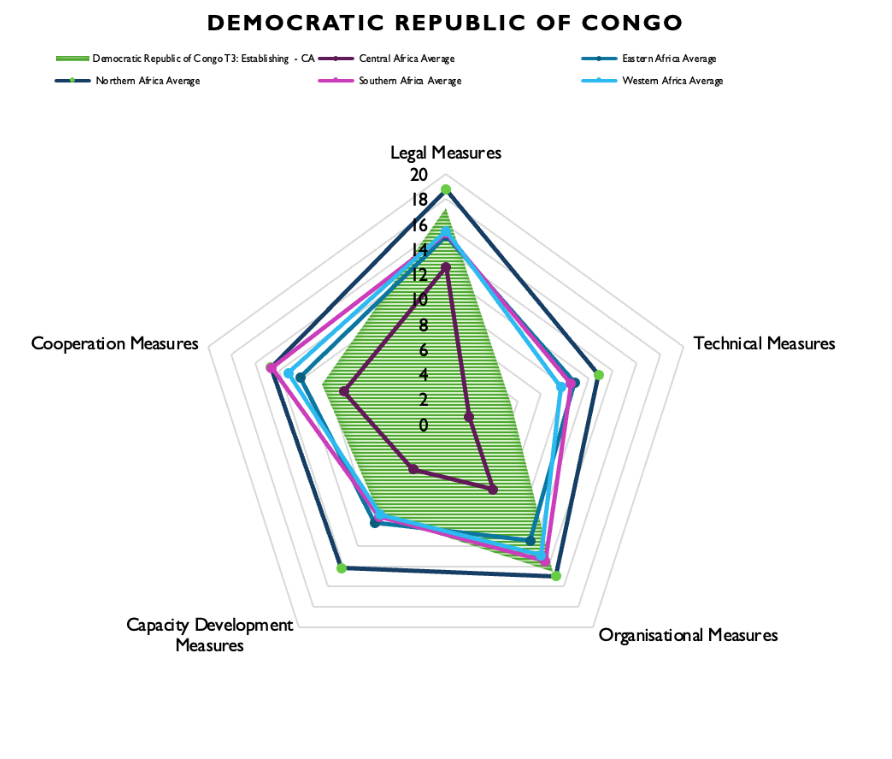


GCI 2024
AFRICA REGION
CONTINENT OUTLOOK
CA: Central Africa Region

Pillar(s) of Relative Strength
None

Area(s) for Priority Action
Legal Measures
Technical Measures
Organisational Measures
Capacity Development Measures
Cooperation Measures

DEMOCRATIC REPUBLIC OF CONGO

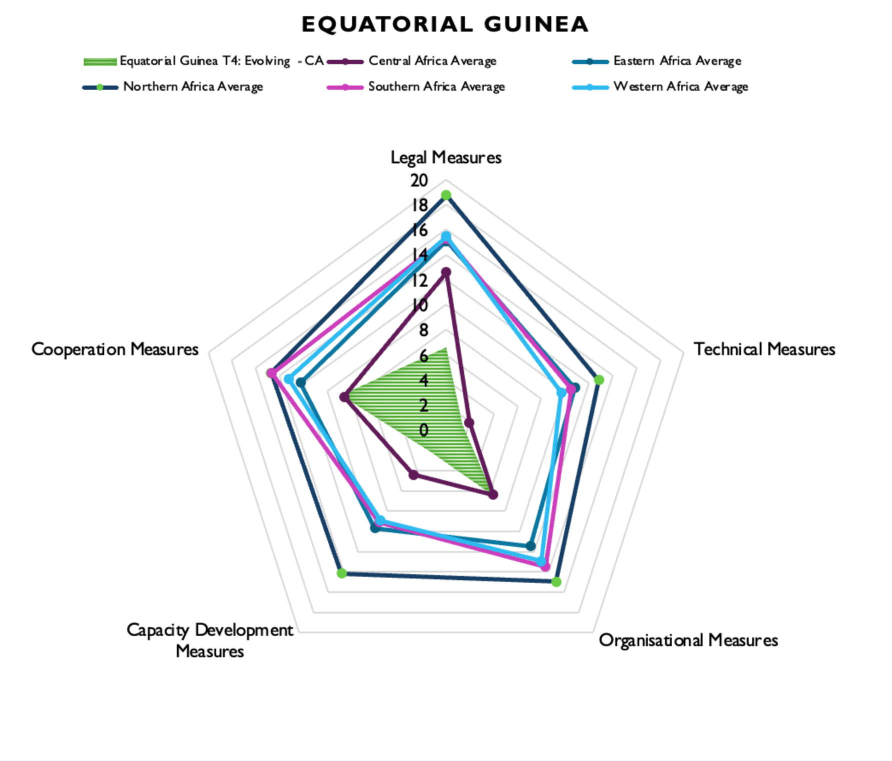


GCI 2024
AFRICA REGION
CONTINENT OUTLOOK
CA: Central Africa Region

Pillar(s) of Relative Strength
None

Area(s) for Priority Action
Legal Measures
Technical Measures
Organisational Measures
Capacity Development Measures
Cooperation Measures

EQUATORIAL GUINEA

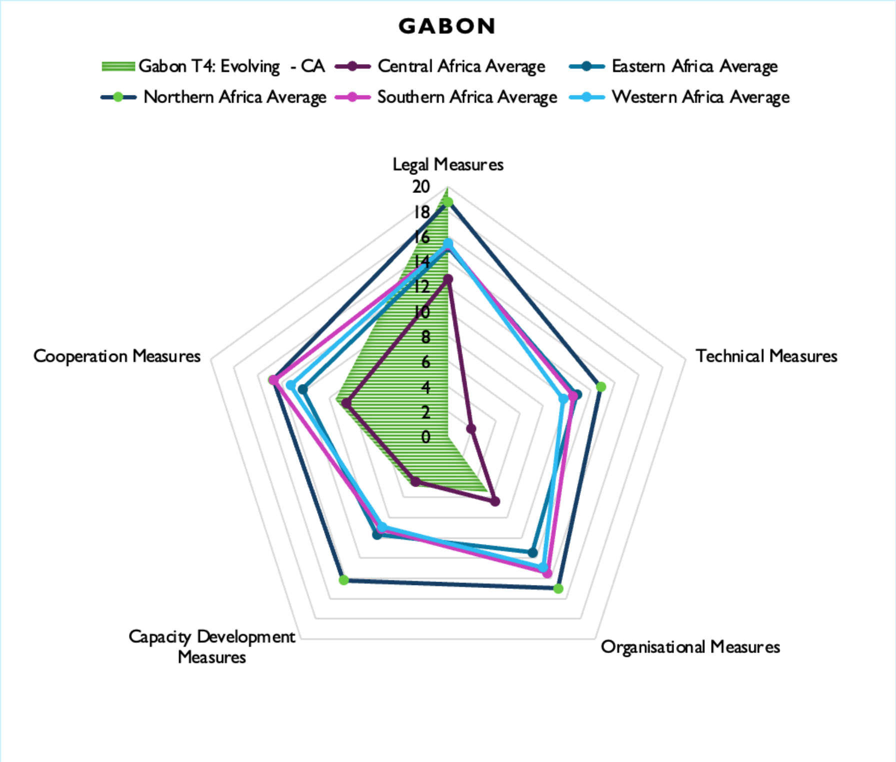


GCI 2024
AFRICA REGION
CONTINENT OUTLOOK
CA: Central Africa Region

Pillar(s) of Relative Strength
None

Area(s) for Priority Action
Legal Measures
Technical Measures
Organisational Measures
Capacity Development Measures
Cooperation Measures

Gabon

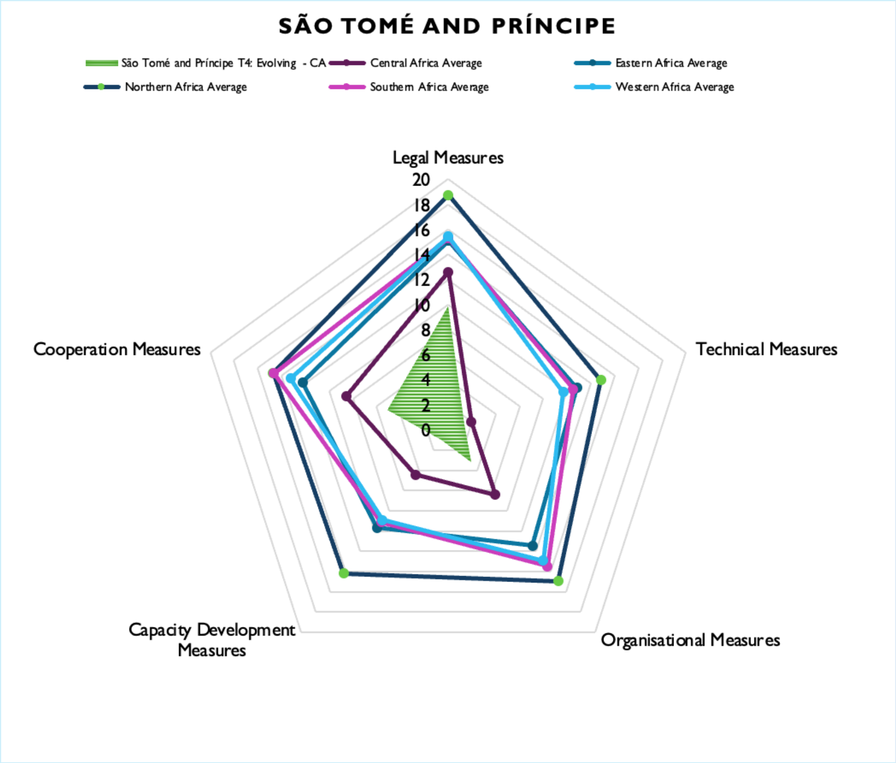


GCI 2024
AFRICA REGION
CONTINENT OUTLOOK
CA: Central Africa Region

Pillar(s) of Relative Strength
Legal Measures

Area(s) for Priority Action
Technical Measures
Organisational Measures
Capacity Development Measures
Cooperation Measures

São Tomé and Príncipe



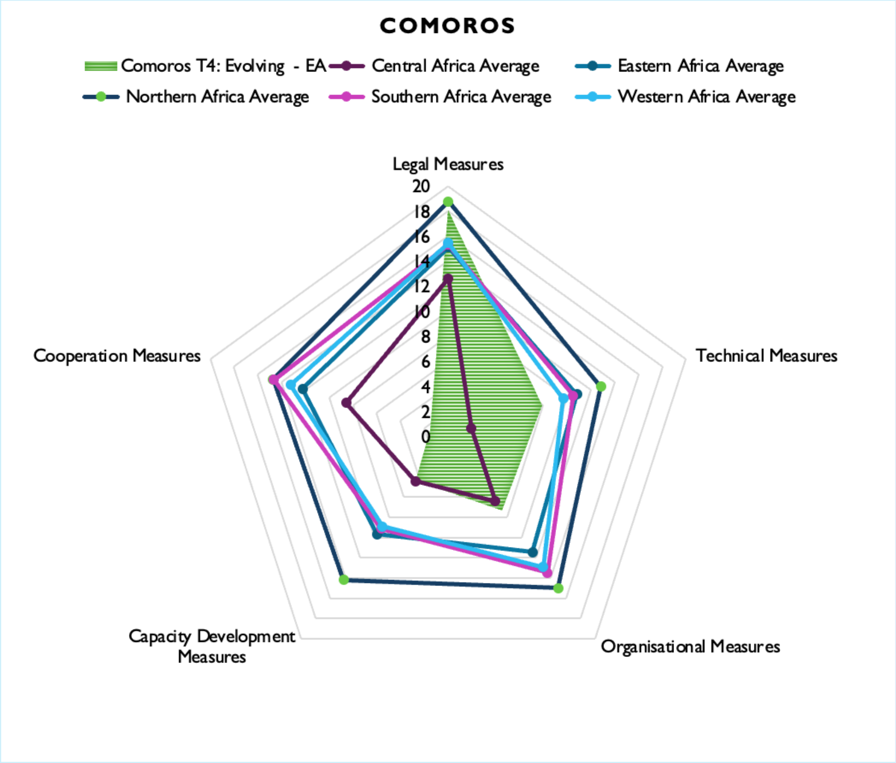
GCI 2024
AFRICA REGION
CONTINENT OUTLOOK
CA: Central Africa Region

Pillar(s) of Relative Strength
None

Area(s) for Priority Action
Legal Measures
Technical Measures
Organisational Measures
Capacity Development Measures
Cooperation Measures

Eastern Africa

Comoros

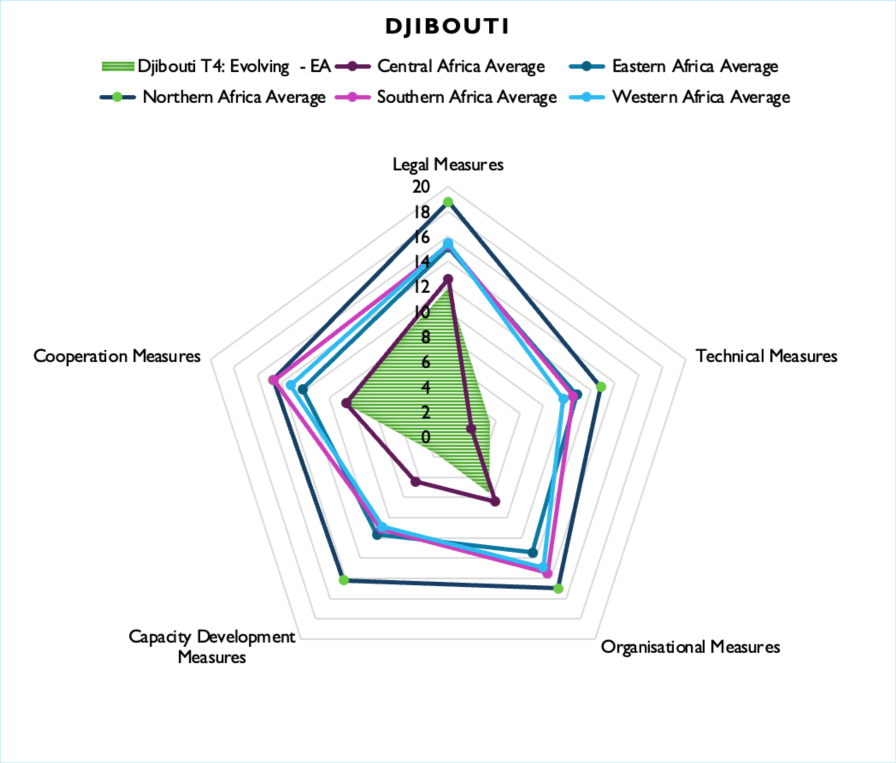


GCI 2024
AFRICA REGION
CONTINENT OUTLOOK
EA: Eastern Africa Region

Pillar(s) of Relative Strength
None

Area(s) for Priority Action
Legal Measures
Technical Measures
Organisational Measures
Capacity Development Measures
Cooperation Measures

Djibouti

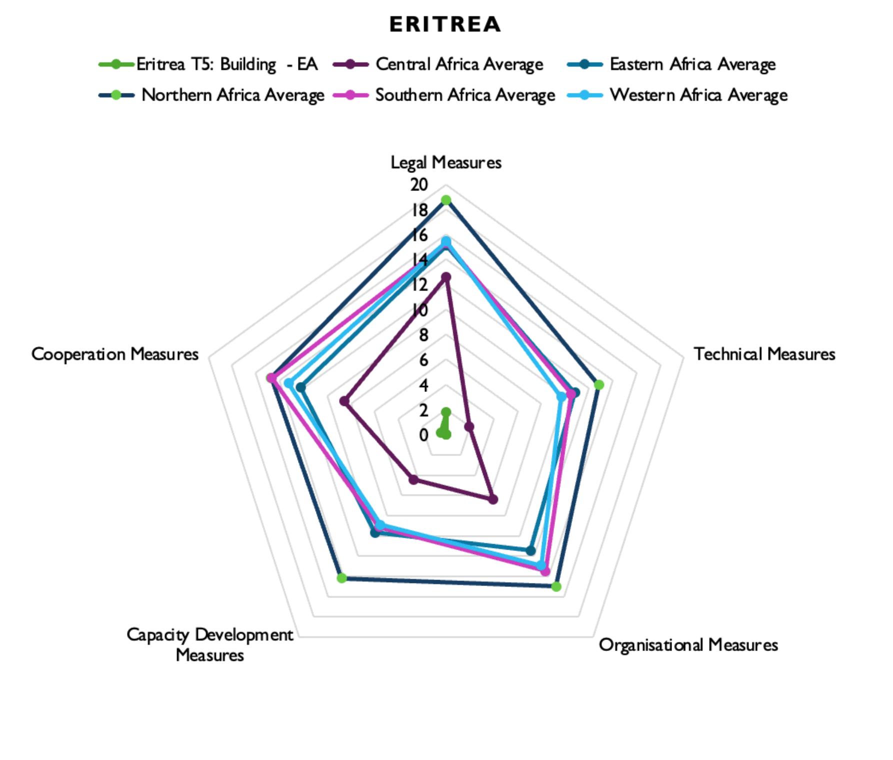


GCI 2024
AFRICA REGION
CONTINENT OUTLOOK
EA: Eastern Africa Region

Pillar(s) of Relative Strength
None

Area(s) for Priority Action
Legal Measures
Technical Measures
Organisational Measures
Capacity Development Measures
Cooperation Measures

