CMAGE

Cyber Security Maturity Assessment Global Ecosystem

Tanzania Report

Maturity Model Assessment

2021

Report Structure

This document begins with a Highlight Report outlining key observations, followed by an introduction to the CREST maturity model structure, and an explanation of assessment methodology used in the research.

Five principal chapters contain detailed observations, one relating to each of the five dimensions of the Cyber security Maturity Assessment of the Global Ecosystem (CMAGE).

Each chapter begins with an overall assessment of the maturity of that particular ecosystem dimension, supported by written commentary highlighting significant observations.

A section-by-section assessment of the maturity of each indicator within the dimension follows.

The assessment of the maturity level assigned to each indicator is shown in the box immediately below the section heading. The box also contains the relevant maturity model definition (drawn from Appendix B).

A short commentary to support the maturity level assessment is also found in the corresponding section.

The report contains six appendices:

Appendix A Glossary
Appendix B Summary of Maturity Level Definitions
Appendix C Professional Certifications & Member Organisations
Appendix D Country Context
Appendix E Bibliography
Appendix F Endnotes

Three standalone extracts of this report are available on request from CREST International:

- A Highlights Report
- A banking sector cyber security risk posture report, and
- A guide to the CREST Maturity Model methodology.

For further information, please contact: info@crest-approved.org

Navigation Key

Move back a page | Move forward a page | Return to contents page | Move back to previously viewed page

Contents

Foreword from Ian Glover, President, CREST International

While organisations and individuals can take steps to maintain and improve their own cyber security, most of us live in a highly connected world.

We rely on the actions of others to play their part in sustaining our collective cyber security.

Knowingly or unknowingly, we are all part of a complex cyber security ecosystem which reaches far beyond the technology itself.

At the organisational level, the cyber security ecosystem comprises:

- Those who set strategy and policy
- Regulators who set and enforce standards
- Those who buy/consume cyber security services
- Those who provide cyber security services
- Those who facilitate information sharing
- Those who prevent and investigate cyber-crimes
- Those who educate, train and nurture the cyber security workforce

In this Cyber security Maturity Assessment of the Global Ecosystem (CMAGE) we have gathered evidence against twenty indicators across five specific dimensions of Tanzania's cyber security ecosystem. CREST has made both quantitative and qualitative assessments to arrive at an overall judgment as to Tanzania's level of cyber security.

This report draws upon open-source evidence gathered and records assessments we have made. While it will never be a complete assessment, it has been externally validated.

The relational database containing the CMAGE model has helped facilitate consistent application of the assessment and allows for ease of update and maintenance of the data, the ability to interrogate the data and to extend the model to include other factors. Importantly, it enables comparisons over time to understand if investments are providing tangible benefits.

The report is not an end in itself. It is the benchmarked starting point for a journey of collaboration between CREST and national and international stakeholders with a shared interest in improving the overall cyber security posture in Tanzania.

Unashamedly, the endpoint - at least from a CREST perspective - is that every financial services institution in Tanzania becomes resilient to cyber-attacks, protecting all stakeholders, particularly the poorest in society.

I would particularly like to thank the Bill & Melinda Gates Foundation for its vision and support in this endeavour.

I would also like to thank all those in Tanzania and the international community who have contributed to this report. Finally, I want to thank everyone at CREST International for their efforts in producing this report and their commitment to the journey that we are all now undertaking.

Ian Glover
President
CREST International

Highlights Report

Background

CREST International seeks to help build capacity, capability, and consistency in Tanzania's cyber security ecosystem. The underlying aim is that every financial institution in Tanzania will become more resilient to cyber-attacks to better protect everyone in society.

A comprehensive understanding of the current situation is an essential starting point. CREST's evaluation methodology, the Cyber security Maturity Assessment of the Global Ecosystem (CMAGE), provides the evidence required to build a practical action plan, focused on areas where improvements are most needed.

It is also a benchmark that allows relatively quick and easy re-assessments to establish whether progress is being made.

The CMAGE contains many months of research and assessment, validated by local subject matter experts.

The results are complex. Inevitably there are areas of good practice and areas where investments of time, effort and money are needed.

The ecosystem is interconnected and interdependent. Making improvements in one part of the ecosystem will bring benefits to other areas as well.

Maturity Model Assessment Summary

Overall Uganda Ecosystem

Maturity Level 2

Having gathered and analysed evidence from multiple sources, CREST assesses Tanzania's cyber security ecosystem to be at Maturity Level 2, a level termed 'Transitional'.

Tanzania has clearly started a developmental journey towards improving all aspects of its cyber security ecosystem.

With concerted effort, it should be possible to progress to Maturity Level 3 by adopting international good practice and utilising IPR-free guidance (being created by CREST International as part of the project's second stage).

Highlights Report

Summary of Observations

The overall maturity assessment for Tanzania's cyber security ecosystem is based upon the assessed maturity of five constituent Dimensions:

1. National Strategy & Capabilities
2. Information Sharing
3. Services Provision
4. Professional Development
5. Banking Sector Risk Profile

Dimensions and Indicators

Within each **Dimension** are a number of **Indicators**, each of which has been assessed against a series of maturity level definitions following the gathering and analysis of evidence.