Eritrea

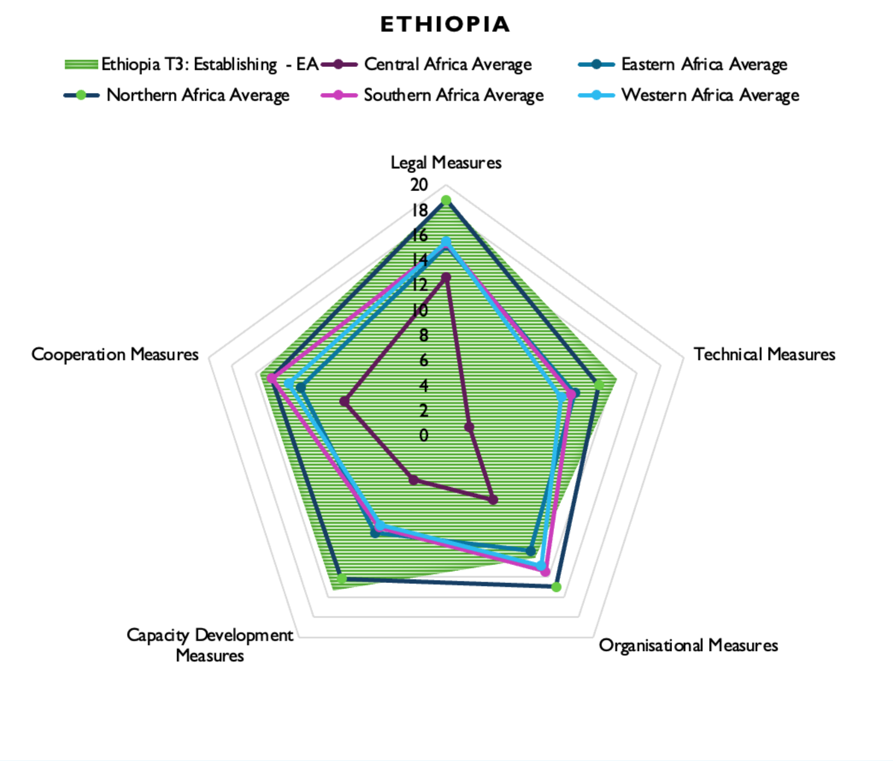


GCI 2024
AFRICA REGION
CONTINENT OUTLOOK
EA: Eastern Africa Region

Pillar(s) of Relative Strength
None

Area(s) for Priority Action
Legal Measures
Technical Measures
Organisational Measures
Capacity Development Measures
Cooperation Measures

Ethiopia

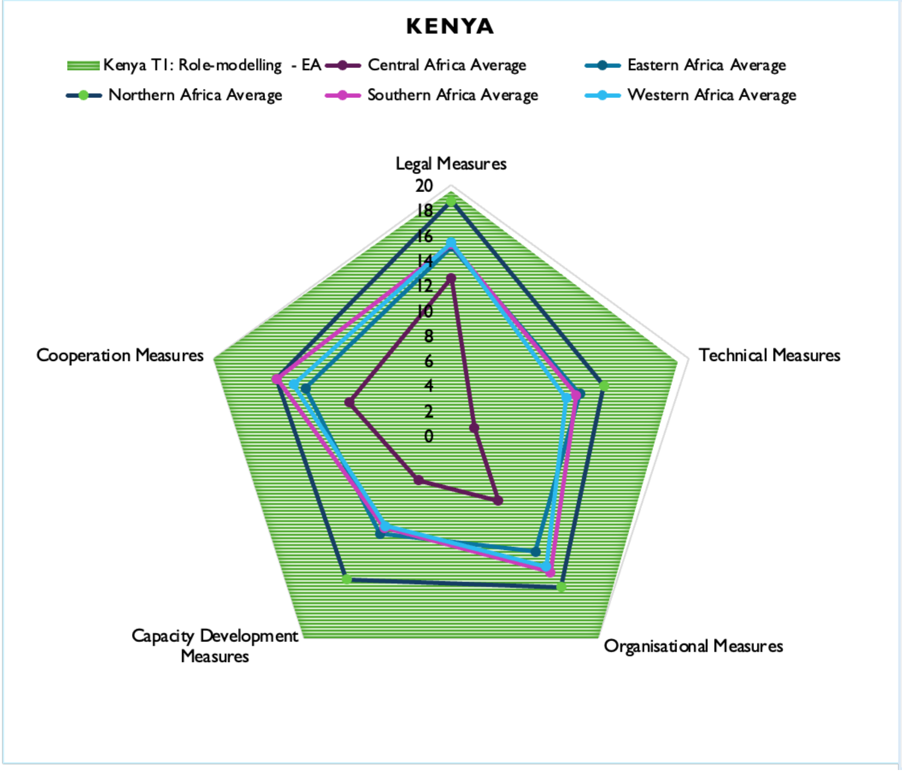


GCI 2024
AFRICA REGION
CONTINENT OUTLOOK
EA: Eastern Africa Region

Pillar(s) of Relative Strength
Technical Measures
Capacity Development Measures
Cooperation Measures

Area(s) for Priority Action
Legal Measures
Organisational Measures

KENYA



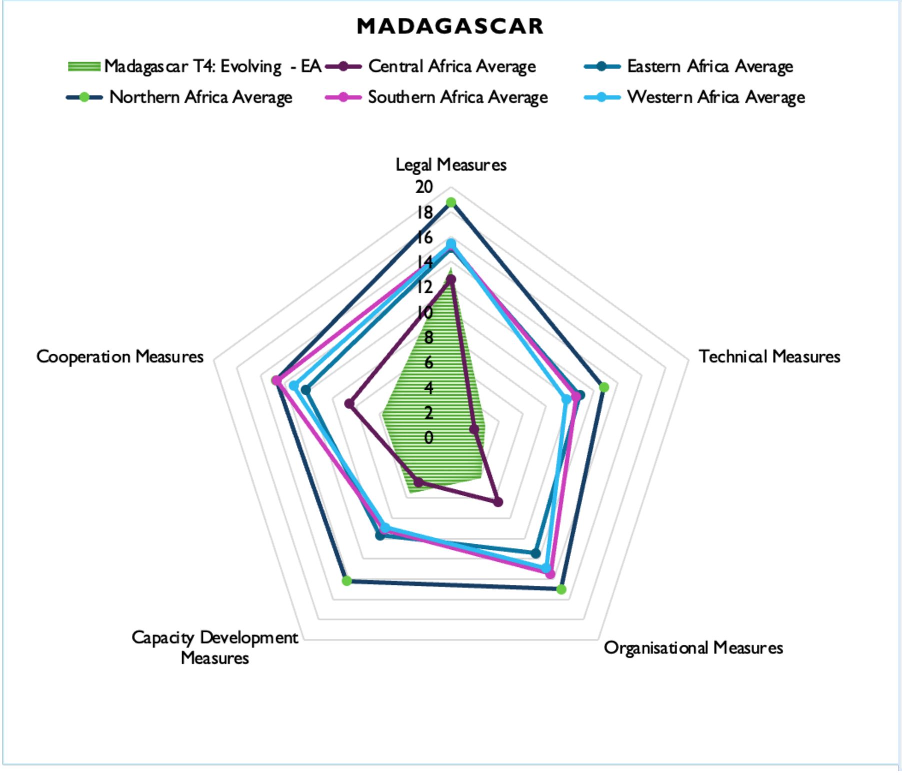
GCI 2024
AFRICA REGION
CONTINENT OUTLOOK
EA: Eastern Africa Region

Pillar(s) of Relative Strength
Legal Measures
Technical Measures
Organisational Measures
Capacity Development Measures
Cooperation Measures

Area(s) for Priority Action
Legal Measures
Technical Measures

Role-modelling Strategic Options
Maintain efficacy of existing measures
Adopt a risk-based approach to build and extend measures across all pillars

MADAGASCAR

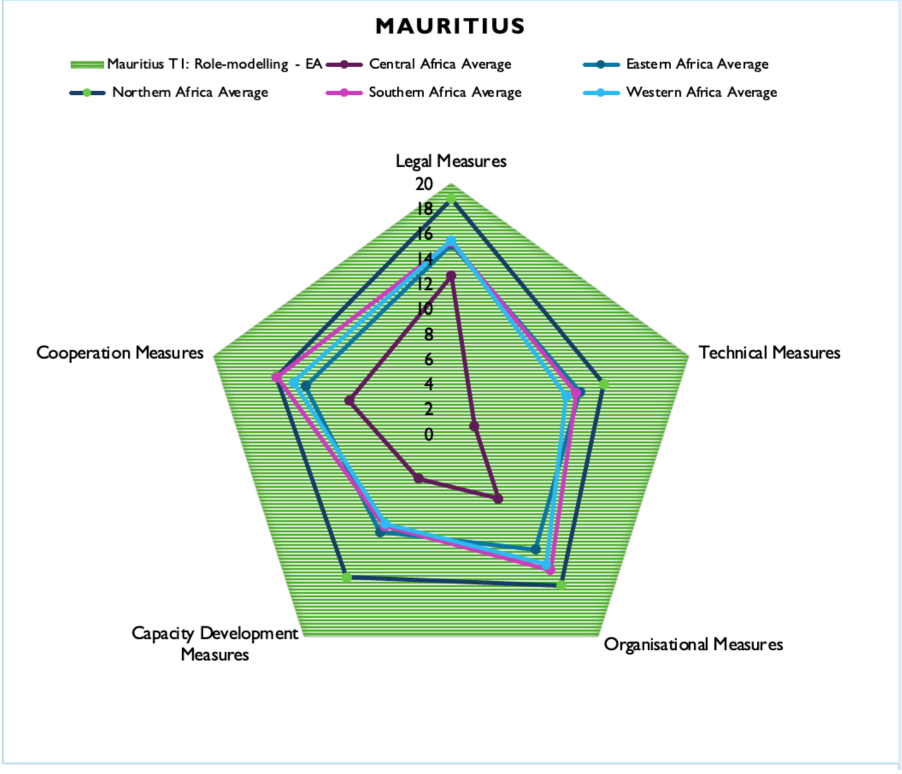


GCI 2024
AFRICA REGION
CONTINENT OUTLOOK
EA: Eastern Africa Region

Pillar(s) of Relative Strength
None

Area(s) for Priority Action
Legal Measures
Technical Measures
Organisational Measures
Capacity Development Measures
Cooperation Measures

MAURITIUS



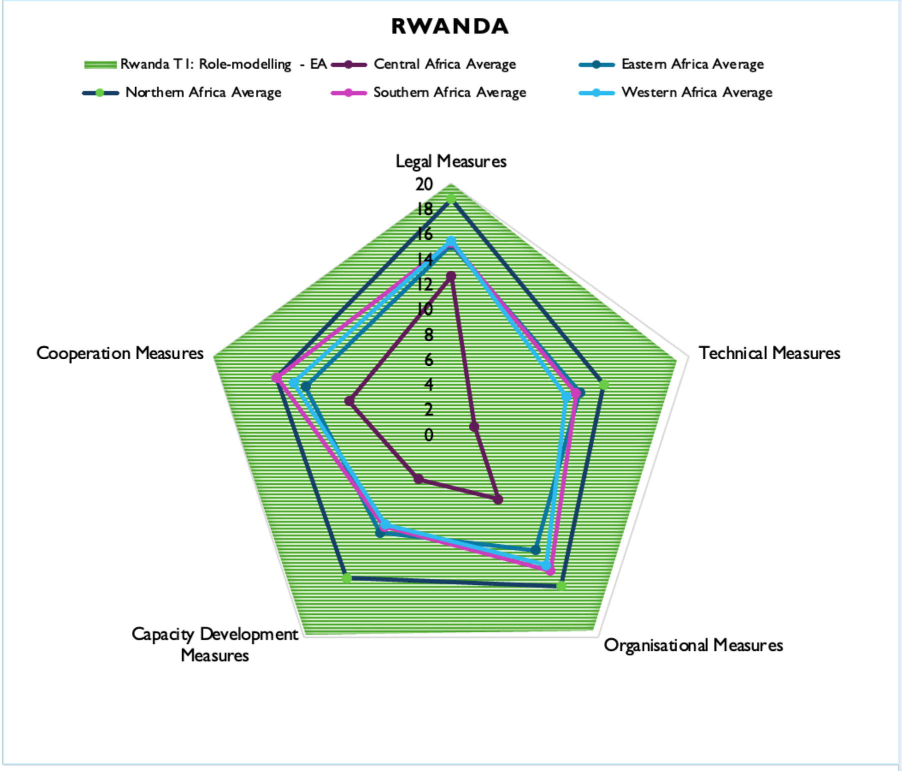
GCI 2024
AFRICA REGION
CONTINENT OUTLOOK
EA: Eastern Africa Region

Pillar(s) of Relative Strength
Legal Measures
Technical Measures
Organisational Measures
Capacity Development Measures
Cooperation Measures

Area(s) for Priority Action
None

Role-modelling Strategic Options
Maintain efficacy of existing measures
Adopt a risk-based approach to build and extend measures across all pillars

RWANDA



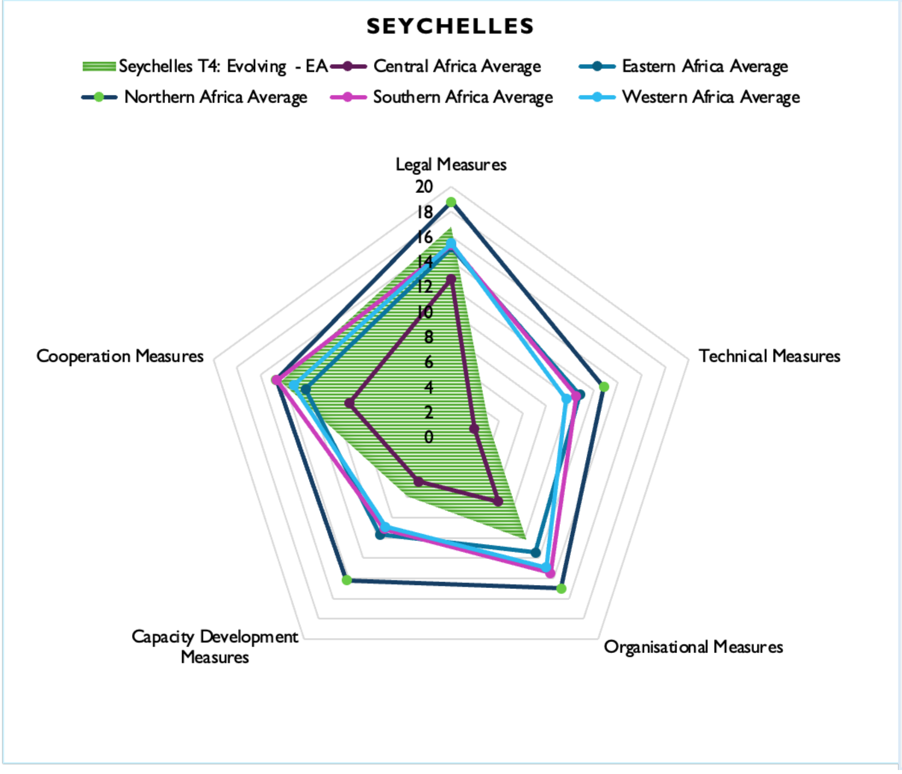
GCI 2024
AFRICA REGION
CONTINENT OUTLOOK
EA: Eastern Africa Region

Pillar(s) of Relative Strength
Legal Measures
Technical Measures
Organisational Measures
Capacity Development Measures
Cooperation Measures

Area(s) for Priority Action
Technical Measures
Organisational Measures
Capacity Development Measures

Role-modelling Strategic Options
Maintain efficacy of existing measures
Adopt a risk-based approach to build and extend measures across all pillars

SEYCHELLES

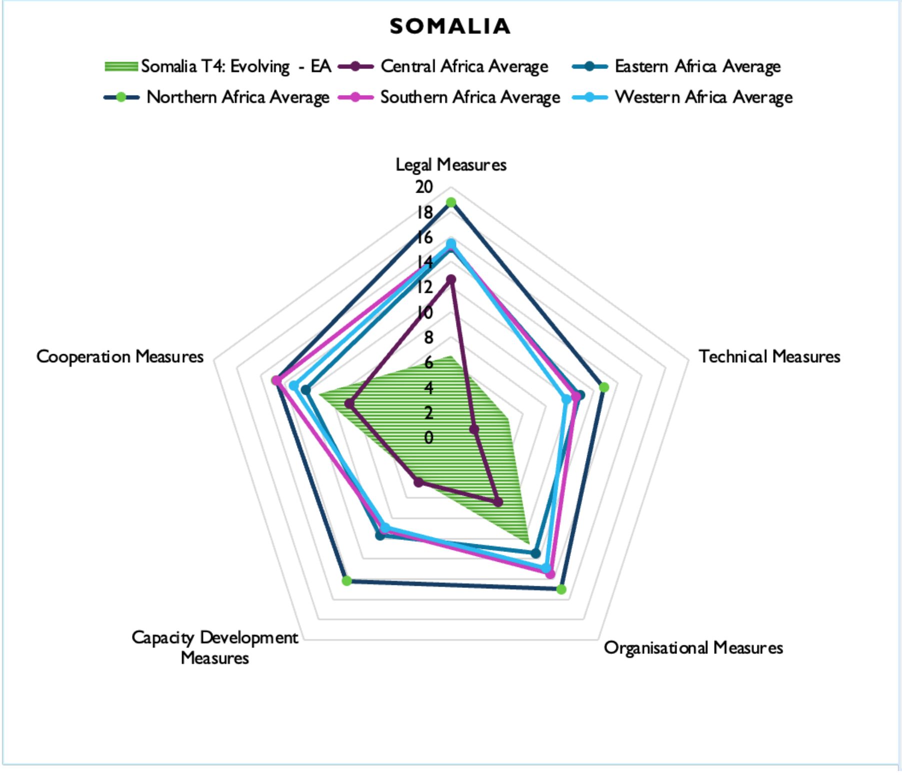


GCI 2024
AFRICA REGION
CONTINENT OUTLOOK
EA: Eastern Africa Region

Pillar(s) of Relative Strength
None

Area(s) for Priority Action
Legal Measures
Technical Measures
Organisational Measures
Capacity Development Measures
Cooperation Measures

SOMALIA

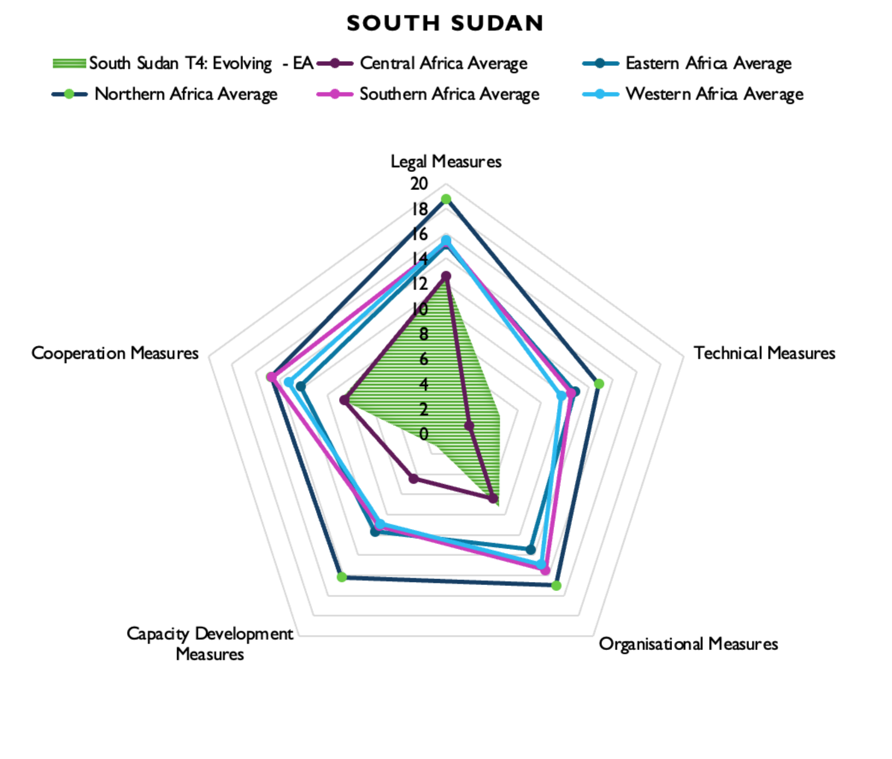


GCI 2024
AFRICA REGION
CONTINENT OUTLOOK
EA: Eastern Africa Region

Pillar(s) of Relative Strength
None

Area(s) for Priority Action
Legal Measures
Technical Measures
Organisational Measures
Capacity Development Measures
Cooperation Measures