Qualitative Assessments — **1-4**

Qualitative Assessments — **5**

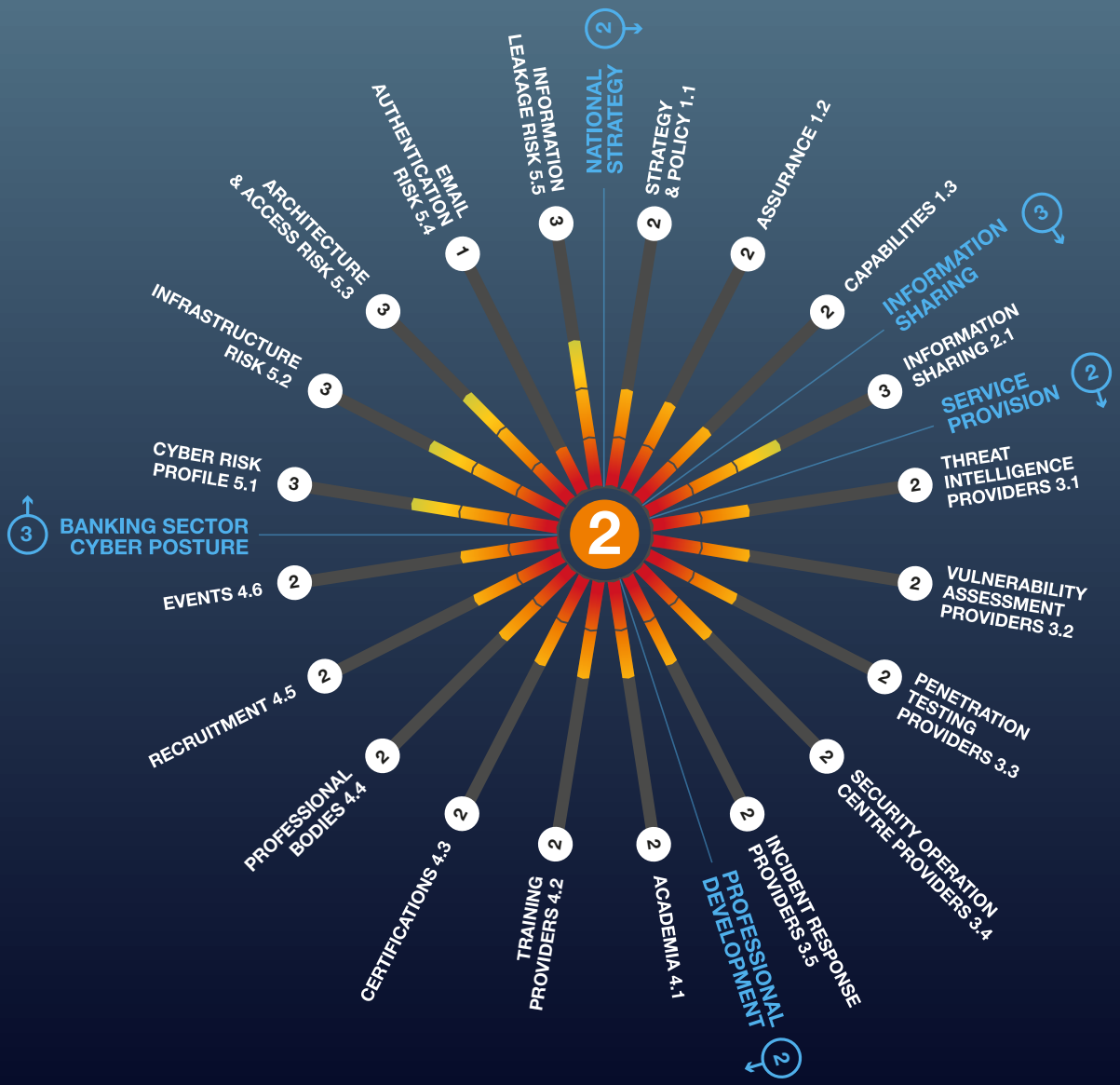
Maturity Scores

A summary of the maturity scores for the five Dimensions and the twenty constituent Indicators are depicted on the following 'starburst' diagram. The length of each radial relates to the assessed maturity of that particular Indicator as confirmed by the number on the white disc at its end. The radials are also colour-coded along their length – as follows:

RED	Level 1
AMBER	Level 2
YELLOW	Level 3
GREEN	Level 4
BLUE	Level 5

Highlights Report

Summary of Observations (continued)



Maturity Levels

1 Emerging
2 Transitional
3 Organised
4 Dynamic
5 Leading

Summary Assessment

Following the ‘starburst’ diagram is a summary assessment of the key observations for each Dimension and Indicator. More detail is contained in the five Dimension-specific chapters of the main report. This highlights report concludes with a section titled ‘next steps’; the starting point for a conversation about practical measures to improve Tanzania’s cyber security ecosystem.

Highlights Report

Key Observations - Dimension 1 - National Cyber Security & Capabilities

The 2015 Cybercrime Act and publication of a National ICT Policy in 2016 (and its implementation strategy) are encouraging first steps in improving Tanzania's cyber security maturity. Publication of the e-Government Security Architecture, launch of a 'CyberStars' competition and establishment of a **Cyber Security Tanzania (CyberTz)** Forum are further evidence of steps to better cyber maturity. Disappointingly, a national focal point for cyber security could not be identified. **It is hoped Tanzania can utilise output from this CMAGE assessment to help focus future activities and use the good practice guidance to provide practical support.**

There is evidence of a cybercrime department in the Tanzania Police Force, but details are lacking, so the scale of investment is unclear and its success in tackling cybercrime is not immediately obvious. In addition to the CyberStars competition, Tanzania should consider using an intervention programme to divert young people with talent away from involvement in cybercrime. Good practice from other countries will help speed the development and effectiveness of other initiatives to reduce cybercrime.

The Bank of Tanzania (BOT) appears to be actively managing risk across regulated institutions. Its website details what is expected by way of supervisory methodology and tools to actively manage risks. BOT also maintains a list of approved external auditors to carry out onsite and offsite surveillance. It does not appear to have a cyber-specific assurance scheme in place.

Dimension 1

National Cyber Security Strategy & Capabilities

Maturity Level 2

Highlights Report

Key Observations - Dimension 2 - Cyber Security Information Sharing

The Tanzania Computer Incident Response Team (TZ-CERT) is the national focal point for coordination of cyber security incident response. It is part of the Tanzania Communication Regulatory Authority (TCRA). TZ-CERT appears to be well-established, with formal regional and international links and a role in capacity building and improving general cyber security awareness. No other CERTs or formal information sharing initiatives were identified, but there is a need to establish these initiatives in critical sectors, such as financial services.

Dimension 2

Cyber Security Information Sharing

Maturity Level 3

Highlights Report

Key Observations - Dimension 3 - Cyber Security Service Provision

Three CREST International member companies offer one or more services from in-country offices.

Seven local companies also offering these services, but their quality could not be assessed.

Several CREST and non-CREST companies offer cyber security services to clients in Tanzania from regional offices in nearby countries.

Overall

There is a good mix of local, regional, and international providers of cyber security services across most of the five disciplines examined. Provision of threat intelligence and security operation centre services is relatively weaker. With some stimulus and focussed investment, Tanzania could develop stronger local capability and generate export opportunities.

Dimension 3

Cyber Security Service Provision

Maturity Level 2

Highlights Report

Key Observations - Dimension 4 - Cyber Security Professional Development

While many of Tanzania's universities and colleges offer generic computer science degrees - some with a small element of cyber security content - far fewer offer specific cyber security courses.

A first-class cyber security industry needs to be underpinned by expansion in cyber security education.

With a few notable exceptions, there is little evidence of independent academic research related to cyber security. There are opportunities for development of an academic research capability in Tanzania, increasing the country's capacity for forward thinking in this important field.

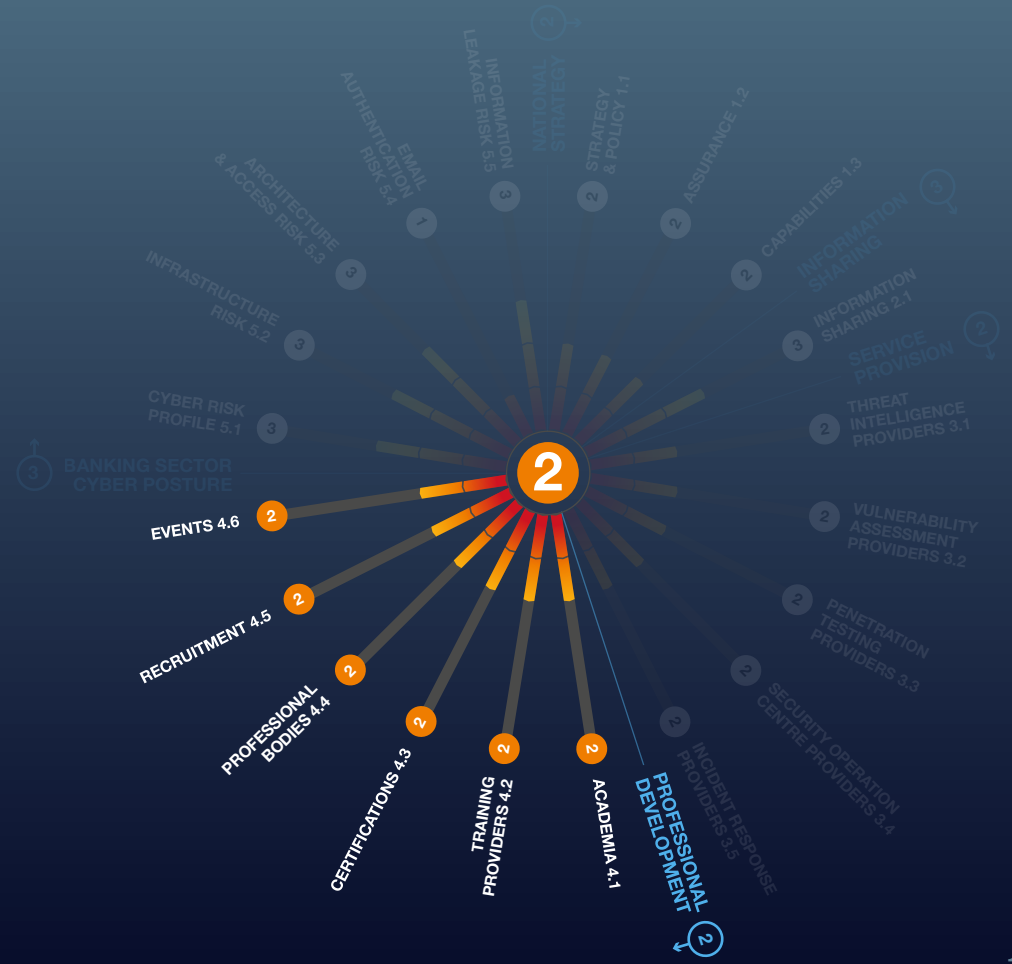
The non-traditional training offered via the previously mentioned TCRS-sponsored CyberStars Competition and the Digital Opportunities Tanzania initiative are noteworthy additions to the mix.