SOUTH SUDAN

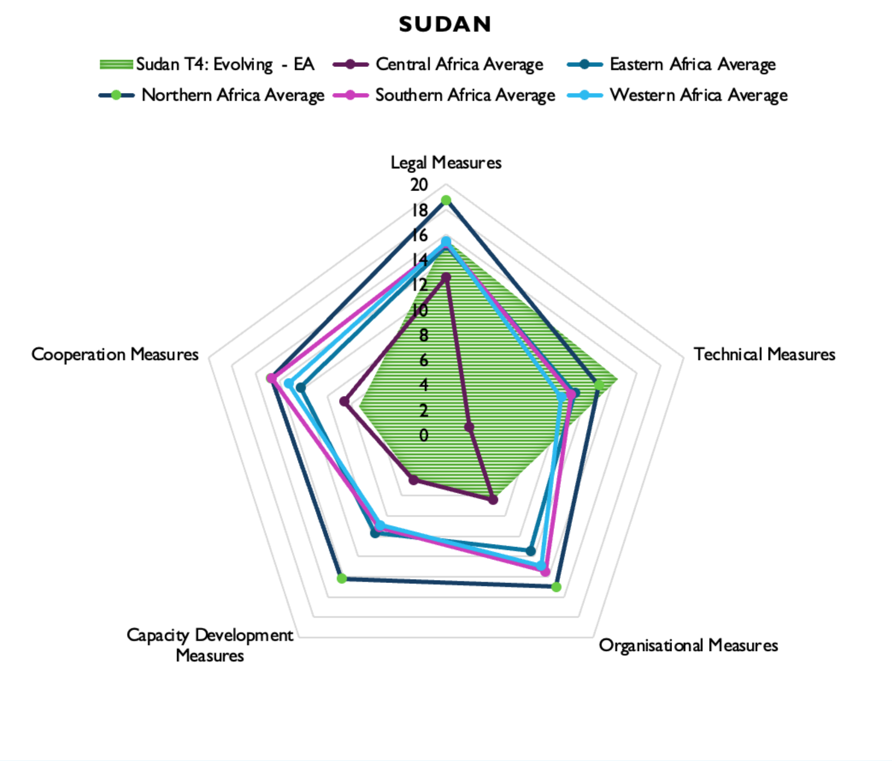


GCI 2024
AFRICA REGION
CONTINENT OUTLOOK
EA: Eastern Africa Region

Pillar(s) of Relative Strength
None

Area(s) for Priority Action
Legal Measures
Technical Measures
Organisational Measures
Capacity Development Measures
Cooperation Measures

SUDAN

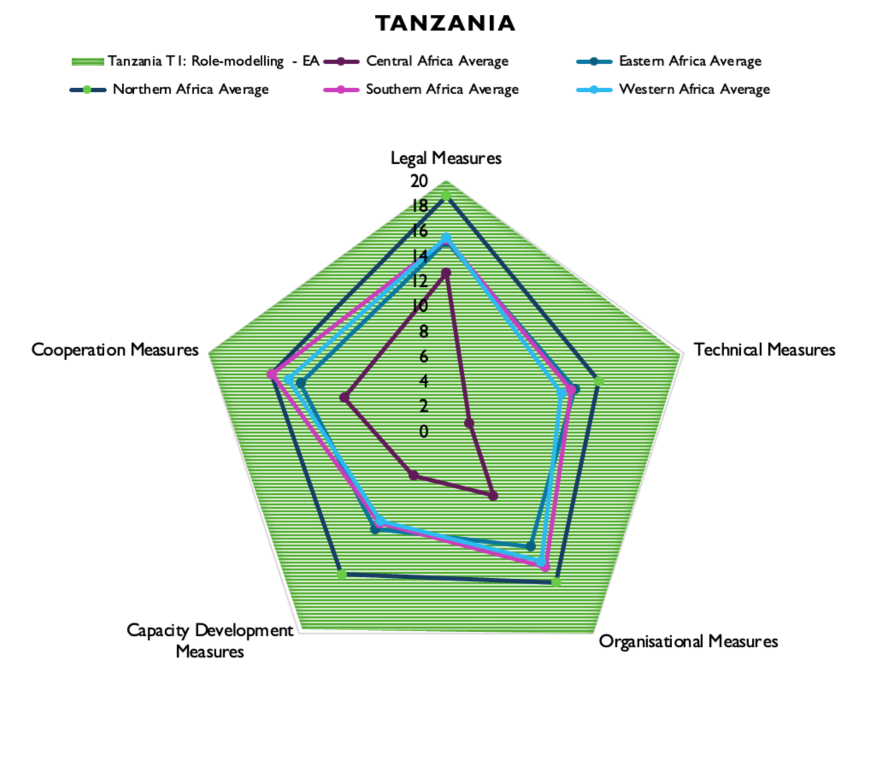


GCI 2024
AFRICA REGION
CONTINENT OUTLOOK
EA: Eastern Africa Region

Pillar(s) of Relative Strength
Technical Measures

Area(s) for Priority Action
Legal Measures
Organisational Measures
Capacity Development Measures
Cooperation Measures

TANZANIA



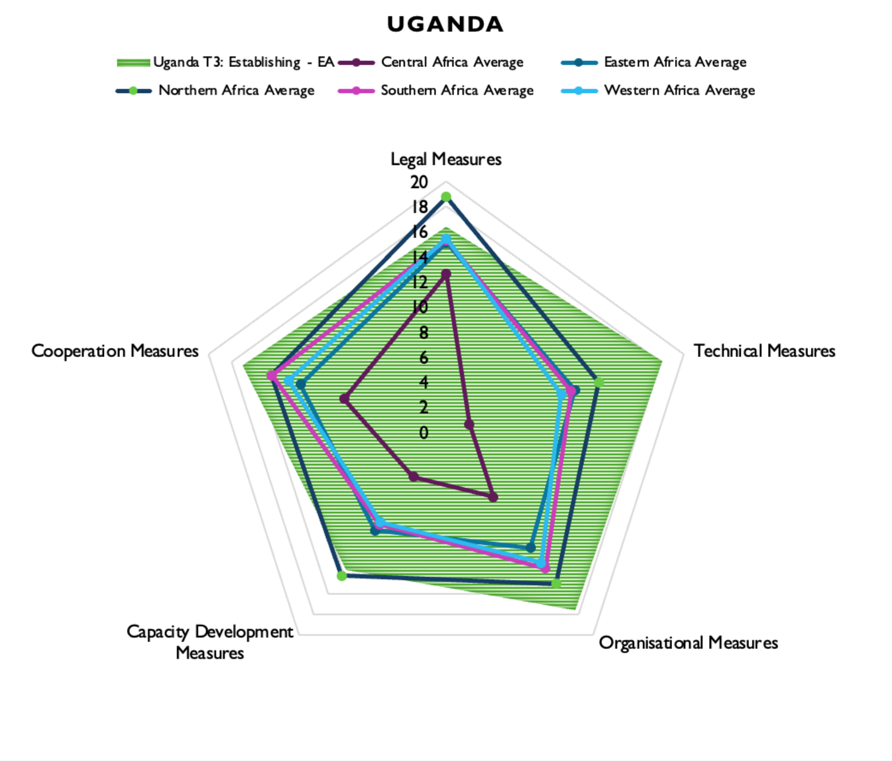
GCI 2024
AFRICA REGION
CONTINENT OUTLOOK
EA: Eastern Africa Region

Pillar(s) of Relative Strength
Legal Measures
Technical Measures
Organisational Measures
Capacity Development Measures
Cooperation Measures

Area(s) for Priority Action
Technical Measures
Capacity Development Measures

Role-modelling Strategic Options
Maintain efficacy of existing measures
Adopt a risk-based approach to build and extend measures across all pillars

UGANDA



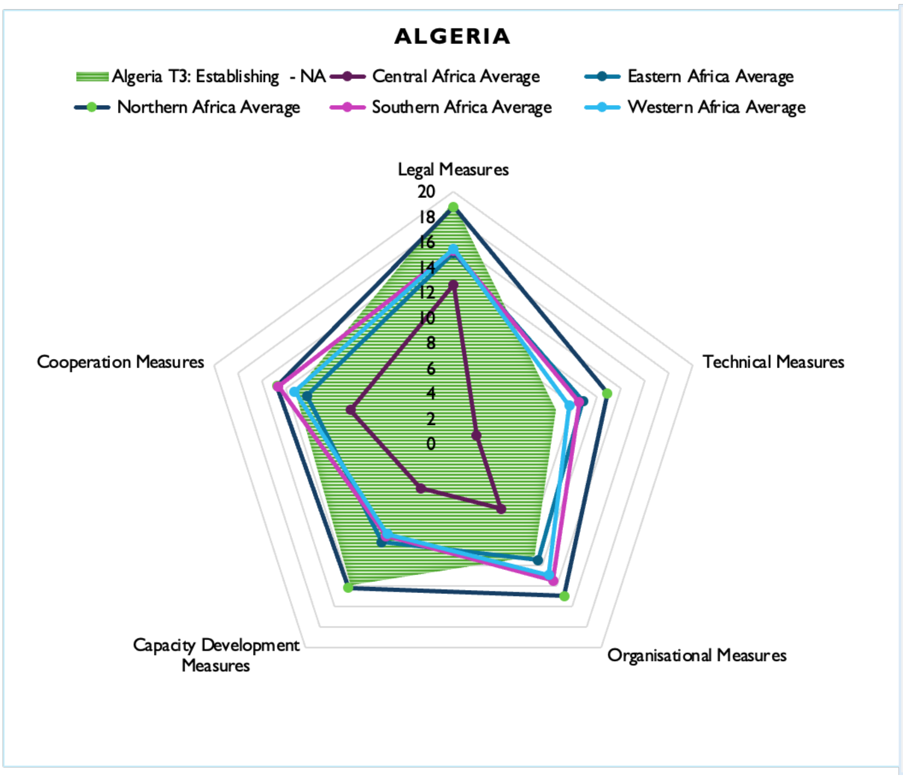
GCI 2024
AFRICA REGION
CONTINENT OUTLOOK
EA: Eastern Africa Region

Pillar(s) of Relative Strength
Technical Measures
Organisational Measures
Cooperation Measures

Area(s) for Priority Action
Legal Measures
Capacity Development Measures

Northern Africa

Algeria

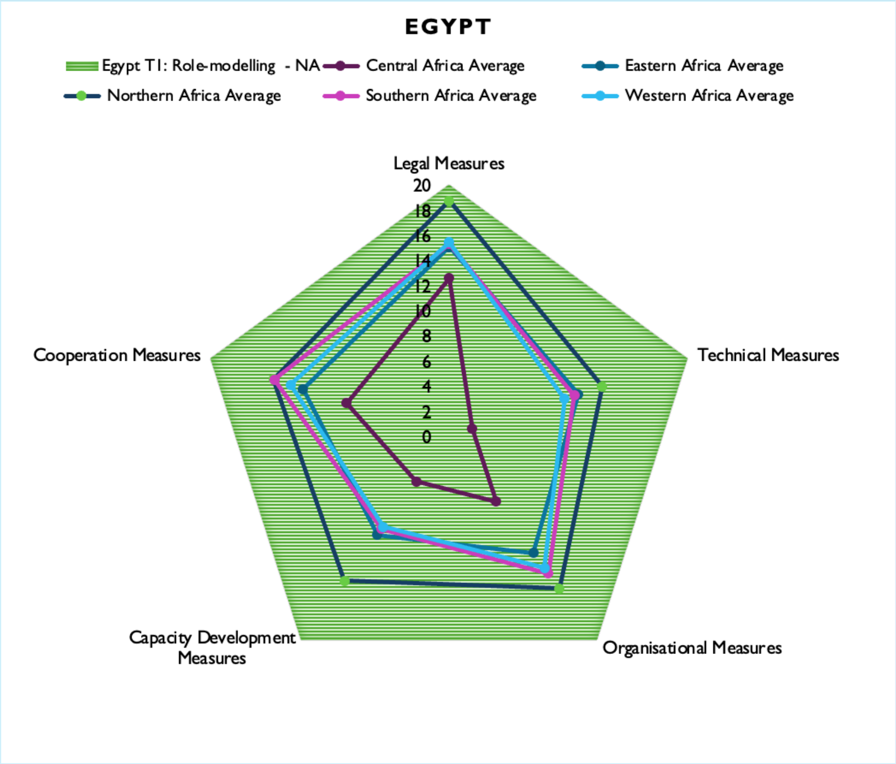


GCI 2024
AFRICA REGION
CONTINENT OUTLOOK
NA: Northern Africa Region

Pillar(s) of Relative Strength
None

Area(s) for Priority Action
Legal Measures
Technical Measures
Organisational Measures
Capacity Development Measures
Cooperation Measures

Egypt



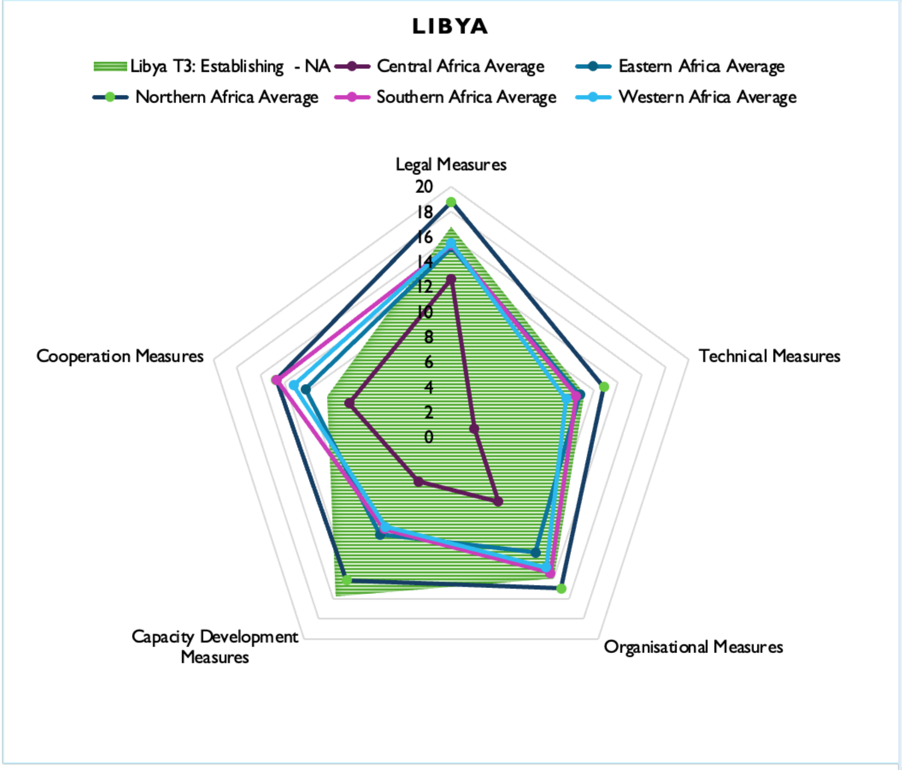
GCI 2024
AFRICA REGION
CONTINENT OUTLOOK
NA: Northern Africa Region

Pillar(s) of Relative Strength
Legal Measures
Technical Measures
Organisational Measures
Capacity Development Measures
Cooperation Measures

Area(s) for Priority Action
None

Role-modelling Strategic Options
Maintain efficacy of existing measures
Adopt a risk-based approach to build and extend measures across all pillars

LIBYA

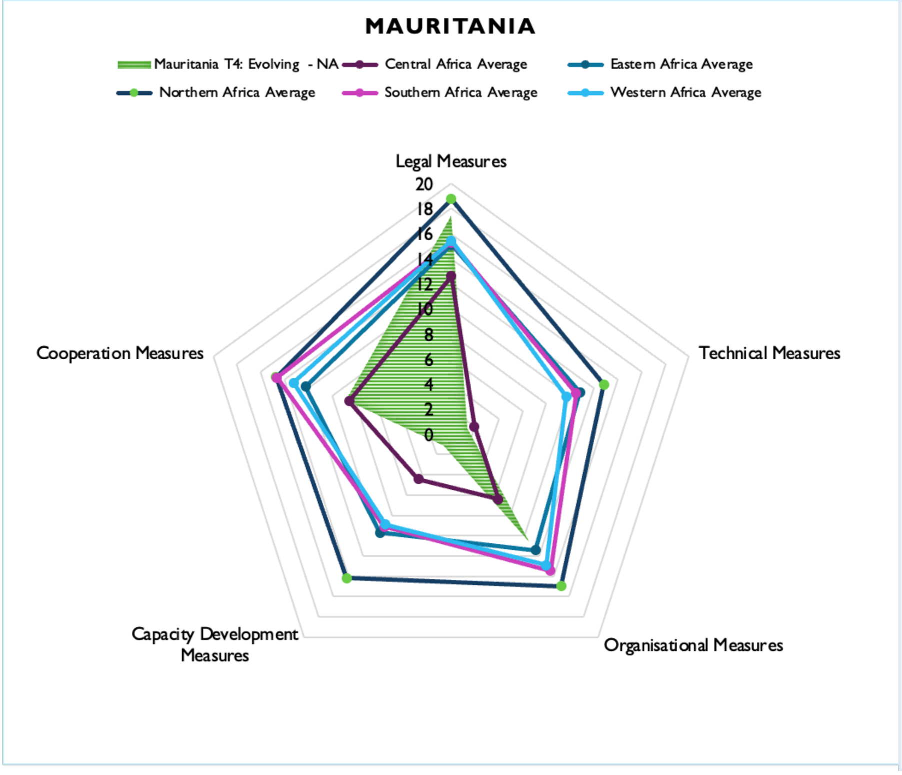


GCI 2024
AFRICA REGION
CONTINENT OUTLOOK
NA: Northern Africa Region

Pillar(s) of Relative Strength
Capacity Development Measures

Area(s) for Priority Action
Legal Measures
Technical Measures
Organisational Measures
Cooperation Measures