Continued on next page...

Dimension 4

Cyber Security Professional Development

Maturity Level 2



Highlights Report

Key Observations - Dimension 4 (continued)

A good blend of in-country and international cyber security training is available.

Improved local provision expands the opportunities for people to train at affordable cost and helps develop the professional cyber security community.

By utilising international good practice, Tanzania could build upon the existing ICT courses to support creation of more specific cyber security courses and qualifications.

Examinations for many international professional certifications are accessible in Tanzania.

CREST's research, there appears to be a lack of importance attached to using certifications to encourage and retain the most talented people into the industry.

But it is likely that the cost of some professional certificates is prohibitive to many.

There is some evidence that take-up in certifications is improving slowly. It is possible that once individuals and companies see the benefits of professional certifications, cost issues could be overcome.

As part of stage two of the project, some 'pump priming' funds may be available to start the process.

Membership of cyber security focused professional bodies helps galvanise the community and provide forums for professional development and mentoring.

While there is evidence of two international professional bodies operating in Tanzania, (although one has a wider risk management portfolio), this needs to be extended and strengthened if it is to support national aspirations to grow the number of cyber security professionals.

Highlights Report

Key Observation - Dimension 5 - Banking Sector Cyber Security Posture

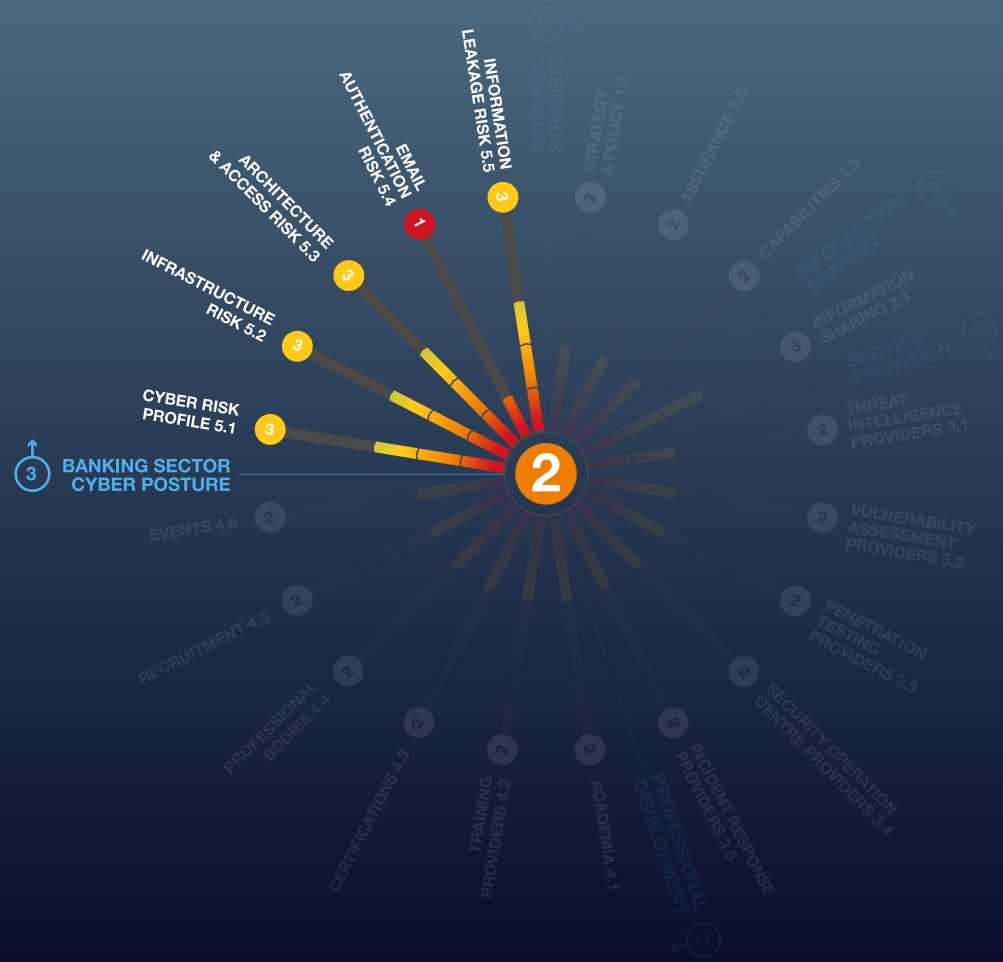
Research suggests several financial services organisations appear – at least, from an external view - to be susceptible to cyber-attacks.
Tanzania's regulators can utilise this assessment to focus attention and highlight areas for review, provide access to the supporting guidance being developed and, where appropriate, encourage take up of technical security measures to improve cyber resilience.

Continued on next page...

Dimension 5

Banking Sector Cyber Security Posture

Maturity Level 3



Highlights Report

Key Observation - Dimension 5 (continued)

For good cyber defences, organisations need to focus on several key risk areas, including:

- Security architecture
- Access control
- Configuration management
- Vulnerability patching
- Email authentication
- Staff training
- Limiting leakage of information which may be of use to an attacker

Without explicit permission, any external observations of an organisation are limited by legal and ethical constraints.

Directly assessing many key risk areas listed above is not possible. However, indirect passive (non-intrusive) assessment can be carried out on internet-connected portions of the organisation's infrastructure.

Using this approach, accessible, measurable indicators were used to gain implicit insights into many key risk areas. Passive external assessments were carried out on the public-facing IT infrastructure of a sample of 57 financial institutions. For obvious reasons, all results were anonymised.

Risk is a combination of vulnerability and threat. Vulnerability can be assessed by measurable observations. Threat is primarily a judgement based on intelligence reports.

CREST assessed the general threat to Tanzania's financial institutions is lower than for larger institutions in more advanced economies. Yet some of Tanzania's financial institutions still attract a significant threat score.

21% Overall, **21%** were awarded a risk rating of 'Very High' or 'High', indicating Maturity Level 3 for Risk Profile.

7% Just **7%** of the sample had evidence of critical vulnerabilities within their infrastructure.

24% A further **24%** appeared to be carrying non-critical vulnerabilities. This indicates Maturity Level 3 for Infrastructure Vulnerability Risk.

7% In respect of Architecture and Access Risk, **7%** of the sample appeared to have one or more remote access ports open on the public-facing infrastructure.

19% Some **19%** appeared to have one or more database ports open, leading to the award of Maturity Level 3 for this risk category.

48% Simple email authentication measures (Sender Policy Framework, (SPF)) have not been adopted by **48%** of the sample.

85% Advanced email authentication measures (Domain-based Message Authentication, Reporting and Conformance, (DMARC)) have not been adopted by **85%** of the sample. Our research indicates Maturity Level 1 for Email Authentication Risk.

33% In **33%** of sampled institutions, at least some staff data was available online because of third-party data breaches, indicating Maturity Level 1 for Information Leakage Risk.

There is significant room for improvement in the cyber security posture of many of Tanzania's banks.

Highlights Report

Next Steps

1. This maturity assessment has not been carried out **as an academic exercise**.
2. Having undertaken the research, CREST International is keen to work with governments, regulators and other stakeholder communities **to drive improvements across Tanzania's cyber security ecosystem**.
3. CREST is in the process of curating a comprehensive **library of IPR-free good practice guides and tools** to assist with ecosystem development.
4. Where there are gaps in the library, CREST will work with **renowned subject matter experts** to develop new guides and tools.
5. The library will be **available throughout 2021** and is shown on the next page.
6. Meanwhile, CREST will be working with **key stakeholders to identify pump-priming activities in Tanzania**, to help create development pathways.