MAURITANIA

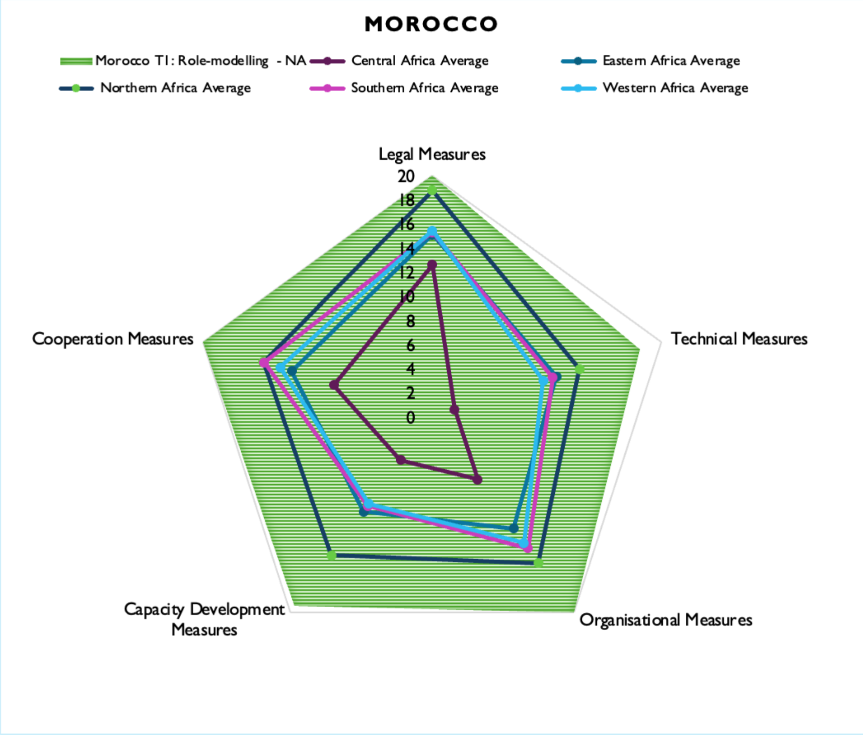


GCI 2024
AFRICA REGION
CONTINENT OUTLOOK
NA: Northern Africa Region

Pillar(s) of Relative Strength
None

Area(s) for Priority Action
Legal Measures
Technical Measures
Organisational Measures
Capacity Development Measures
Cooperation Measures

Morocco



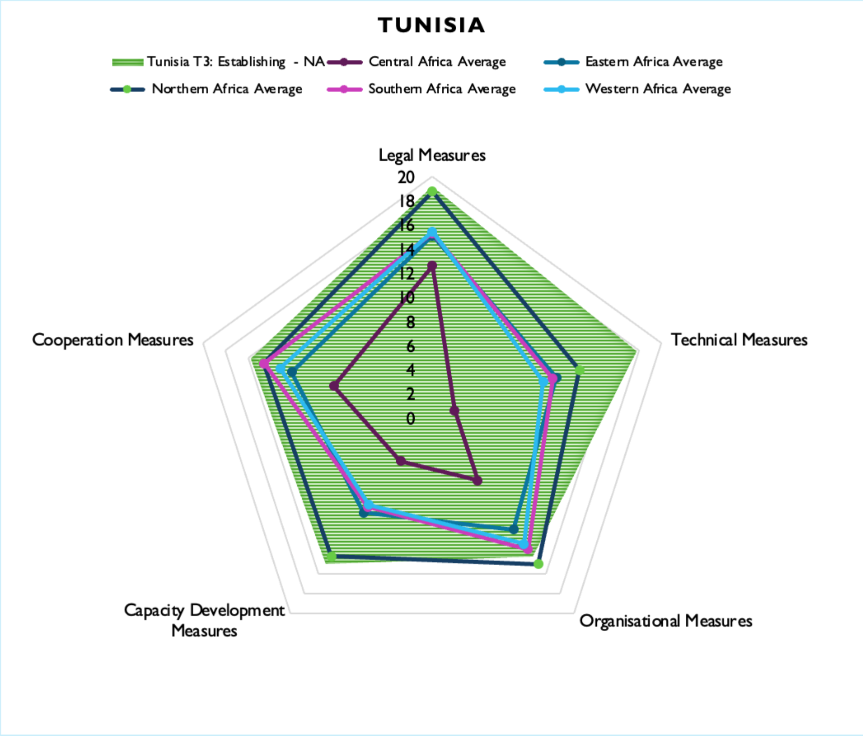
GCI 2024
AFRICA REGION
CONTINENT OUTLOOK
NA: Northern Africa Region

Pillar(s) of Relative Strength
Legal Measures
Technical Measures
Organisational Measures
Capacity Development Measures
Cooperation Measures

Area(s) for Priority Action
Technical Measures
Capacity Development Measures

Role-modelling Strategic Options
Maintain efficacy of existing measures
Adopt a risk-based approach to build and extend measures across all pillars

Tunisia



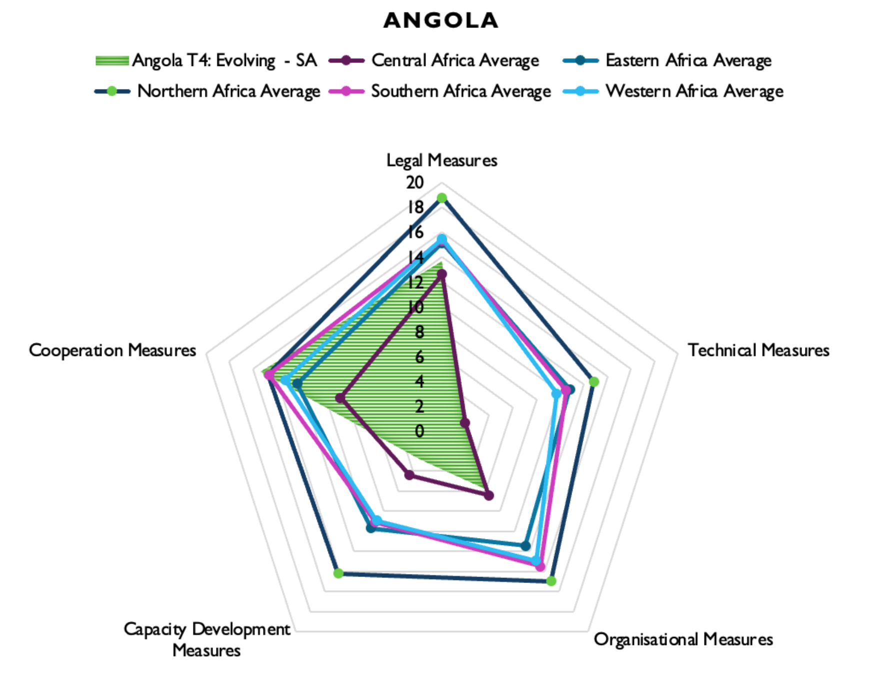
GCI 2024
AFRICA REGION
CONTINENT OUTLOOK
NA: Northern Africa Region

Pillar(s) of Relative Strength
Technical Measures
Cooperation Measures

Area(s) for Priority Action
Legal Measures
Organisational Measures
Capacity Development Measures

Southern Africa

Angola

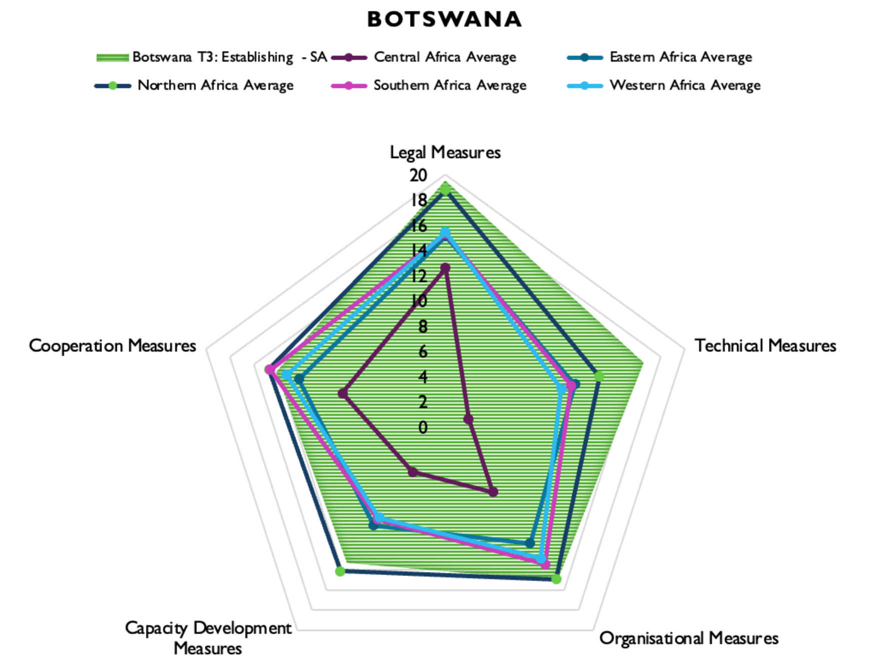


GCI 2024
AFRICA REGION
CONTINENT OUTLOOK
SA: Southern Africa Region

Pillar(s) of Relative Strength
None

Area(s) for Priority Action
Legal Measures
Technical Measures
Organisational Measures
Capacity Development Measures
Cooperation Measures

Botswana



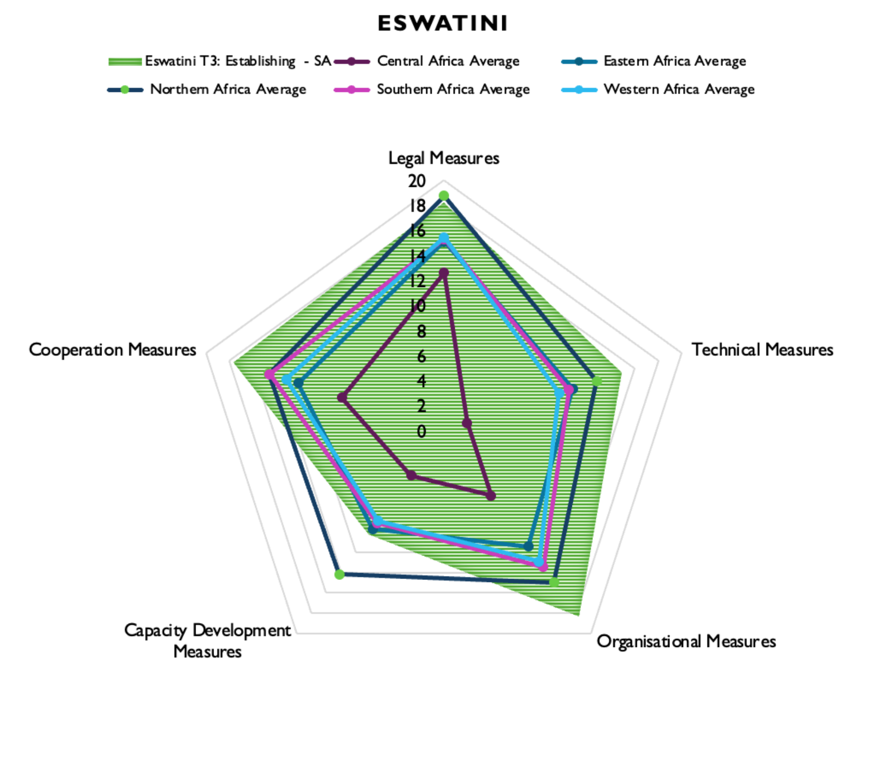
GCI 2024
AFRICA REGION
CONTINENT OUTLOOK

Pillar(s) of Relative Strength
SA: Southern Africa Region

Pillar(s) of Relative Strength
Legal Measures
Technical Measures

Area(s) for Priority Action
Organisational Measures
Capacity Development Measures
Cooperation Measures

Eswatini

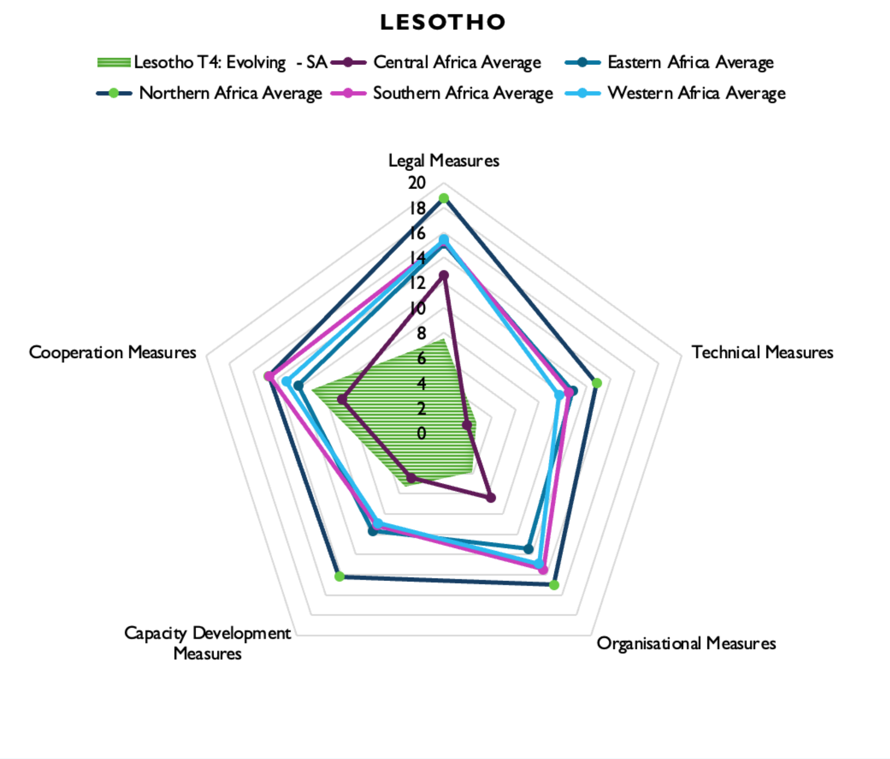


GCI 2024
AFRICA REGION
CONTINENT OUTLOOK
SA: Southern Africa Region

Pillar(s) of Relative Strength
Technical Measures
Organisational Measures
Cooperation Measures

Area(s) for Priority Action
Legal Measures
Capacity Development Measures

Lesotho

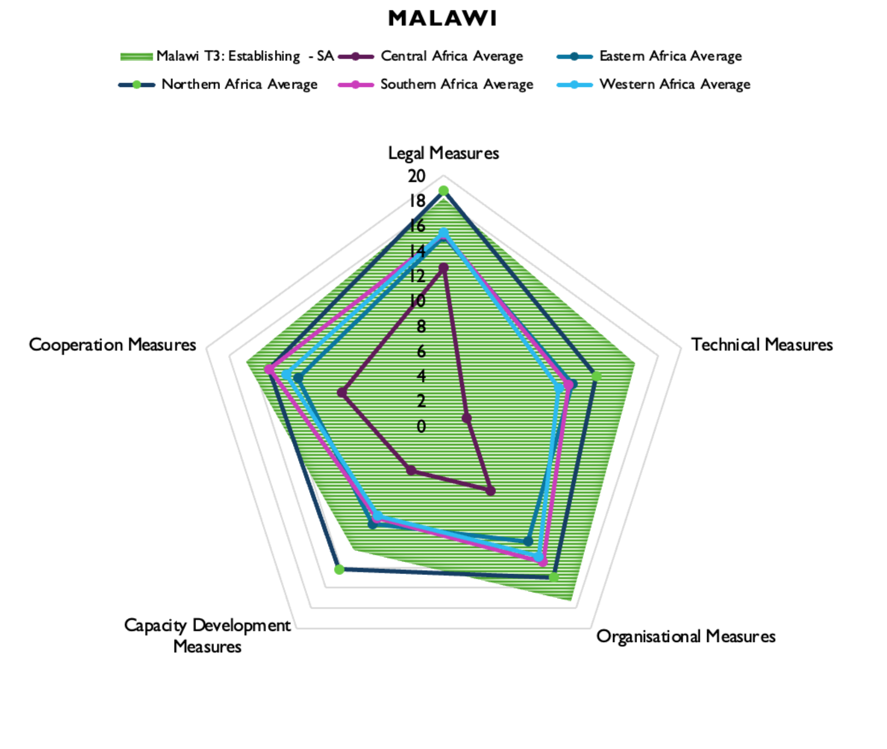


GCI 2024
AFRICA REGION
CONTINENT OUTLOOK
SA: Southern Africa Region

Pillar(s) of Relative Strength
None

Area(s) for Priority Action
Legal Measures
Technical Measures
Organisational Measures
Capacity Development Measures
Cooperation Measures

MALAWI

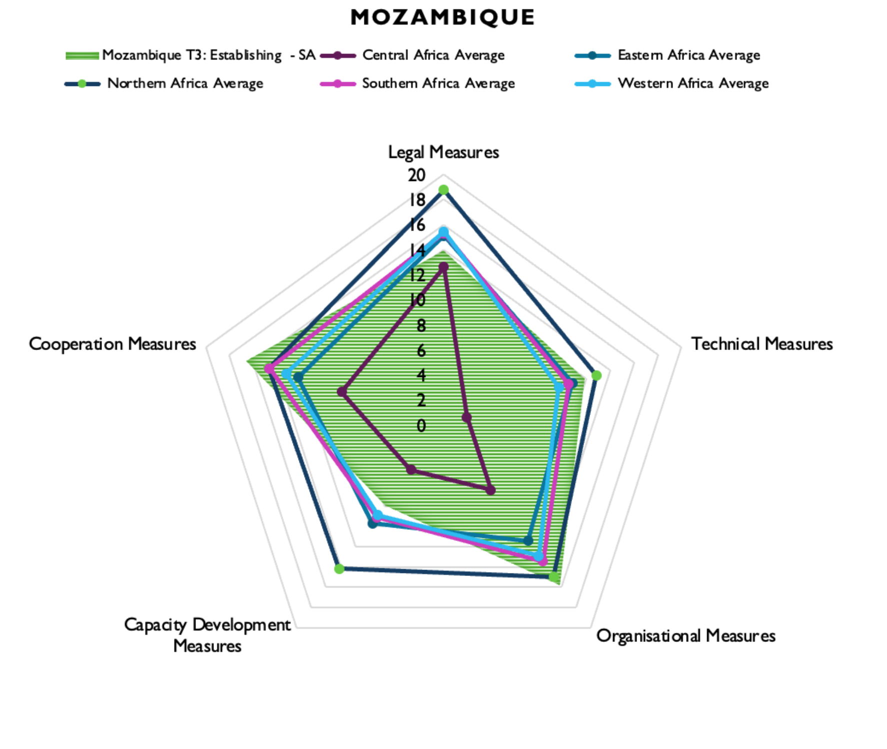


GCI 2024
AFRICA REGION
CONTINENT OUTLOOK
SA: Southern Africa Region

Pillar(s) of Relative Strength
Technical Measures
Organisational Measures
Cooperation Measures

Area(s) for Priority Action
Legal Measures
Capacity Development Measures

MOZAMBIQUE

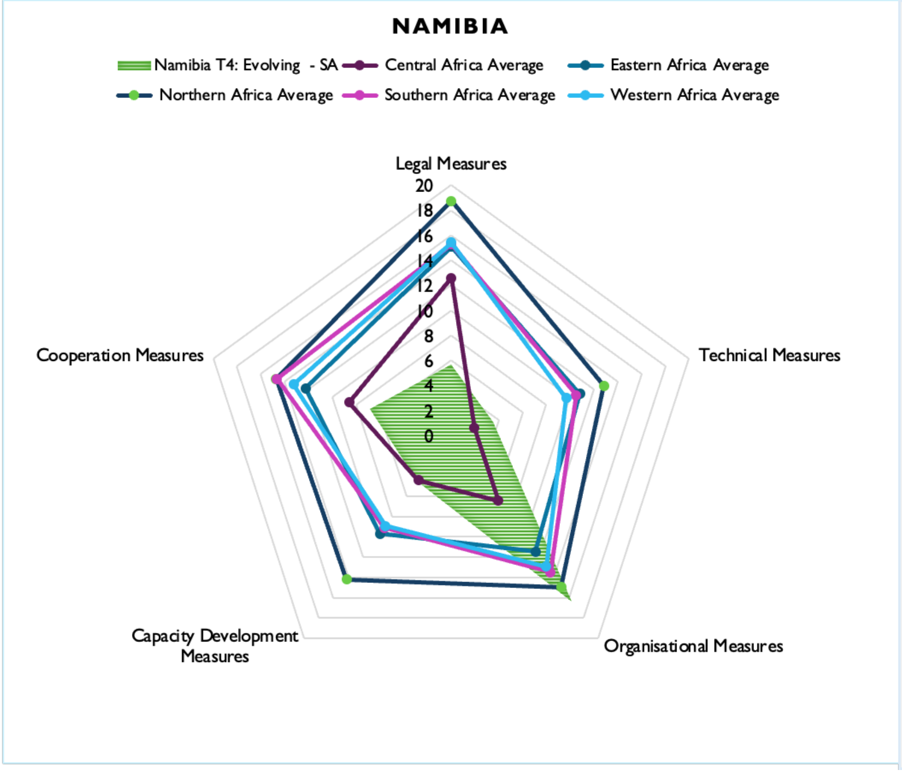


GCI 2024
AFRICA REGION
CONTINENT OUTLOOK
SA: Southern Africa Region

Pillar(s) of Relative Strength
Organisational Measures
Cooperation Measures

Area(s) for Priority Action
Legal Measures
Technical Measures
Capacity Development Measures

Namibia

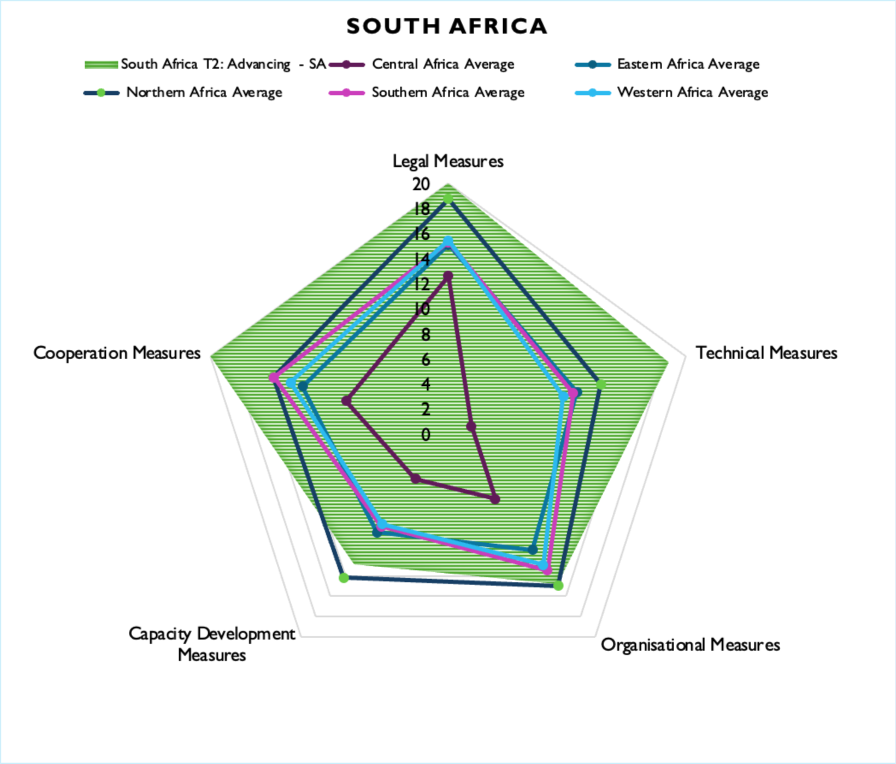


GCI 2024
AFRICA REGION
CONTINENT OUTLOOK
SA: Southern Africa Region

Pillar(s) of Relative Strength
Organisational Measures

Area(s) for Priority Action
Legal Measures
Technical Measures
Capacity Development Measures
Cooperation Measures

South Africa

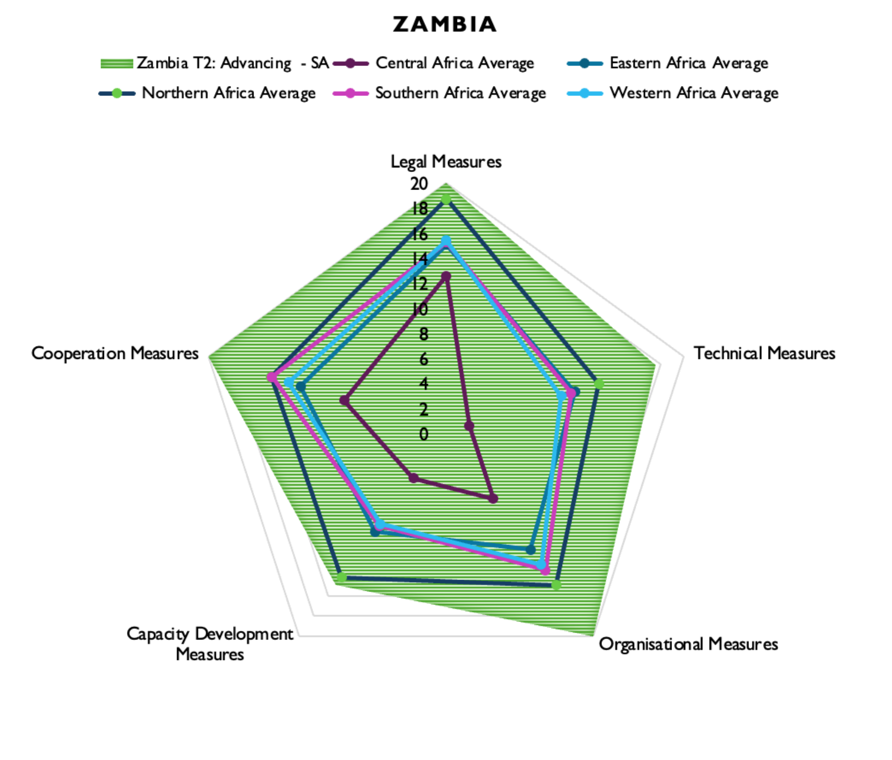


GCI 2024
AFRICA REGION
CONTINENT OUTLOOK
SA: Southern Africa Region

Pillar(s) of Relative Strength
Legal Measures
Technical Measures
Organisational Measures
Cooperation Measures

Area(s) for Priority Action
Technical Measures
Organisational Measures
Capacity Development Measures

ZAMBIA

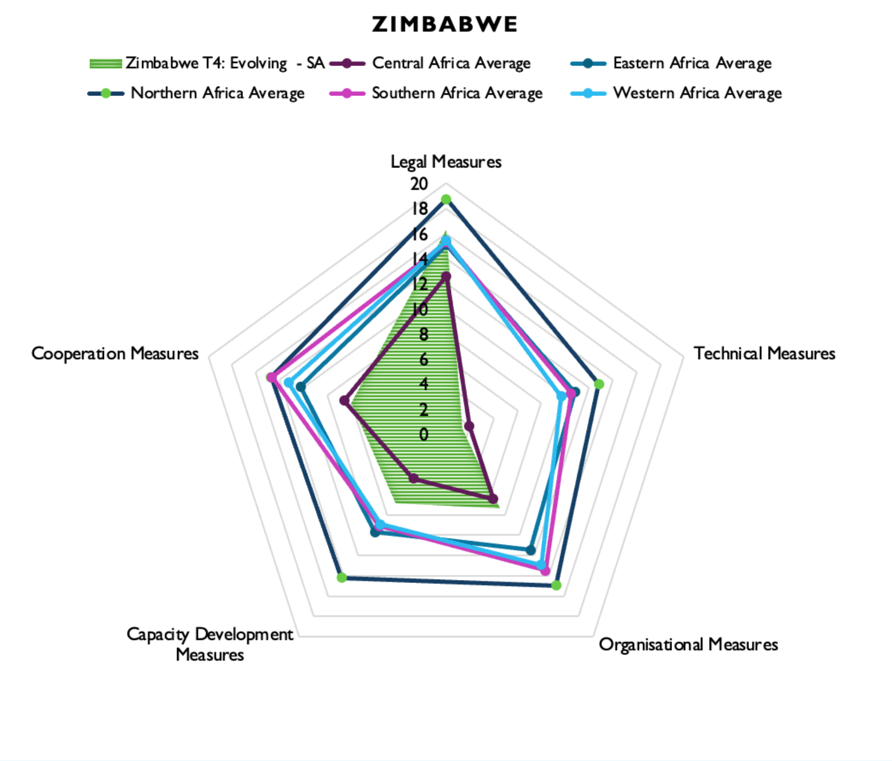


GCI 2024
AFRICA REGION
CONTINENT OUTLOOK
SA: Southern Africa Region

Pillar(s) of Relative Strength
Legal Measures
Technical Measures
Organisational Measures
Capacity Development Measures
Cooperation Measures

Area(s) for Priority Action
Technical Measures
Capacity Development Measures

ZIMBABWE



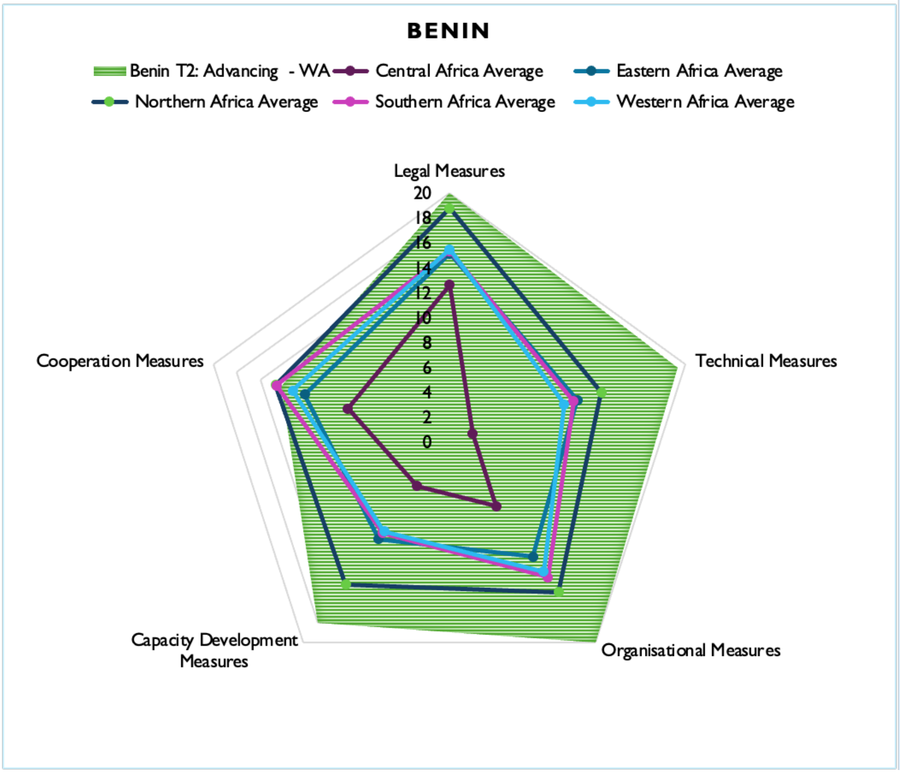
GCI 2024
AFRICA REGION
CONTINENT OUTLOOK
SA: Southern Africa Region

Pillar(s) of Relative Strength
None

Area(s) for Priority Action
Legal Measures
Technical Measures
Organisational Measures
Capacity Development Measures
Cooperation Measures

Western Africa

Benin

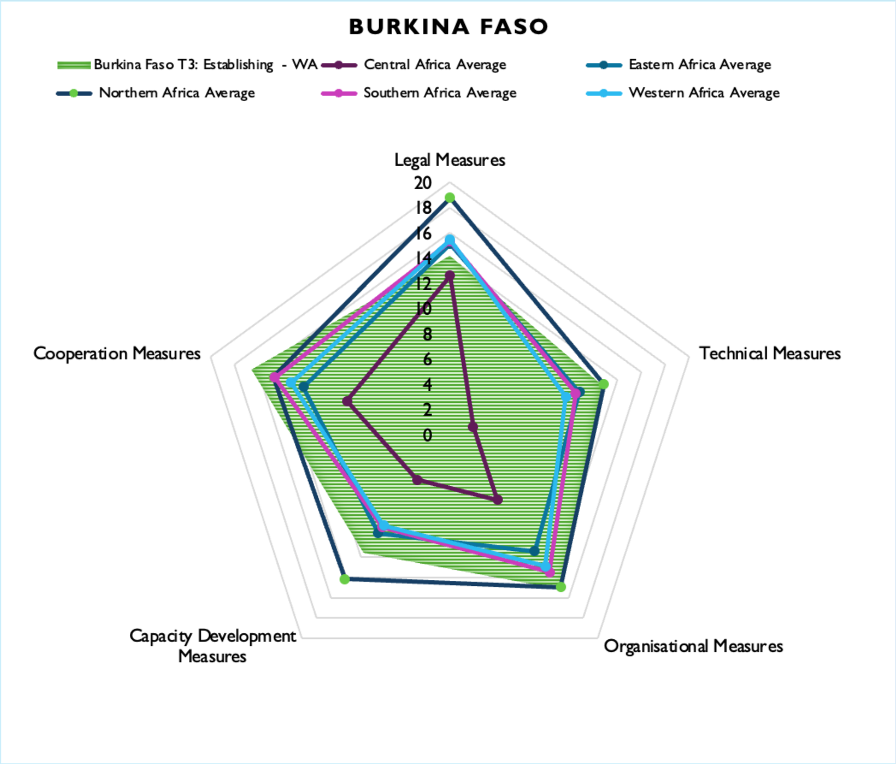


GCI 2024
AFRICA REGION
CONTINENT OUTLOOK
A:Western Africa Region

Pillar(s) of Relative Strength
Legal Measures
Technical Measures
Organisational Measures
Capacity Development Measures

Area(s) for Priority Action
Capacity Development Measures
Technical Measures
Cooperation Measures

Burkina Faso

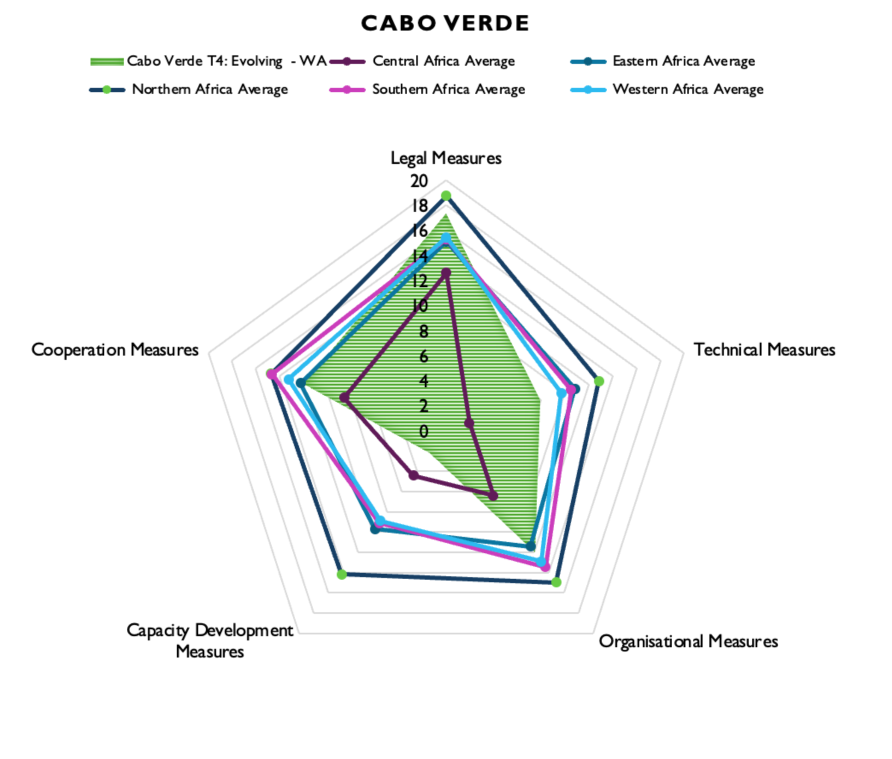


GCI 2024
AFRICA REGION
CONTINENT OUTLOOK
A:Western Africa Region

Pillar(s) of Relative Strength
Cooperation Measures

Area(s) for Priority Action
Legal Measures
Technical Measures
Organisational Measures
Capacity Development Measures