Highlights Report

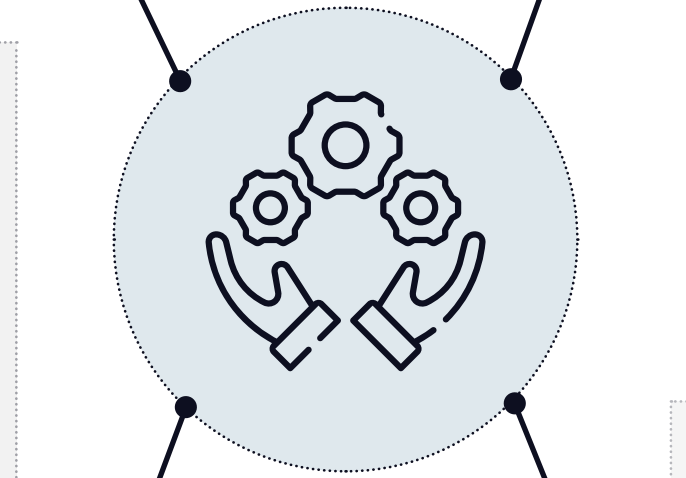
2021 Good Practices Guides and Tools

Goverment Strategy Policy

- Establishing National Cyber Security Strategies
- Introduction to Intervention / Prevention Activities
- Establishing a Cyber Crime Intervention Programme
- Establishing an Effective Cyber Crime Unit

Service Suppliers

- Introduction to Cyber Security Threat Intelligence
- Microfinance and Challenger Bank Threat Intelligence Maturity Model
- Standards of Vulnerability Assessment
- Vulnerability Analysis Maturity Model
- Procurement of Penetration Testing Services
- Penetration Testing Maturity Model for Financial Services, Challenger and Microfinance Organisations
- Critical Function of Security Operations Centres
- SOC Maturity Assessment Model
- Incident Response Maturity Model for Microfinance and Challenger Banks
- Guide Structure, Development and Deployment of Incident Reponse Teams
- Strategy Reports to Tier 3 (small organisations) Incident Response Services



Training and Academia

- Common University Degree Level Course Syllabus
- CMAGE Maturity Models for professional training providers
- Platform for Career Pathways

Security Postures

- Improving Technical Public Facing Cyber Hygiene
- Metrics for Measuring Improvement in Cyber Hygiene
- Cyber Security for Microfinance and Challenger Banks
- Generic Guide to Simulated Targeted Attack and Response
- Cyber Security Awareness Programme Community Projects

Introduction

Introduction

Background

This report seeks to provide a benchmarked assessment of the maturity of Tanzania's cyber security ecosystem.

1. The output from this maturity model can be used to help key stakeholders identify areas where emphasis should be placed to help build capacity, capability, and consistency within the ecosystem.

   The library of good practice guides and tools being developed by CREST can then be readily used to support a programme of improvements.

2. Where requested, CREST will seek to work with stakeholders to ensure improvements are delivered to the benefit of all. Periodic re-assessments can be made against this benchmarked starting point to ensure progress is being made.

3. **The Bill & Melinda Gates Foundation's Financial Services for the Poor (FSP) programme**[1] seeks to support government and private-sector partners in a shared effort to establish financial services for the world's poorest people. Financial exclusion traps millions of people globally in a cycle of poverty that is difficult to escape. The programme aims to equip people with the means to build more prosperous and secure lives for themselves, their families, and their communities.

4. Financial services must be underpinned by the best possible cyber security measures if they are to minimise the risk of the most financially vulnerable people becoming victims of cybercrime. The best possible cyber security is only delivered when a holistic approach is taken to improve the cyber security ecosystem in which the entity exists.

5. CREST International has considerable experience in taking a holistic approach to addressing the shortcomings of cyber security ecosystems. CREST also has considerable experience of working with financial regulators in Europe, Asia, and North America. It is therefore delighted to be actively supporting the Gates Foundation's FSP programme.

CREST International

6. **CREST is an international not-for-profit accreditation and certification body** that represents and supports the technical information security market[2]. It seeks to build cyber security capacity, capability and consistency by providing internationally recognised accreditation for organisations and professional certification for individuals providing cyber security services. It particularly focuses upon **Vulnerability Assessment, Penetration Testing, Cyber Incident Response, Threat Intelligence and Security Operations Centre services**.

7. **In carrying out its mission, CREST International works with a variety of stakeholders across the cyber security ecosystem, in**:

   - *Helping governments set national cyber security strategy and policy*
   - *Helping regulators establish assurance schemes that set and maintain performance standards*
   - *Helping the buying community purchase consistent quality services*
   - *Helping the supplier community deliver benchmarked cyber security services*
   - *Maintaining partnerships with academia and training providers*
   - *Maintaining dialogue with other professional bodies to ensure consistency*
   - *Supporting individuals to improve their knowledge and certify their skills.*

Introduction

Research Methodology

8. **Apart from the section of this report dealing with the banking sector cyber security posture, evidence used in preparing it has been gathered using open-source methods, including internet-based research, supplemented - where needed for clarity - by email and telephone enquiries.** The research has also been presented to audiences of local and international subject matter experts for feedback and validation.

9. For the banking sector cyber security posture, CREST worked with **Orpheus Cyber**[3], a leading cyber threat intelligence service provider, to carry out a passive (non-intrusive) external assessment of the public-facing IT infrastructure from a sample of the country's financial institutions.

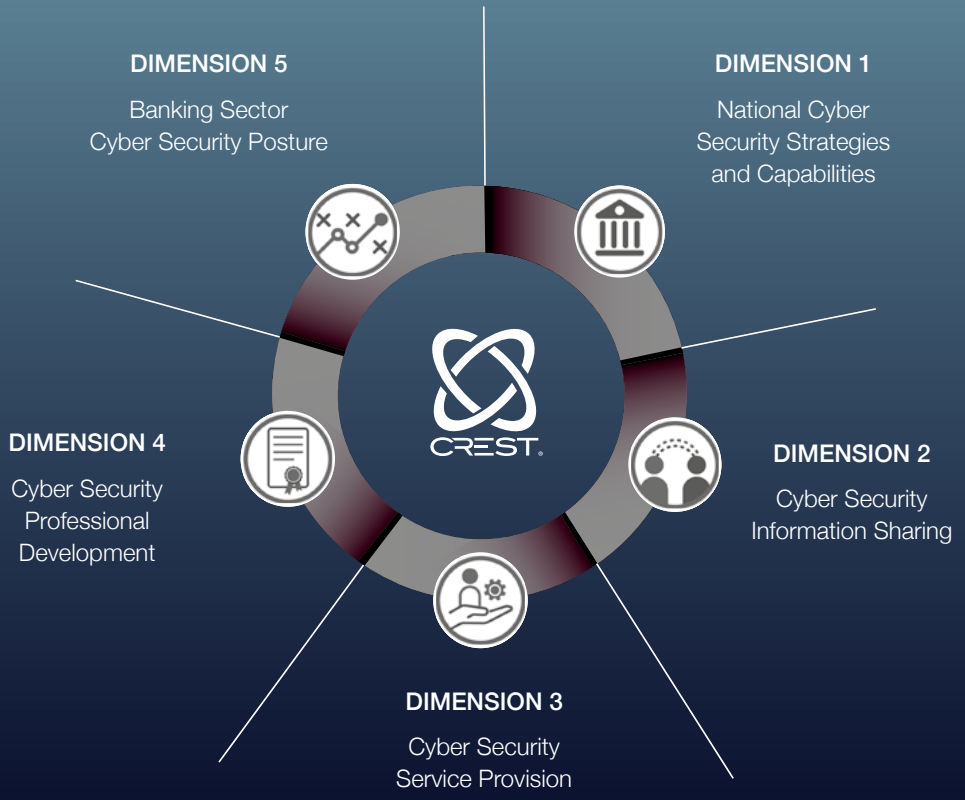
   The assessments were carried out by computer, to common standards, allowing for comparisons, benchmarking and periodic automated reassessments, if required. CREST believes this methodology is a global first - the first time that rapid, automated mass assessment has been used as part of cyber security maturity modelling.

10. **Any omissions or corrections that arose during the validation process have now been incorporated into the evidence**. This report represents the baseline upon which improvements to the country's cyber security can be subsequently measured. It is envisaged the report will be updated periodically with stakeholder support to assist in reporting progress.

CMAGE Structure

11. This Cyber security Maturity Assessment of the Global Ecosystem (CMAGE) is based on a research methodology originally developed by CREST International in 2018. The structure of the CMAGE has matured through its practical application to the conduct of ten country assessments during 2020.