Cabo Verde

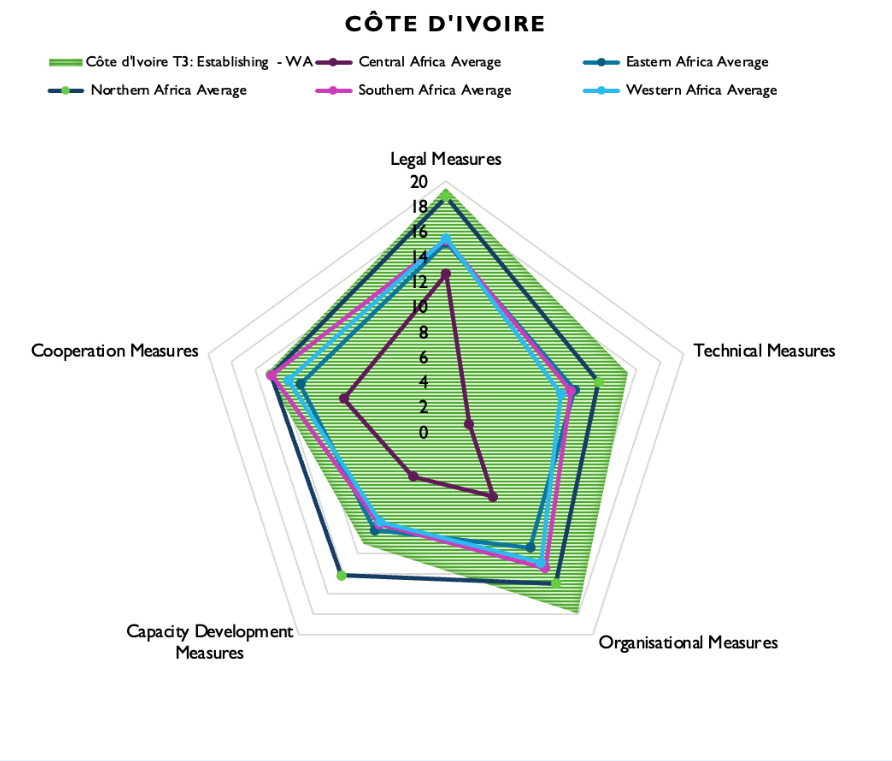


GCI 2024
AFRICA REGION
CONTINENT OUTLOOK
WA: Western Africa Region

Pillar(s) of Relative Strength
None

Area(s) for Priority Action
Legal Measures
Technical Measures
Organisational Measures
Capacity Development Measures
Cooperation Measures

Côte d'Ivoire

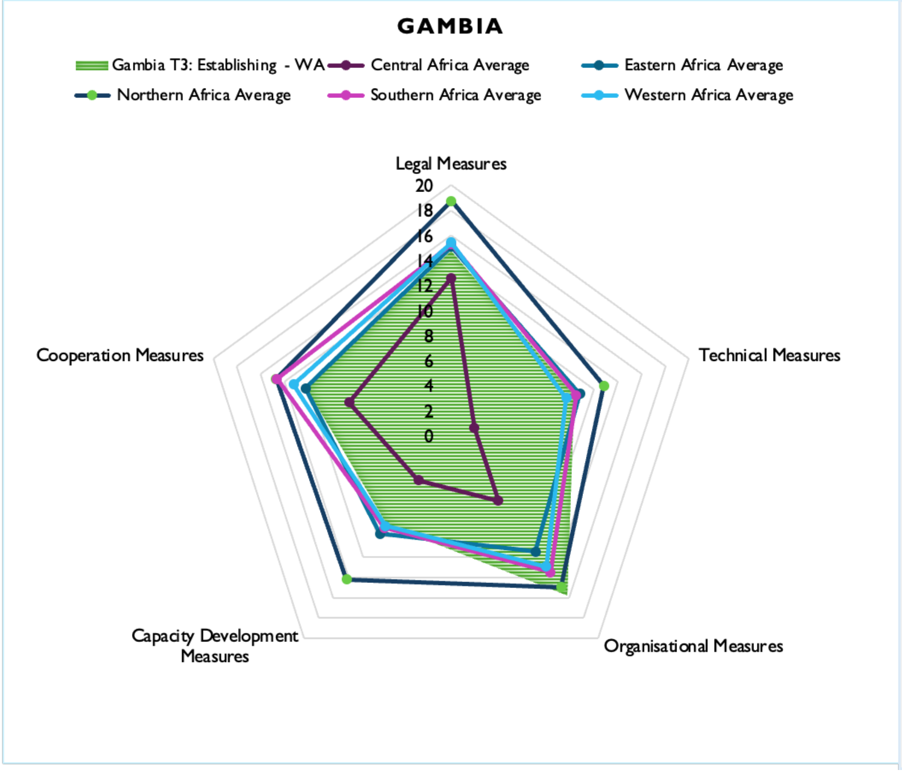


GCI 2024
AFRICA REGION
CONTINENT OUTLOOK
WA: Western Africa Region

Pillar(s) of Relative Strength
Legal Measures
Technical Measures
Organisational Measures

Area(s) for Priority Action
Capacity Development Measures
Cooperation Measures

GAMBIA

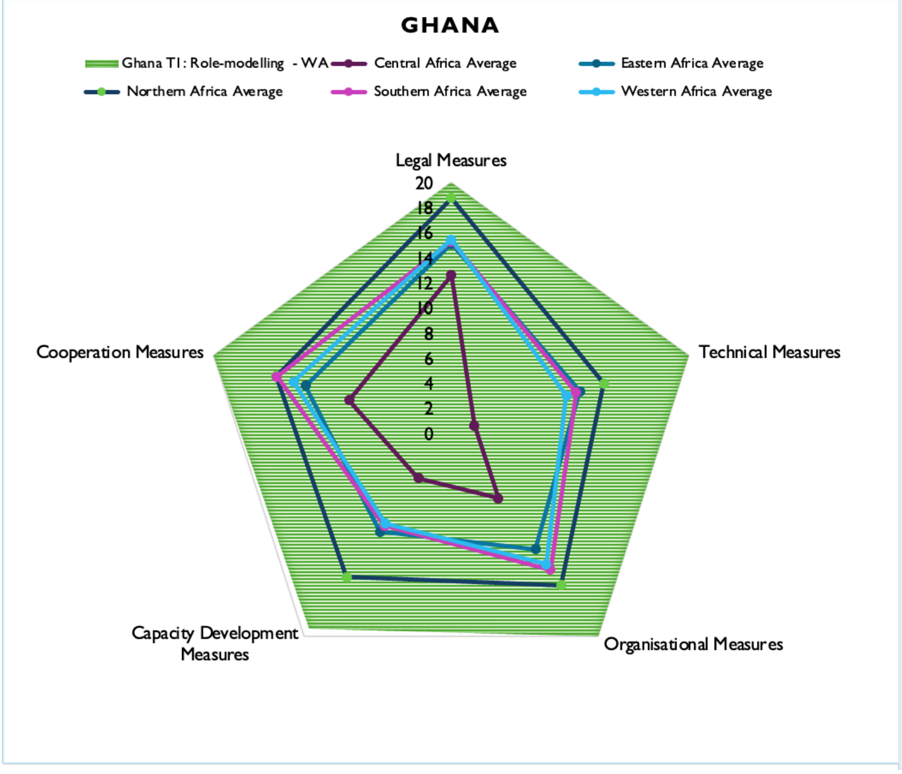


GCI 2024
AFRICA REGION
CONTINENT OUTLOOK
WA: Western Africa Region

Pillar(s) of Relative Strength
Organisational Measures

Area(s) for Priority Action
Legal Measures
Technical Measures
Capacity Development Measures
Cooperation Measures

GHANA



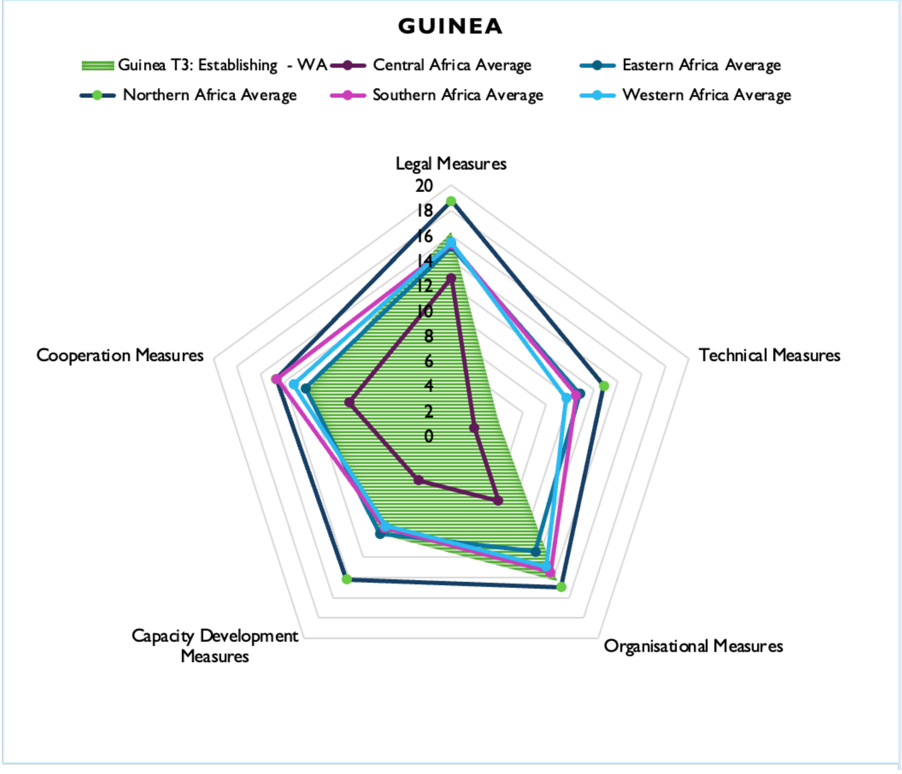
GCI 2024
AFRICA REGION
CONTINENT OUTLOOK
WA: Western Africa Region

Pillar(s) of Relative Strength
Legal Measures
Technical Measures
Organisational Measures
Capacity Development Measures
Cooperation Measures

Area(s) for Priority Action
Capacity Development Measures

Role-modelling Strategic Options
Maintain efficacy of existing measures
Adopt a risk-based approach to build and extend measures across all pillars

GUINEA

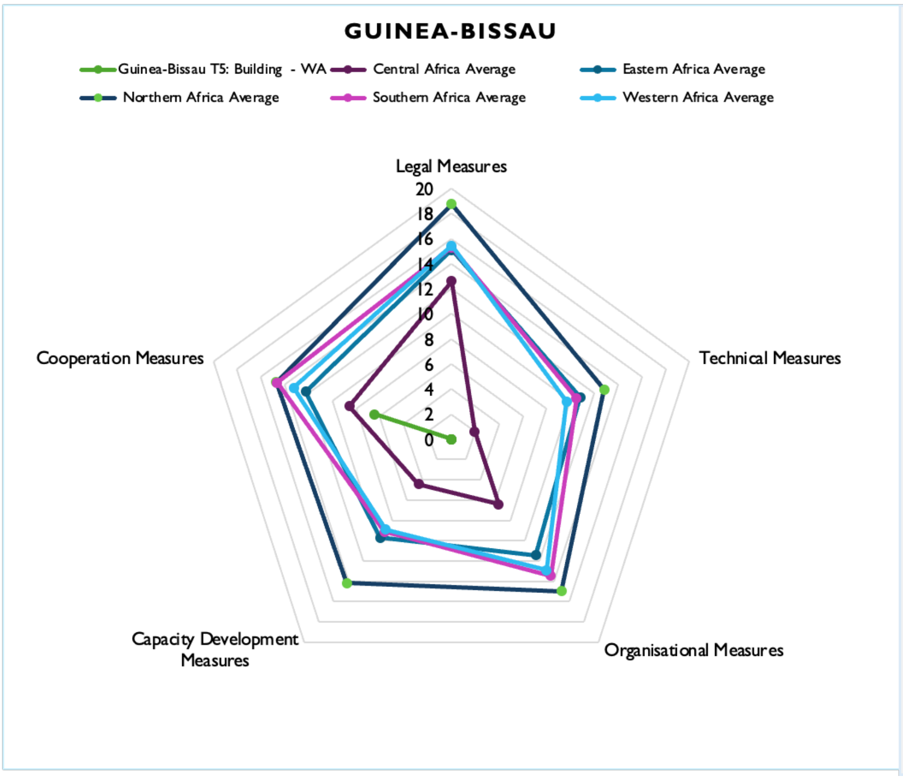


GCI 2024
AFRICA REGION
CONTINENT OUTLOOK
WA: Western Africa Region

Pillar(s) of Relative Strength
None

Area(s) for Priority Action
Legal Measures
Technical Measures
Organisational Measures
Capacity Development Measures
Cooperation Measures

GUINEA-BISSAU

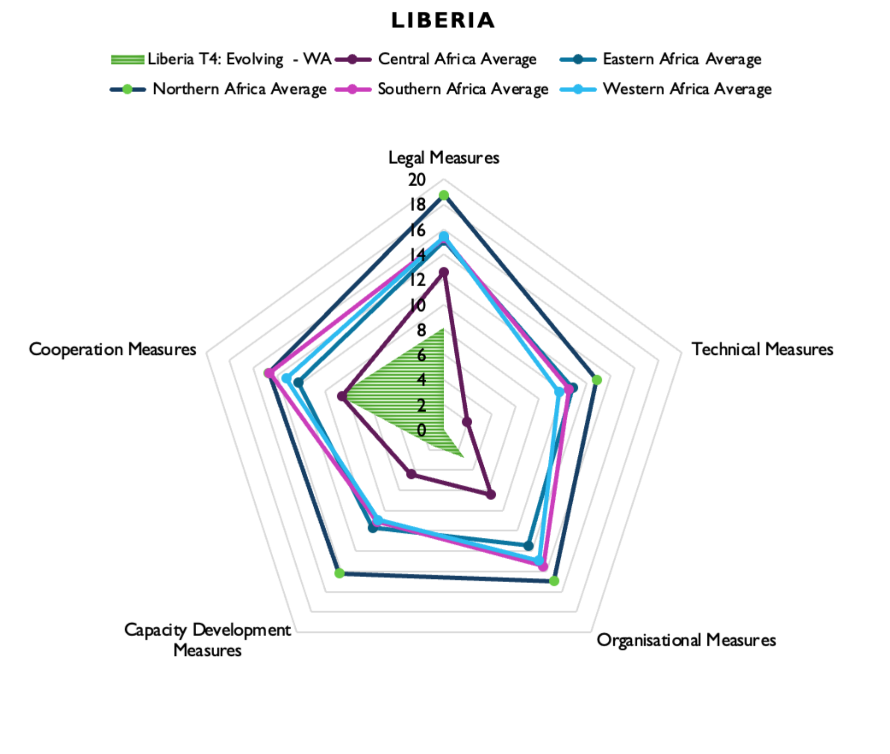


GCI 2024
AFRICA REGION
CONTINENT OUTLOOK
WA: Western Africa Region

Pillar(s) of Relative Strength
None

Area(s) for Priority Action
Legal Measures
Technical Measures
Organisational Measures
Capacity Development Measures
Cooperation Measures

Liberia

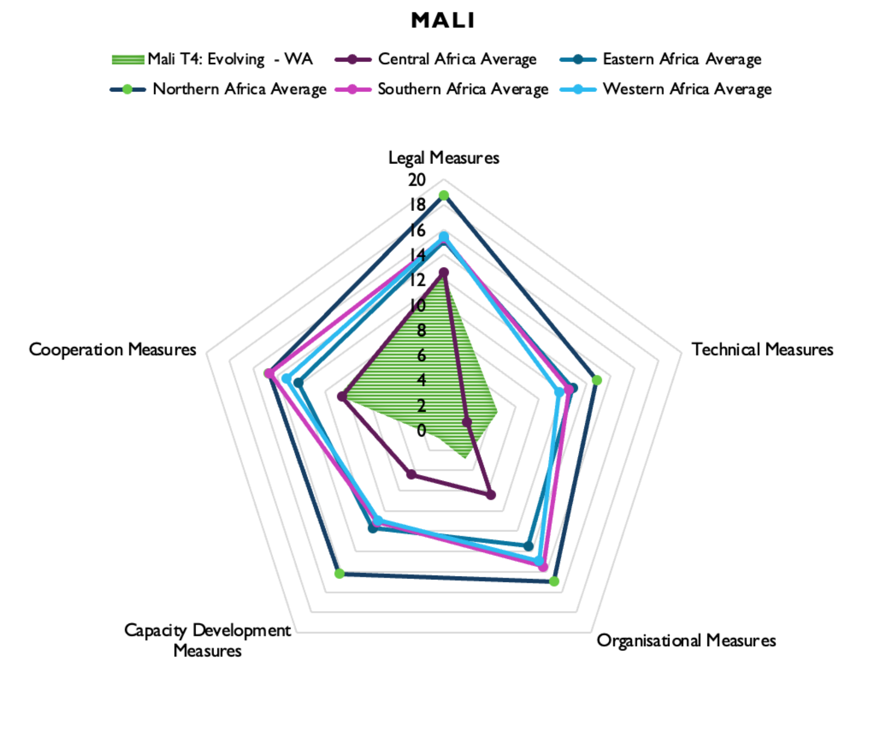


GCI 2024
AFRICA REGION
CONTINENT OUTLOOK
WA: Western Africa Region

Pillar(s) of Relative Strength
None

Area(s) for Priority Action
Legal Measures
Technical Measures
Organisational Measures
Capacity Development Measures
Cooperation Measures