The CMAGE is based on assessment of twenty separate Indicators across five Dimensions. The five Dimensions are depicted diagrammatically in the image below.



Introduction

Maturity Level Definitions

12. Each indicator has been assigned a **set of five maturity level definitions** against which evidence gathered can be consistently assessed. In **Dimensions 1-4** assessment is qualitative in nature. In **Dimension 5**, evidence is quantitatively assessed against computer-generated metrics.
13. For simplicity of notation, each dimension is also allocated its own maturity level, based upon assessments given to each of its constituent indicators using, where appropriate, qualitative judgement.
14. **In all cases, a generic label has been assigned to each of the five levels of the maturity model, as follows:**

15. The complete listing of the Dimensions and their associated Indicators is shown in the table, right. A full listing of the five maturity level definitions for each indicator can be found at **Appendix B.**

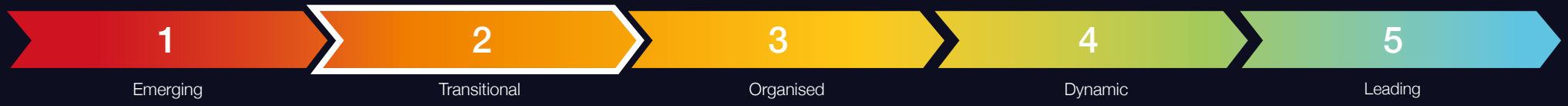
DIMENSION		INDICATOR	
QUALITATIVE ASSESSMENT			
1	**National Cyber Security Strategy & Capabilities**	1.1	Government Strategy & Policy
		1.2	Regulator/Government Operated Assurance Schemes
		1.3	Law Enforcement & Cyber Defence Capabilities
2	**Cyber Security Information Sharing**	2.1	Computer Emergency Response Teams (CERTs)
3	**Cyber Security Service Provision**	3.1	Threat Intelligence Providers
		3.2	Vulnerability Assessment Providers
		3.3	Penetration Testing Providers
		3.4	Security Operations Centre Providers
		3.5	Incident Response Providers
4	**Cyber Security Professional Development**	4.1	Academia & Higher Education
		4.2	Training Providers
		4.3	Professional Certifications
		4.4	Professional Cyber Membership Organisations
		4.5	Specialist Recruitment
		4.6	Events & Exhibitions
QUANTITATIVE ASSESSMENT			
5	**Banking Sector Cyber Security Posture**	5.1	Banking Sector Cyber Risk Profile
		5.2	Infrastructure Vulnerability Risk
		5.3	Architecture & Access Risk
		5.4	Email Authentication Risk
		5.5	Information Leakage Risk

Dimension 1

National Cyber Security Strategy & Capabilities

National Cyber Security Strategy & Capabilities

Overall Dimension Assessment: *Maturity Level 2*



National strategy is of vital importance.

16. Without a national strategy for cyber security, it would be difficult for law enforcement and the judicial system to tackle cybercrime.

    Academia and professional training providers would struggle to know what courses to provide; potential students would find it diffficult to understand career options. It would also be difficult to justify and target research. **Without a national strategy, the public and private sectors would have no guidance or framework to base their own cyber security policies on.**

    A lack of national strategy for cyber security undermines economic growth. Examining the National Cyber Security Strategy provides good insight into a nation's willingness to implement cyber security measures and to tackle cybercrime. A national strategy sets the standards for all other sectors to follow.

17. In conducting its research, CREST was looking for:

    - Government strategic guidance, policy and legislation published in relation to information/cyber security
    - When it was published
    - How thorough it was
    - Whether it empowered goverment departments and agencies to act, and if the strategy has been implemented and updated.

18. **The Tanzania Development Vision 2025 was developed in the 1990s and launched in 2000,** with the aim that Tanzania would be a middle-income country by 2025[4]. Chapter 4 covers the 'Driving Forces for Realization of the Vision', and states that Information and Communication Technologies are essential for a competitive social and economic transformation. It describes ICT as a major driving force across all sectors of the economy[5].

19. The Ministry of Finance and Planning's (MFP's) booklet, 'Tanzania Development Plan, Vision and Investment Priorities to Achieve Middle Income Status by 2025', splits the Development Vision 2025 into three five-year plans with an overarching Long Term Perspective Plan which spans all three and acts as a roadmap[6].

    a. The theme of the first Five Year Development Plan, 2011-2016 (FYDP I), was "Unleashing Tanzania's Latent Growth Potentials" and had developing ICT infrastructure as a priority[7].

    b. The theme of the second Five Year Development Plan, 2016-2021 (FYDP II), was "Nurturing an Industrial Economy". One of the nine priority interventions was to develop ICT based industry and technology adaption which included developing cyber cities and software parks[8].

    c. The theme of the third Five Year Development Plan, 2021/22-2025/26 (FYDP III), is "Realising Competitiveness-led Export Growth"[9]. Research did not find further details.

National Cyber Security Strategy & Capabilities

Overall Dimension Assessment: *Maturity Level 2* (continued)

20. **The MFP has a four-volume Implementation Strategy for the National Five-Year Development Plan 2016/17 – 2020/21,** published in April 2018[10]. Volume 1, The Action Plan[11], has cyber security objectives. This is covered in more detail in Indicator 1.2 of this section.

21. The Ministry of Works, Transport and Communications is the author of the National ICT Policy and Implementation plan. **At the time of writing this report, the Ministry's website was unavailable,** so no more information on the organisation was found.

22. **An Information Communication Technologies (ICT) Commission was established in 2015 as a recommendation of the 2003 National ICT Policy,** which outlined the need for a body holding responsibility for coordination and facilitation of relevant policy throughout the country[12]. The ICT Commission encourages registration of all ICT professionals at four levels: ICT Consultant, ICT Professional, ICT Graduate and ICT Technician[13].

    There was no evidence available on the Commission website as to how many professionals have taken up this opportunity. The National ICT Policy 2016 and corresponding Implementation Plan is publicly available on its website[14].

23. The E-Government Authority/Internet Authority[15] is a public institution created in 2019 by the eGovernment Act No 10 of 2019[16]. The Internet authority inherited the Government Agency Network formed in 2012[17]. It has responsibility to coordinate, oversee and promote government cyber efforts and encourage implementation of policies, regulations, standards, and guidelines for public institutions[18]. Its services include review and verification of ICT systems, ICT policy preparation, manufacturing ICT systems and validation of ICT projects[19].

24. **The Tanzania Industrial Research and Development Organisation's ICT Division** has a role in cyber security and forensics research and development. It also provides consultancy on the use of ICT in SME operations[20].

Overall Assessment

25. Tanzania is assessed as being at Maturity Level 2 across all three review areas. The National ICT Policy in 2016[21] and the 2016-2021 Implementation Plan[22], (both of which stem from the Tanzania Development Vision 2025[23]), combined with the MFP Implementation Strategy for the National Five-Year Development Plan 2016–2021[24] go into detail as to how this five-year plan will be implemented and who is responsible. Together, the documents show significant intent by Tanzania to make developmental progress.

26. At government level, several documents tighten up cyber security legislation and empower organisations to act towards improving cyber security in Tanzania, including:

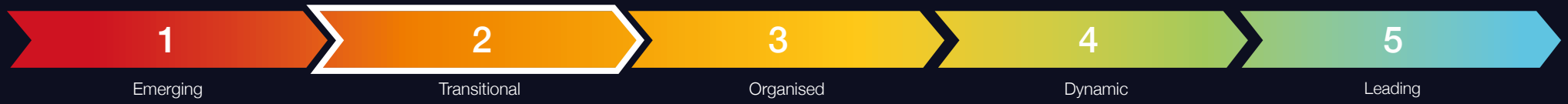
    - The Cybercrimes Act 2015[25], which empowered investigative authorities
    - The Electronic and Postal Communications, Computer Emergency Response Team Regulations 2018[26] which empowered the TCRA and the National TZ-CERT, and
    - The eGovernment Act 2019[27], which empowered the Internet Authority's influence over public institutions.

Development Approach

27. Tackling cybercrime needs to become more effective within Tanzania. Increased focus on awareness campaigns would assist in building momentum and confidence. Creating a specific financial sector cyber security policy and a financial sector CERT would strengthen national cyber security. A focus on human capacity building measures would be a complimentary approach.

National Cyber Security Strategy & Capabilities

Indicator 1.1 Government Strategy & Policy



Assessment – *Maturity Level 2*
Some evidence of up-to-date strategies and policies aimed at improving the country's cyber security posture and/or capabilities.

Government strategy must be reviewed and updated regularly to help establish priorities and focus activities.

28. CREST's research sought information on publicly available strategic level policy and legislation relating to national cyber/information security, how up to date it is, and which agencies were empowered to uphold it.

29. **The National Information and Communication Technology Policy (NICTP)** 2016 was formulated in accordance with national vision statements described in the Tanzania Development Vision 2025, which recognises that ICT is central to transforming society and the economy[28]. NICTP 2016, Chapter 3 gives an overview of the issues and 10 policy objectives[29], which are covered in more detail in the implementation strategy.

30. The National Information and Communications Technology Policy (NICTP) 2016 – Implementation Strategy 2016/17 – 2020-21[30] builds on NICTP 2003 which set out the legal framework for promoting Tanzania's ICT sector. NICTP 2016 covers legal reforms, by updating and introducing cyber and other related laws such as:
    - The Universal Communications Service Access Act no 11 of 2006
    - The Evidence Act no 15 of 2007
    - Act No. 3 of 2011 (and others)
    - The Electronic and Postal Communications Act No. 3 of 2010
    - The Cybercrime Act no 14 of 2015, and
    - The Electronic Transactions Act No 13 of 2015[31].

31. The NICTP 2016[32] covers ICT development in industry, access to ICT in Education, and ICT sector challenges, such as cybercrime. Chapter 4 is the Implementation Strategy which has numerous objectives with dated targets. Objective 8, 12 and 13 mention cyber security in one form as detailed below[33].

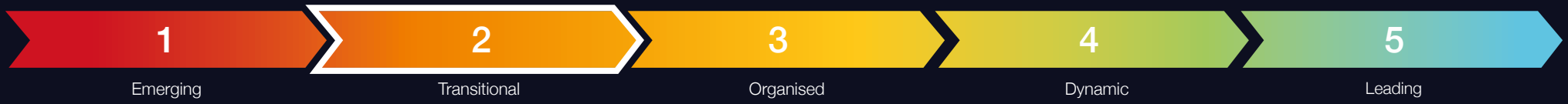
32. Objective 8 focuses on enhancing efficiency and transparency in management and utilisation of source ICT resources for a sustainable ICT industry[34]. Strategy 8.2 promotes utilisation of country codes in cyber space, to facilitate transformation towards an information society, with a target of 60% of the population sensitised on the use of these country codes by June 2021[35].

33. Objective 12 focuses on strengthening the legal and regulatory framework to facilitate acquisition, utilisation, and development of ICT. One of its KPIs is to ensure cyber offences are recognised in the respective laws[36] from 2016 onwards and by June 2021[37]. Objective 13 focuses on creating a secure environment to help build confidence and trust in the use of ICT products and services. One of its major KPIs is to have a National Cyber Security Strategy in place[38] by June 2021[39].

34. At the time of writing, no evidence of a National Cyber Security Strategy was found, but recent legislation will meet some of the objectives listed above, such as the Electronic and Postal Communications CERT Regulations 2018 and the eGovernment Act 2019 - which are covered in the next section.

National Cyber Security Strategy & Capabilities

Indicator 1.2 Regulator/Government Operated Assurance Schemes



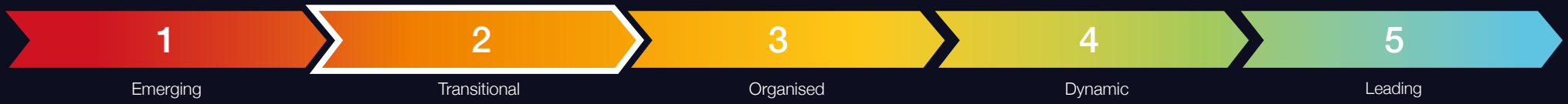
Assessment – *Maturity Level 2*
Central Bank (and/or other financial services regulators) maintain accurate records. Some evidence of good regulation of financial services sector. Little evidence of regulators operating in other sectors.

The central bank or other lead financial authority of any nation is essential in setting the ethical standards and operating frameworks for banks and financial institutions operating in-country.

35. CREST's research focused on looking for any publicly available policies and laws which support and uphold financial ethics, integrity, and cyber security.
36. Volume 1 – The Action Plan[40], of the Ministry of Finance and Planning Implementation Strategy for the National Five-Year Development Plan 2016/17 – 2020/21[41], covers cyber security as follows:
    a. Para 2.3.1.5, Industrial Research and Development Institutions, covers establishment of Advanced Cyber Security Training Services by the Tanzania Industrial Research and Development Organisation (TIRDO). It was reported as being 90% complete at the time the strategy was published[42].
    b. Para 2.3.6.1, ICT Sector, acknowledges a challenge with increased use of ICT is a corresponding rise in cybercrime. One of its objectives is to enhance Advanced Cyber Security Training Services (TIRDO)[43], to increase cyber security in all sectors by June 2021. Cyber security training is also listed, to raise awareness of issues between 2017-2021[44].
    c. Para 2.3.6.2, E-Government, aims to enhance cyber security in E-Government services to ensure information security[45]; with three outputs[46].
        i. To research activities on cyber security with other major players by June 2020, establishing a Government Cyber Security Centre between 2017-2019 and conducting Cyber Security research between 2018 to 2020
        ii. To develop a Government Information Systems Assessment Plan by June 2018, and
        iii. An ICT infrastructure to be established and operational by June 2019[47].
    d. The Annexes contain tables for each sector, with objectives, outputs, actions, time frame, the financial allocation for each objective and which organisation is responsible for implementation[48]. Such detail reveals the level of planning that went into this plan.
37. The eGovernment Authority (known as the Internet Authority[49]) was later established by the eGovernment Act No 10 of 2019[50].
38. No specific cyber or ICT security Policy from the Bank of Tanzania was found. But the Bank did request tenders in 2012-13 for consultancy services to provide vulnerability assessment and establish adequacy of ICT assets controls[51]. As a public institution, it is legally bound to comply with policies and standards directed by the Internet Authority[52] and the eGovernment Act No 10 of 2019[53].

National Cyber Security Strategy & Capabilities

Indicator 1.3 Law Enforcement & Cyber Defence Capabilities



Assessment – *Maturity Level 2*

Some reporting of cybercrime and its impact. Evidence of investment in law enforcement capabilities to tackle cybercrime. Evidence of some strategy/policy/legal support for tackling cybercrime. Some public awareness. Evidence of some government and military interest in cyber defence matters. Little evidence of specific measures within the financial services sector to tackle cybercrime.

39. **It is important to understand the level of reporting for cybercrime,** as this is evidence of it being openly recognised, discussed, and taken seriously as an issue in a public forum. CREST's research looked for what and where cybercrime was being reported, and what official action was being reported as taken to combat it.

40. **The Cyber Crime Act 2015 defines cybercrimes and their associated penalties, lays out jurisdiction of the Act, powers of police investigation and the liabilities of service providers[54].** However, the Electronic and Postal Communications Act (EPOCA) 2010[55] developed the National Tanzania Computer Emergency Response Team (TZ-CERT)[56], which sits under the Tanzania Communications Regulatory Authority (TCRA)[57].

41. The TCRA, as regulatory authority, has strategic objectives which include providing efficient, affordable, reliable, and secure ICT systems and infrastructure to the public, especially in underserved areas[58]. It offers a wide range of legislation and policy available to the public online, including the Computer Emergency Response Team Regulations 2018[59].