Mali

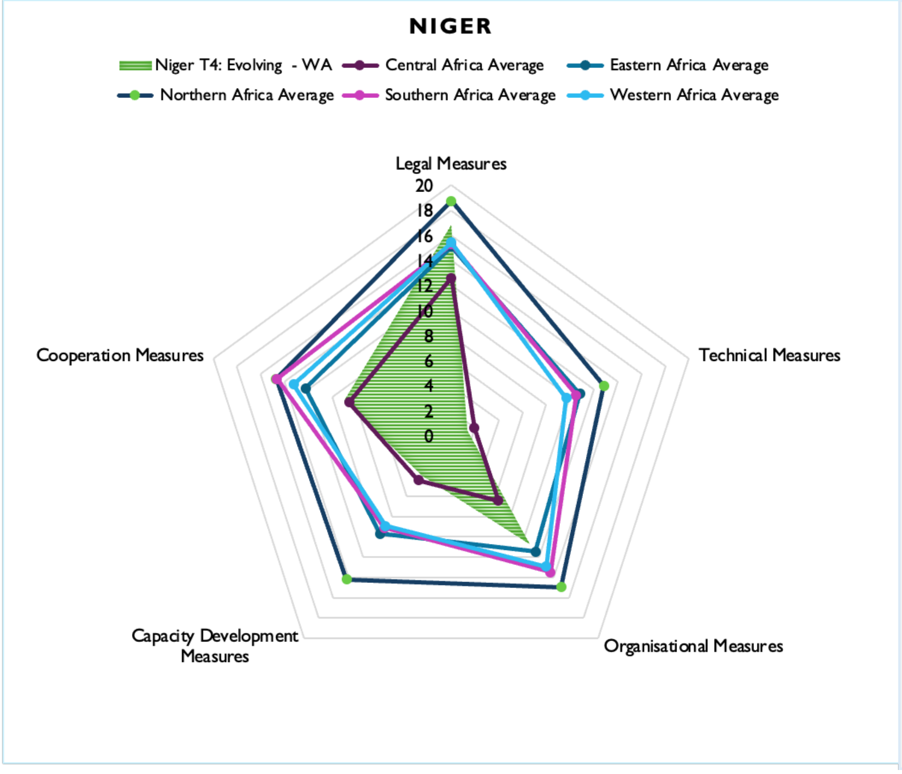


GCI 2024
AFRICA REGION
CONTINENT OUTLOOK
WA: Western Africa Region

Pillar(s) of Relative Strength
None

Area(s) for Priority Action
Legal Measures
Technical Measures
Organisational Measures
Capacity Development Measures
Cooperation Measures

NIGER

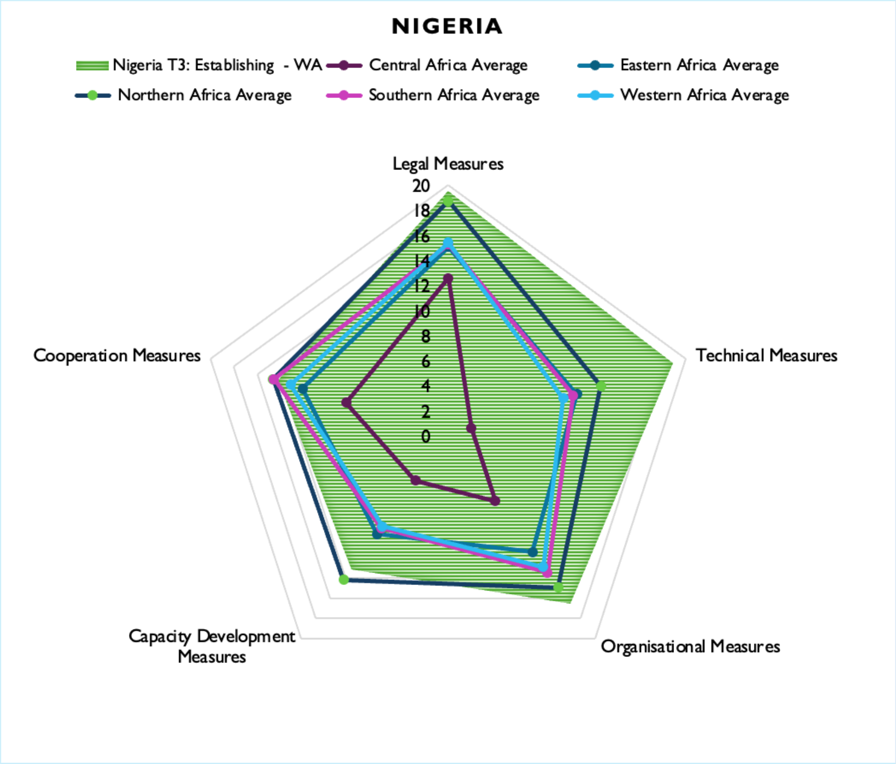


GCI 2024
AFRICA REGION
CONTINENT OUTLOOK
WA: Western Africa Region

Pillar(s) of Relative Strength
None

Area(s) for Priority Action
Legal Measures
Technical Measures
Organisational Measures
Capacity Development Measures
Cooperation Measures

NIGERIA

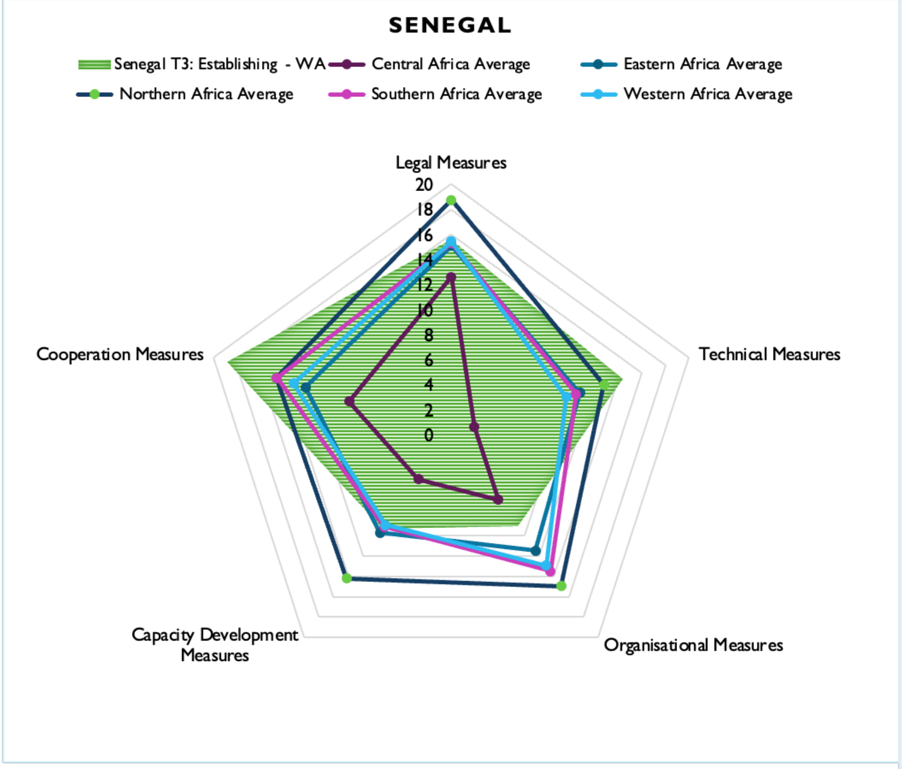


GCI 2024
AFRICA REGION
CONTINENT OUTLOOK
WA: Western Africa Region

Pillar(s) of Relative Strength
Legal Measures
Technical Measures
Organisational Measures

Area(s) for Priority Action
Capacity Development Measures
Cooperation Measures

SENEGAL

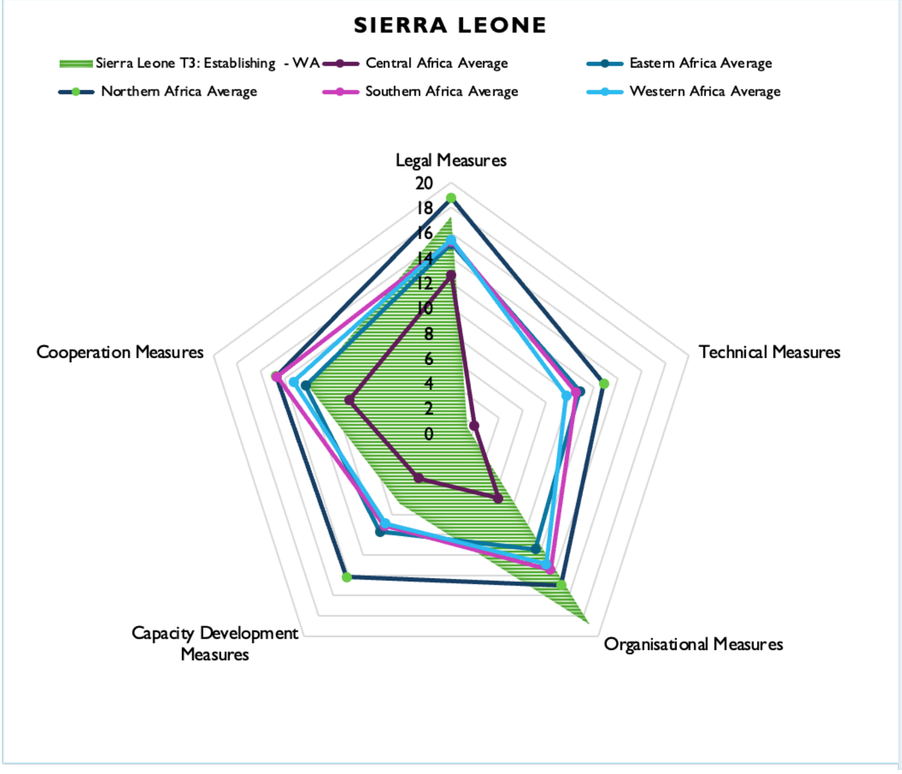


GCI 2024
AFRICA REGION
CONTINENT OUTLOOK
WA: Western Africa Region

Pillar(s) of Relative Strength
Technical Measures
Cooperation Measures

Area(s) for Priority Action
Legal Measures
Organisational Measures
Capacity Development Measures

SIERRA LEONE

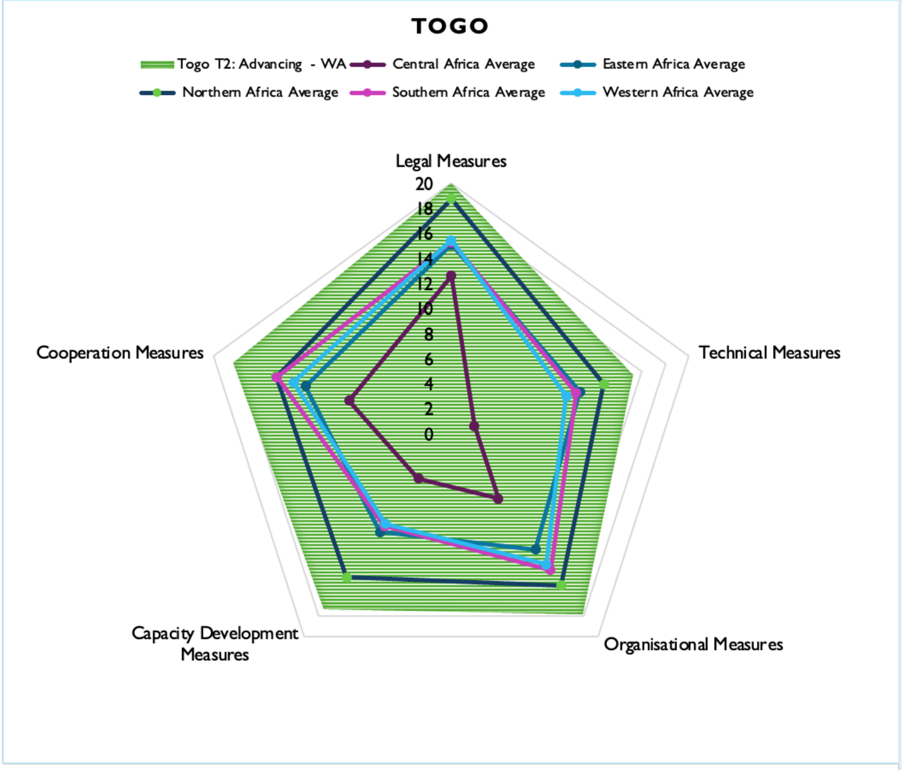


GCI 2024
AFRICA REGION
CONTINENT OUTLOOK
WA: Western Africa Region

Pillar(s) of Relative Strength
Organisational Measures

Area(s) for Priority Action
Legal Measures
Technical Measures
Capacity Development Measures
Cooperation Measures

Togo



GCI 2024
AFRICA REGION
CONTINENT OUTLOOK
WA: Western Africa Region

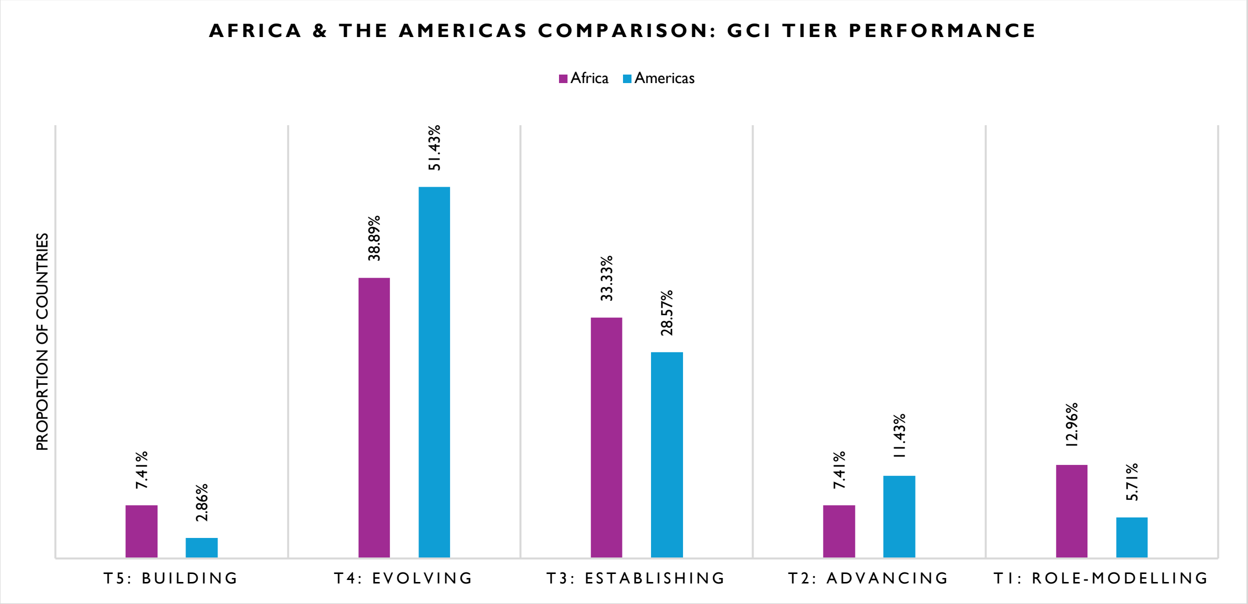
Pillar(s) of Relative Strength
Legal Measures
Technical Measures
Organisational Measures
Capacity Development Measures
Cooperation Measures

Area(s) for Priority Action
Technical Measures
Organisational Measures
Capacity Development Measures
Cooperation Measures

Comparative Analysis of Africa & The Americas

The comparative analysis examines 99 countries across Africa and the Americas, representing more than half of the member countries reviewed in the current edition of the GCI. These countries also form a significant portion of the Global South, encompassing Least Developed Countries (LDCs), Landlocked Developing Countries (LLDCs) and Small Island Developing States (SIDS). These countries are typically characterised by socio-economic vulnerabilities[63] and resource constraints and availabilities, which can impact national priorities, necessitating a skilful balance between addressing cybersecurity risks and meeting competing demands. By comparing the average performances of these countries and regions across cybersecurity pillars and tier levels, we can identify challenges, and emphasise positive insights, and opportunities. This approach aims to highlight key lessons, foster stronger collaboration and drive the development of more innovative and sustainable cybersecurity solutions for the Global South in particular.

FIGURE 10: AFRICA & THE AMERICAS GCI 2024 TIER PERFORMANCE



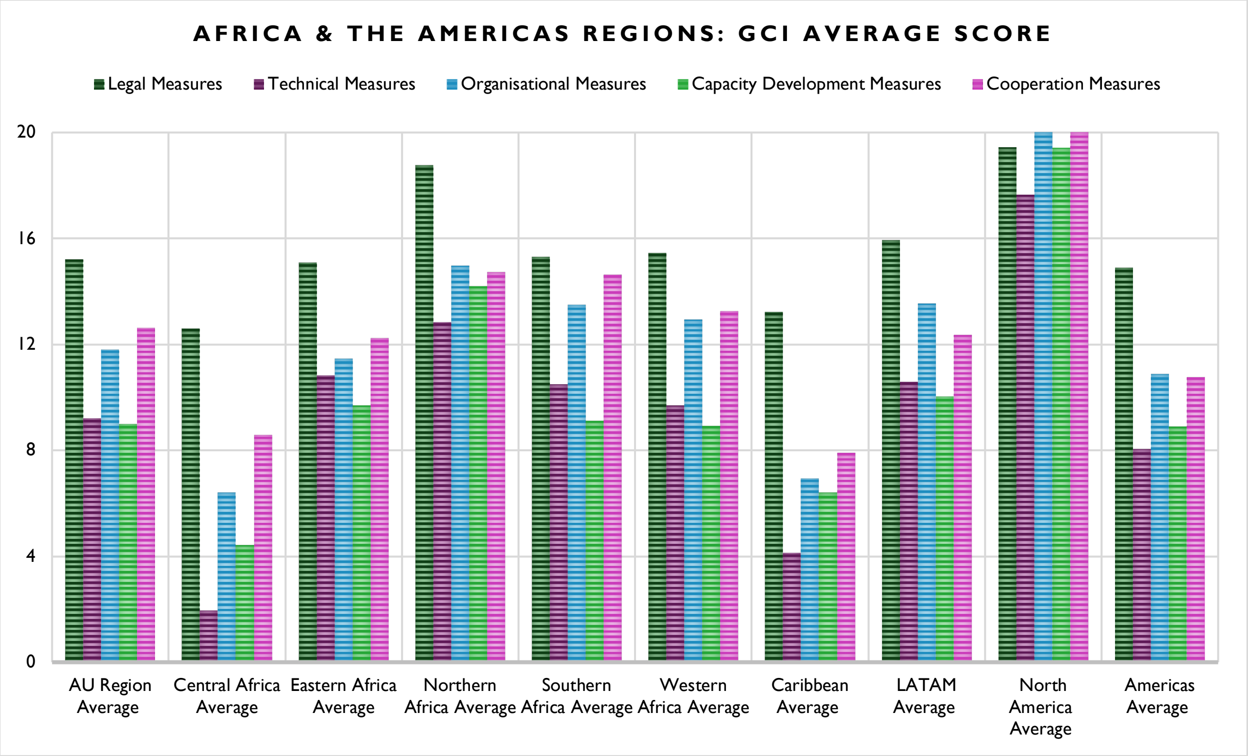
GCI Performance Trends

- Africa has a greater proportion of countries at the role-modelling stage than the Americas, and this trend is also evident when considering the combined role-modelling and advancing stages. This can be interpreted as Africa being more advanced in cybersecurity commitments, Figure 10.
- Both Africa and the Americas have a majority of countries at the Evolving and Establishing stages, suggesting that many of these countries are still in the early stages of adopting comprehensive cybersecurity measures and beginning to better establish more cybersecurity programs and initiatives to manage national cybersecurity risks. However, this trend also presents an opportunity for these countries to increase their adoption of appropriate measures to enhance their cybersecurity postures.