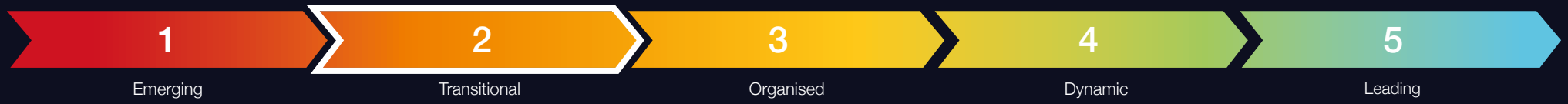
42. The Electronic and Postal Communications, Computer Emergency Response Team Regulations 2018[60] covers:

    - The TRCA's authority over the national CERT
    - The CERT's responsibilities
    - The requirements of its constituencies
    - The people and organisations the CERT serves
    - The obligations of service providers[61]

43. **The eGovernment Act No 10 of 2019[62] is thorough legislation, establishing the Internet Authority[63] and the eGovernment Authority Board, which comprises eight members from government ministries and other public institutions[64].** It holds authority to enforce compliance by public institutions to the National ICT Policy and other eGovernment related policies, laws, guidelines, and standards. It is also charged with developing mechanisms of enforcement of ICT security standards and guidelines, alongside implementation of government-wide cyber security strategies[65].

National Cyber Security Strategy & Capabilities

Indicator 1.3 Law Enforcement & Cyber Defence Capabilities (continued)



Assessment – *Maturity Level 2*

Some reporting of cybercrime and its impact. Evidence of investment in law enforcement capabilities to tackle cybercrime. Evidence of some strategy/policy/legal support for tackling cybercrime. Some public awareness. Evidence of some government and military interest in cyber defence matters. Little evidence of specific measures within the financial services sector to tackle cybercrime.

44. Part VII of the Act provides authority to establish an eGovernment Security Operations Centre, which will deliver services including vulnerability assessment and penetration testing services on networks and systems, as prescribed by the eGovernment Authority.

    Part VII stipulates all public institutions must carry out identity and access management and ICT security incident management. All acquisition, development, and maintenance of ICT systems in public institutions must meet ICT security control requirements.

    Part VIII covers Electronic Data Management; Part IX, Financial Provisions and Part X offences and penalties[66]. It is a comprehensive document for public institutions to comply with. This Act, and establishment of the authority, meets one of the objectives of the Implementation Strategy Volume 1 The Action Plan of the National Five-Year Development Plan 2016/17 – 2020/21[67].

45. **Tanzania's Police Force has cyber capability within its Criminal Investigation Division (CID).** The CID coordinates and supervises professional investigation on matters relating to fraud, offences committed through cyber space, theft, predicate offences, or embezzlement occurring within or against the National and International Financial community[68]. No further information was found on the police force website.

46. A 2020 All Africa website article quotes the Head of Cybercrime Department, Senior Superintendent of Police (SSP) Joshua Mwangaza, as saying that reporting of cybercrime incidents fell from 7000 in 2018 to 3000 in 2020, at the date of the article. The article states that the TCRA was conducting Cybercrime Act awareness training, working with the heads of religious organisations[69]. This ties in with the National ICT Policy 2016, Objective 8, to increase public awareness to the country's acts and codes[70].

47. While there are authorities and legislation in place to combat cybercrime, not a lot of evidence was found during research as to how effective these organisations or legal acts are in their implementation. It is therefore difficult to ascertain if they are having a positive effect in reducing cybercrime in Tanzania.

Dimension 2

Cyber Security Information Sharing

Cyber Security Information Sharing

Overall Dimension Assessment: *Maturity Level 3*

Information sharing is vital to achieving a collective understanding of cyber security risks and vulnerabilities, to counter threats posed by cybercriminals.

48. There is no commercial advantage to be gained by not sharing information. Open publication of academic research and sector-specific information exchanges are example mechanisms for sharing information on cyber security risks, threats, and vulnerabilities. **There is not much evidence of either of these mechanisms being currently well-established in Tanzania.**

49. Information sharing also enables the spread of best practice. Research focused on looking for expert groups such as Computer Emergency Response Teams (CERTs) - teams of information/cyber security experts responsible for protection against, and detection and response to cyber security incidents.

    They provide cyber security services, as well as running cyber security awareness campaigns or events for other organisations and the public. Some CERTS operate nationally, or within specific sectors, and may have links to other regional or international CERTs to enable greater sharing of best practice.

50. The research also looked for any evidence of other organisations working as cyber security awareness groups, in specific sectors or wider. With CERTs and various Information sharing groups, evidence was sought on how many exist and which sectors of society, business, or other stakeholders they provide services to.

Overall Assessment

51. Tanzania is currently at Maturity Level 3. TZ CERT[71] is a member of FIRST[72] and Africa CERT[73]. It is empowered by The Electronic and Postal Communications, Computer Emergency Response Team Regulations 2018[74]. Its position within the Tanzania Communications Regulatory Authority (TCRA) is likely to have assisted to reach it to ENISA Tier 2 status[75]. Its involvement in capacity building is worthy of note.

Development Approach

52. The development of finance sector-specific information sharing arrangements should be encouraged.

Cyber Security Information Sharing

Indicator 2.1 Computer Emergency Response Teams (CERTs)

Assessment – *Maturity Level 3*
Evidence that National CERT has international links (FIRST etc) and is following international standards. Meets ENISA CERT Maturity Model Tier 2 requirements.

53. **The greater the number of organisations sharing cyber security information and expertise,** the wider the spread of cyber security awareness and knowledge.

> **"Knowledge is like money: to be of value it must circulate, and in circulating it can increase in quantity and, hopefully, in value."**
> - American author Louis L'Amour (1908-1988)

54. **The Tanzania Computer Emergency Response Team (TZ-CERT)**[76] is responsible for coordinating response to cyber security incidents at national level. It cooperates with regional and international entities involved with management of cyber security incidents. **TZ-CERT was established under section 124 of the Electronic and Postal Communications Act (EPOCA) No3/2010**[77] and sits within the TCRA.

55. TZ-CERT was given further authority via The Electronic and Postal Communications, Computer Emergency Response Team Regulations 2018[78] which outlined responsibilities including:

- Maintaining a trusted national point of contact within and beyond national boundaries, that responds to cyber security standards
- Raising awareness and enhancing technical capacity of cyber security
- Coordinating with other sector-specific CERTS, including the government network CERT, and acting as a bridge between them and international CERTS
- Developing a national roadmap for improving cyber security awareness.

Cyber Security Information Sharing

Indicator 2.1 Computer Emergency Response Teams (CERTs) (continued)

Assessment – *Maturity Level 3*

Evidence that National CERT has international links (FIRST etc) and is following international standards. Meets ENISA CERT Maturity Model Tier 2 requirements.

56. The regulations also list the duties of constituents it serves, in terms of actions to take towards cyber security. Some of these duties include:
    - Maintaining and securing the environment for their organisation's internet connectivity and internet networks
    - Complying with security standards, guidelines and minimum-security specifications and requirements as recommended by the CERT or their service providers.

57. Service provider obligations are given in detail and include, as examples:
    - To provide a secure environment for the connectivity of their subscriber base
    - To notify the National CERT of any significant security breaches
    - To abide by CERT guidelines and directives as prescribed by the authority (TCRA).

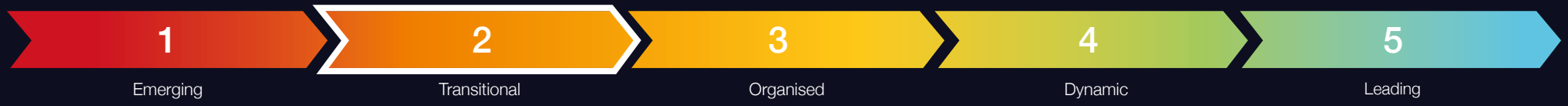
58. TZ-CERT is a member of Africa CERT[79] and the Forum of Incidence Response Security Teams (FIRST)[80] which provides it with good regional and international links and means it meets the requirements for ENISA Tier 2 status[81].

Dimension 3

Cyber Security Service Provision

Cyber Security Service Provision

Overall Dimension Assessment: *Maturity Level 2*



Professional cyber security service provision is essential to protect individual organisations and by default, the national economy. Service providers form part of the front line in the fight against cybercrime.