[63] See UNCTAD Report, Forging a Path Beyond Borders: The Global South, for example.

- Africa has a higher proportion of countries at the Establishing stage, signifying that many African countries are in the process of solidifying their cybersecurity structures and measures.
- The percentage of countries in the Building stage is lower in the Americas, indicating that fewer countries in the Americas are in the initial stages of developing their cybersecurity capabilities.

FIGURE 11: COMPARATIVE ANALYSIS: AFRICA & THE AMERICAS GCI AVERAGE



REGIONAL INSIGHTS

- North America dominates across all measures, reinforcing the USA and Canada's relatively more advanced and well-established cybersecurity measures and frameworks, Figure 11. Notably, several of the current good practice frameworks, such as the NIST cybersecurity framework, originate from that region and underscore the importance of research and innovation in fostering developments in cybersecurity.
- Northern Africa follows as the next best performer, where it shows a strong performance in legal measures. However, when compared with North America, opportunities for growth in technical, organisation, capacity building and cooperation measures are highlighted.
- Latin America, Eastern, Northern, Southern and Western Africa show closely similar cybersecurity commitments across all pillars with notable relative strengths in legal measures, as well as organisational and capacity development measures. Technical and capacity development measures exhibit more gaps in cybersecurity commitment levels.
- Central Africa and the Caribbean show the lowest level of cybersecurity commitment, with notable gaps in technical, organisational, capacity development and cooperation measures.

AFRICA AND THE WAY FORWARD

OVERVIEW

The GCI 2024 report reiterated that opportunities still exist for further coordinated actions, improvements and expansions of the breadth and depth of cybersecurity measures, irrespective of a country's overall score or level of tier performance[64]. With this in mind, we present recommendations based on the tier performances. Despite the tailored proposals, however, general recommendations based on each cybersecurity pillar can provide a baseline cybersecurity policy framework for countries to adopt. This general cybersecurity policy framework focuses on several key areas spanning the cybersecurity pillars.

Developing and Strengthening Legislative and Enforcement Frameworks: Implementing robust policies, laws and regulations to combat cyber threats and enhance cybersecurity governance. Countries with existing cybercrime and cybersecurity legal frameworks should also look to improve the effectiveness of these laws by developing and adopting policies, laws, and regulations addressing matters such as child online use and protection, critical information infrastructure protection, and other relevant subjects aligned with the evolving landscape.

Fostering Education and Workforce Development. Promoting digital and cybersecurity literacy, advancing research that addresses local issues, and raising awareness about cyber risks are fundamental to building resilience as countries pursue digital development goals. A key strategy includes integrating hands-on learning curricula that introduce cybersecurity skills to younger ages, embedding these concepts from primary school onwards. In addition, investing in training programs to develop a skilled cybersecurity workforce and incentivising research and innovation are crucial pillars. This holistic approach not only enhances current capabilities but also ensures a sustainable pipeline of talent and innovation to meet evolving cybersecurity challenges.

Encouraging Partnerships and Cooperation: Fostering collaboration between the private sector, government entities, civil society, and other stakeholders is an effective knowledge sharing mechanism. Our analysis has identified increased engagement in the region through PPPs to combat cybercrime and achieve shared cybersecurity goals. Countries can therefore explore these and other forms of partnerships to rapidly build capacity in specific areas, such as the deployment of national CERTs and tailored capacity-building activities.

Increasing Membership in Cybercrime and Cybersecurity Treaties. Only 16 African countries, or 29%, have ratified the Malabo Convention, and 13 or 24% are signatories only[65]. Eleven countries, or 20%, are parties to the Budapest Convention, with 8 or 15% invited to accede[66]. The overall status represents a significant opportunity for the continent to better harness the opportunities of multilateral cybersecurity cooperation.

Building Institutional Capacities: Countries should explore establishing and enhancing institutions like national CERTs and cybersecurity agencies to help address the current low representation of such entities across the continent. A phased development approach is also a viable option.

[64] https://www.itu.int/en/ITU-D/Cybersecurity/Documents/GCIv5/2401416_1b_Global-Cybersecurity-Index-E.pdf
[65] https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection
[66] https://www.coe.int/en/web/cybercrime/parties-observers

Investing in Capabilities and Technologies: Allocating adequate resources to adopt and improve cybersecurity technologies and capabilities is necessary in the current landscape. While considering other national priorities, emphasising cybersecurity is also essential for development.

Building on these baseline recommendations, we present some tailored proposals that also highlight shared patterns at different levels of cybersecurity commitment.

T5 Performers: Building

The initial stage of cybersecurity commitment highlights challenges in developing and implementing government-led initiatives across all cybersecurity pillars. These countries are faced with both common and diverse challenges, including workforce constraints, digital infrastructure challenges and conflicts. At this stage, it is prudent for countries to prioritise some of the cybersecurity pillars and establish plans and strategies for building a more robust, adaptive and resilient cybersecurity ecosystem.

- The absence of technical measures is a consistent challenge among the four countries. However, sectors such as finance and utilities often have well-established regulatory frameworks and cybersecurity standards. Countries can leverage the expertise, standards, and knowledge from these sectors to build incident response teams for instance. These teams can initially serve their specific sectors and eventually scale up to form national CERTs.
- Leveraging Public-Private Partnerships (PPPs) is another effective approach to scale up national cybersecurity efforts quickly. Several countries have successfully utilised this approach in diverse areas to increase their cybersecurity profiles. Countries at the Building stage can therefore prioritise specific areas under the cybersecurity pillars.
- As a signatory of the Malabo Convention, Guinea-Bissau has the opportunity to move to ratification and leverage collaboration with other member countries to enhance its legislative and law enforcement capacity and other areas. Other T5 performers should also consider membership in this treaty to enhance cooperation and leverage other potential benefits.
- Countries can leverage existing programs of inter-governmental organisations such as task forces in AFRIPOL and INTERPOL to build capacity for investigations and enforcement.
- Criminal codes should be reviewed to ensure they adequately address the evolving classification of cybercrime offences and revised as necessary. Additionally, there should be coordinated efforts to develop modern, technology-neutral cybercrime and cybersecurity laws that feature key provisions of multilateral treaties to better leverage harmonisation and cooperation.
- Based on Burundi's overall GCI scores, it can leverage certain opportunities to advance to the next level of commitment to cybersecurity.

T4 Performers: Evolving

Evolving performers are typically characterised by low performance across most pillars, particularly in technical, organisational, and capacity development measures. However, targeted efforts in legal and cooperation measures can serve as key levers to bridge the existing cybersecurity gaps and enhance overall GCI performance. At this level, countries should prioritise building capabilities in key cybersecurity pillars and indicators to bolster cybersecurity posture. Countries should adopt similar recommendations to countries at the Building stage, including the following:

- Continue the development of legislative frameworks to effectively address the evolving landscape and align the frameworks with prevailing good standards and conventions.
- The establishment of government and national CERTs should be prioritised to address the general low technical capabilities that exist among countries at the Evolving stage. A phased development approach may be adopted that sees the serial roll-out and expansion of the mandate of the CERT.
- Capacity development measures that target the general population and users of government services should be priorities to bring awareness to digital safety and cybersecurity risks. This is especially pertinent to countries with medium to high EGDI values. Counties at this level could start by undertaking general population awareness campaigns and adopt existing legislative constructs like community gatherings to collect relevant data that can enhance targeted awareness campaigns for special groups.
- Build and refine national cybersecurity strategies and governance structures to support a more secure digital transformation in government and other sectors.
- Several countries that are parties to at least one cybercrime/cybersecurity treaty should actively explore enriching collaboration opportunities to strengthen other cybersecurity pillars, including technical capabilities and capacity development initiatives. These countries include Cameroon (Budapest Convention), Angola, Congo Republic, Mauritania, Namibia, Niger, and São Tomé and Príncipe (Malabo Convention), which. Signatories should take urgent steps to ratify, while other countries should explore the potential benefits of cooperation through signing or accession.

Based on their respective overall GCI scores, Cabo Verde and São Tomé and Príncipe have the best opportunities to advance their cybercrime and cybersecurity capabilities in the areas discussed and advance to the Establishing stage of cybersecurity commitment.

T3 Performers: Establishing

The greatest opportunities for growth in cybersecurity reside in the technical, organisational, capacity development and cooperation measures. Legal measures reflect the strongest or most mature capabilities for many of the Establishing countries. At this level, countries should focus on developing maturity in key capabilities and strengthening overall cybersecurity posture. In that regard, countries should:

- Continue strengthening the legal framework to support national resilience, such as creating and revising legally binding rules for government agencies and critical infrastructure operators.
- Prioritise the establishment of government and national CERTs and develop the maturity of existing CERTs. This may mean increased engagement in awareness and education initiatives, more active participation in regional/international CERT networks, developing and leading cybersecurity drills, and developing threat intelligence networks to bolster threat intelligence information collection and sharing.
- Create new and revised NCS as well as strengthen NCS governance to enable improved accountability and monitoring to ensure that cybersecurity strategic goals are actions are met.
- Enrich capacity development measures to include more targeted campaigns, develop national curricula and promote growth in the cybersecurity industry through appropriate government incentives.

- Strengthen cooperation mechanisms include leveraging existing arrangements to realise capacity building and sharing outcomes and fostering increased inter-agency cooperation.

Based on their respective overall GCI scores, Nigeria, Tunisia, and Uganda have the best opportunities to advance their cybercrime and cybersecurity capabilities in the areas discussed and advance to the Advancing stage of cybersecurity commitment.

T2 Performers: Advancing

The Advancing countries have opportunities for growth in technical, organisational, capacity development, and cooperation measures, as some gaps are observed in these cybersecurity pillars. Countries at this stage should focus on holistic maturation and innovation across key cybersecurity pillars to enable more robust, adaptive, and resilient solutions as they advance their capabilities. Advancing performers should therefore consider the following:

- The legal measures pillar stands out for all these countries. However, opportunities exist in not only maintaining a robust cybercrime and cybersecurity framework that can effectively address current issues, including implementing laws in emerging areas, such as AI but also for countries to actively review these frameworks through practices such as RIAs to ensure that they are meeting desired goals. In addition, enhancing enforcement mechanisms such as implementing appropriate solutions to improve monitoring and enforcement of laws and ensuring that enforcement measures are effective and dissuasive.
- Ensuring that the roles and responsibilities of national CERTs are not only codified but also in keeping with current good practices and extending sectoral CERT activities, such as increased and active participation in national activities including leading national cybersecurity drills and information sharing schemes, are strategies that Advancing countries should consider. In addition, developing and refining national frameworks for cybersecurity standards adoption can help in improving transparency and accountability in cybersecurity governance.
- Strengthening the life cycle management and other good practices in implementing national cybersecurity strategies and providing increased attention to child online protection strategies and action plans are essential measures in combatting risks. Advancing countries should also investigate more relevant and precise cybersecurity metrics to measure the effectiveness of tracking risks to be able to adapt to the dynamic landscape.
- Capacity development measures have multiplier effects. In that regard, countries should continue to prioritise awareness, education, research and innovation. Areas of opportunities include reviewing and enhancing government incentives and prioritising key areas of cybersecurity such as research, workforce development, and professional training.
- Three of four countries are parties to at least one multilateral treaty. South Africa is invited to accede to the Budapest Convention and is a signatory to the Malabo Convention. This presents the opportunity for ratification of one or both major treaties, in the case of South Africa and for other countries to increase their participation in multilateral cybersecurity treaties and leverage cooperation and capacity-building opportunities. Opportunities also exist for countries to increase the extent and level of collaboration between government agencies, deepen bilateral agreements based on shared objectives, and continue to leverage PPPs to foster growth and innovation within the cybersecurity industry.

Based on their respective overall GCI scores, Benin and Zambia have the best opportunities to advance their cybercrime and cybersecurity capabilities in the areas discussed and advance to the Role-modelling stage of cybersecurity commitment.

T1 Performers: Role-modelling

Assessing the totality of the cybersecurity commitment of the Role-modelling countries highlights that growth opportunities exist in four pillars, while only the cooperation measures pillar stands out for all these countries. Hence, similar recommendations for Advancing countries are also applicable here. This involves deepening the extent of government-led cybersecurity initiatives across each pillar as well as maintaining role-modelling status. This means proactively responding to emerging threats, trends and developments in the cybersecurity ecosystem to manage risks and enhance capabilities more effectively. In addition, these countries should prioritise the holistic development and innovation of cybersecurity measures across all cybersecurity pillars. This helps to ensure that national cybersecurity capacity and infrastructure are robust, adaptive, and resilient, capable of effectively responding to the constantly evolving threat landscape. This approach not only mitigates current risks but also prepares for future challenges.

Several countries achieved an overall GCI score of 100 out of 100. This should be a strong motivation to maintain this score, actively examine potential gaps and vulnerabilities, and prioritise growth in strategic, defensive and responsive cybersecurity capabilities.

Conclusion

According to INTERPOL[67], African nations have made significant strides in enhancing their cyber defences and improving law enforcement responses. However, numerous challenges remain in establishing a comprehensive, coordinated, and sustainable approach to countering cybercrime across the continent. These challenges arise from a complex interplay of varied and interconnected factors, contributing to the widening disparity in cyber capabilities and government-led actions to combat cybercrime and enhance cybersecurity in the region.

To help tackle this problem, we probe the cybersecurity commitments of 54 African countries based on the GCI 2024 report. Our report seeks to feature national and regional trends, challenges, and notable activities undertaken by different governments and entities to enhance capabilities in the region and propose strategic actions to improve cybersecurity commitments.

Our analysis explores the GCI scores and rankings of countries within the AU region, spotlighting both strengths and areas needing improvement. We report on the progress made over the previous GCI edition and note that several countries in different AU regions have made significant progress, while a few countries appear to have stalled. The report delves into the relationship between the EGDI and GCI, uncovering significant disparities that could lead to heightened cybersecurity risks, underutilised cybersecurity capacity, and a decline in public trust in digital services in the region.

[67] INTERPOL African Cyberthreat Assessment Report 2024

Additionally, the study conducts a cross-hemispheric analysis of GCI performance in the Americas and Africa, highlighting both differences and similarities in experiences. These findings emphasise the importance of enhanced collaboration and knowledge sharing as strategic approaches to building cybersecurity capabilities, particularly in the Global South.

The report provides actionable recommendations for countries to improve their GCI scores and develop robust cybersecurity measures across key pillars. It also offers insights that enable countries to benchmark their performance against neighbouring, regional, and continental peers, fostering improved cooperation and cybersecurity governance to effectively combat cybersecurity risks, safeguard national sovereignty, and bolster economic prosperity.

About the Authors

Lenah Chacha

Lenah Chacha is a seasoned cyber and information security architect with over ten years of experience. She currently serves as the technical program manager at Upanzi Network project at Carnegie Mellon university that focuses on cybersecurity, digital identity, and financial inclusion. She leads work in identity, cybersecurity, e-government and the use of AI in various applications and fields.

Her expertise includes technical product management, protection of financial systems and environments, cybersecurity incident analysis and response, cybersecurity information risk analysis. Lenah has previously worked in the private, public and non-profit sectors and has a track recording of building and expanding services that respond to market demand. She is also a co-author of Evaluating Mobile Banking Application Security Posture Using the OWASP's MASVS Framework and later research on how secrets are handled in the most used mobile applications in Africa and their corresponding risks. Her recent interest combines cybersecurity and artificial intelligence and digital identity for cross-border movement of people and business.

One of her recent roles was serving as a Global Cybersecurity Index (GCI) consultant with the International Telecommunication Union's (ITU) GCI v5 project team, where she contributed to desk reviews, analysed submissions from ITU member states, and provided research insights for the final report. Lenah holds a Master's Degree in Information Technology from Carnegie Mellon University and certified Ethical hacker, Application security Engineer and Project Management Professional (PMP).

Corlane Barclay

Dr. Corlane Barclay is a distinguished professional with a terminal degree in Information Systems, an Attorney-at-Law and a certified Project Management Professional (PMP). She is a legislative drafter, program manager, researcher, and consultant based in the Caribbean, with extensive experience across the education, military, public, and private sectors.

Dr. Barclay is passionate about utilising her multidisciplinary expertise and leadership to advance digital security, policy and legislative development, particularly in matters that impact the region. This led to the establishment of DPO Caribbean, a premier advisory business specialising in data protection, cybersecurity, digital policy and legislation services. She is also the co-author of *Cybercrime and Cybersecurity in the Global South: Concepts, Strategies and Frameworks for Greater Resilience* (Routledge) and, over a decade ago, spearheaded the creation of a graduate course of study (MSc) in Information Systems Management at a tertiary institution in Jamaica. Additionally, she orchestrated several developmental milestones, including the establishment of the Caribbean Institute of Cyber Science at the Caribbean Military Academy and the drafting of a revised National Cybersecurity Strategy (NCS) and Action Plan as part of a national cybersecurity capacity-building program in Jamaica. Her most recent contributions include assisting regional intergovernmental bodies in advancing their strategic cybersecurity, privacy and data protection initiatives and her role as a Global Cybersecurity Index (GCI) consultant with the International Telecommunication Union's (ITU) GCI v5 project team, where she contributed to desk reviews, analysing submissions of ITU member states, and providing quantitative and qualitative research insights to the final report.

She recently published the report, *An Analysis of the Global Cybersecurity Index (GCI) 2024: Progress, Challenges and Opportunities for Cybersecurity in the Caribbean* (ISBN: 978 976 97440 0 4) as a call to action for Caribbean countries.

DPO Caribbean
20 West Kings House Road
Kingston, Jamaica, WI

ISBN: 978 976 97440 1 1

9 789769 744011

Published in Kingston
Jamaica, WI, 2024