59. Research into how cyber security services are currently provided in Tanzania involved:
    - Identifying cyber security service providers
    - Examining what services they were offering
    - Identifying what accreditations they held, and
    - Identifying whose accredited services and certifications they provided.
60. The location of company offices and customer reach were also recorded. Were they were local companies, so registered and only based in Tanzania? CREST examined if they were regional companies, registered in another African country, but with offices and the ability to reach customers in other countries in the region. Or were they a large international organisation, with multiple global office locations which may be located in-country? If not, can they provide services into Tanzania without having a permanent physical presence in-country, or anywhere in the African region? When examined together, these factors combined give an idea of the maturity of the cyber security industry.
61. Several companies identified provided more than one cyber security service, such as security services, training and events for example, so they appear in more than one indicator. Where possible, ICT companies providing solutions via the purchase of other technology products, such as software, were excluded from the research.

Overall Assessment

62. Tanzania is currently assessed as being at Maturity Level 2 across all five service provision disciplines. Some progress is being made towards Level 3 goals in some disciplines. There are no local CREST member companies, but three CREST member companies have local offices. There are a small number of local service providers across all disciplines.

Development Approach

63. Demand-led growth in the number of service providers should encourage investment. Encouragement from the government and regulators should lead to the adoption of benchmarked standards. Greater clarity on open security within the National ICT policy would assist.

Cyber Security Service Provision

Indicator 3.1 Threat Intelligence Providers

1 Emerging | 2 Transitional | 3 Organised | 4 Dynamic | 5 Leading

Assessment – *Maturity Level 2*

Some local/regional providers and a few CREST International members with local offices. Some competition but with no measure of quality of service for local providers.

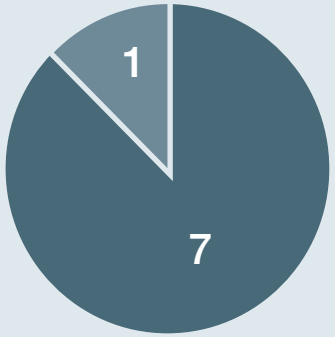
Cyber Threat Intelligence

64. Cyber Threat Intelligence (CTI) is information about current and future cyber threats and actors that adversly affect a nation's or organisation's cyberspace. Cyberspace can be defined as an interactive domain made up of digital networks[82]. Threat Intelligence includes open source information, and intelligence from technical, human, social media and dark web sources.

65. The research looked for companies that provided cyber threat intelligence services to organisations in Tanzania, and where these services were being delivered from. For the purposes of a robust cyber security environment, the ideal scenario is a host of Threat Intelligence service providers based in Tanzania. Evidence of quality, though any accreditions or partnerships these companies may have, was also sought.

Office Location	Non-CREST Accredited	CREST Accredited	Total
In-country	4	2	6
Regional	0	0	0
International	1	7	8
Total	5	9	14

66. Some **14 companies were found during research providing Threat Intelligence Services into Tanzania.** It was good to find some locally based companies, which **included two CREST accredited international organisations.** But most companies discovered were CREST accredited internationally based organisations, offering services to Tanzanian clients upon request.



Of the **eight international organisations** that provide services into Tanzania, **seven are CREST-accredited**.

It is not confirmed how frequently the threat intelligence services of these international organisations are being used.

Cyber Security Service Provision

Indicator 3.2 Vulnerability Assessment Providers

1 Emerging | 2 Transitional | 3 Organised | 4 Dynamic | 5 Leading

Assessment – *Maturity Level 2*

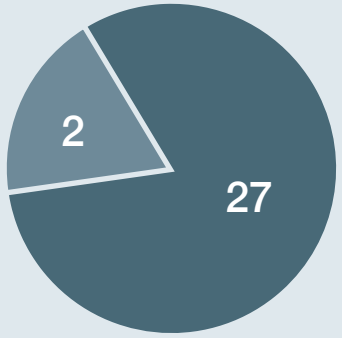
Some local providers and a few CREST International members with local offices. Some competition but with no measure of quality of service for local providers.

Vulnerability Assessment (VA)

67. Vulnerability Assessment (VA) is defined by CREST as: "*The examination of an information system or product to determine the adequacy of security measures; the identification of security deficiencies; to predict the effectiveness of the proposed security measures; and to confirm the adequacy of such measures after implementation*[83]." As with Threat Intelligence, research focused on looking for companies which provide VA services in Tanzania, ideally based in Tanzania.

Office Location	Non-CREST Accredited	CREST Accredited	Total
In-country	8	3	11
Regional	0	0	0
International	2	27	29
Total	10	30	40

68. **CREST's research found 40 companies offering Vulnerability Assessment Services into Tanzania.** The vast majority were CREST accredited international organisations, **three of which had offices in country,** while the rest were internationally based. In total, **there are eleven companies operating in Tanzania, eight of which are in-country companies**. It is worth noting that TZ-CERT provides this service to its clients.



There are **29 international companies offering VA services** into Tanzania from international offices elsewhere, **27 of which are CREST accredited members**.

Cyber Security Service Provision

Indicator 3.3 Penetration Testing Providers

1 Emerging | 2 Transitional | 3 Organised | 4 Dynamic | 5 Leading

Assessment – *Maturity Level 2*

Some local providers and a few CREST International members with local offices. Some competition but with no measure of quality of service for local providers.

Penetration Testing

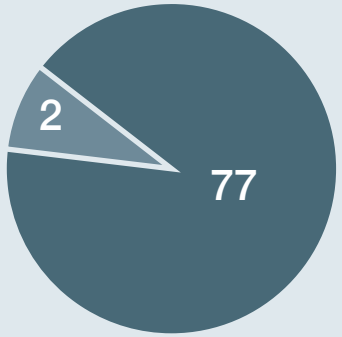
69. The UK's National Cyber Security Centre (NCSC) define penetration testing as: *"A method for gaining assurance in the security of an IT system by attempting to breach some or all of that system's security, using the same tools and techniques as an adversary might. Penetration testing should be viewed as a method for gaining assurance in your organisation's vulnerability assessment and management processes, not as a primary method for identifying vulnerabilities*[84]*."*

70. CREST's research found significantly more companies providing penetration testing than any other cyber security service. Many service providers, however, provide more than one cyber security service. In assessing the maturity of the cyber industry, efforts focused on looking for as many service providers based in Tanzania as could be identified.

Office Location	Non-CREST Accredited	CREST Accredited	Total
In-country	8	3	11
Regional	0	2	2
International	2	77	79
Total	10	82	92

71. In total, **91 companies were found providing Penetration Testing services into Tanzania.** Unsurprisingly, the majority were CREST accredited, internationally based organisations that provide their services into Tanzania as requested.

72. A total of **eleven in-country companies were found**, of note was TZ-CERT. **Three of the in-country based companies were CREST accredited international members.** A further **two companies provided Penetration Testing services** from elsewhere in the region.



There are **79 international organisations providing penetration services into Tanzania** from international offices, **77 of which are CREST-accredited**.

Cyber Security Service Provision

Indicator 3.4 Security Operation Centre Providers

1 Emerging | 2 Transitional | 3 Organised | 4 Dynamic | 5 Leading

Assessment – *Maturity Level 2*

Some local/regional providers and a few CREST International members with local offices. Some competition but with no measure of quality of service for local providers.

Security Operations Centres

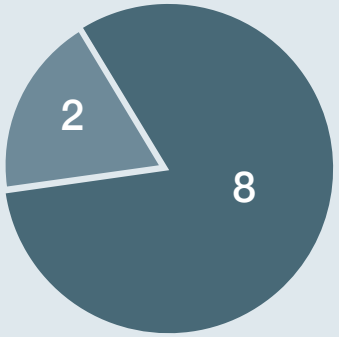
73. CREST provides a detailed definition of what Security Operations Centres are: *"An Information Security Operations Centre (SOC) is a facility where enterprise information systems (web sites, applications, databases, data centres and servers, networks, desktops and other endpoints) are monitored, assessed, and defended. Depending on the nature of the SOC, organisations may offer a variety of services including monitoring, detection, threat hunting, log analysis, incident management, forensic imaging, malware analysis, reverse engineering, mitigation advice and general good practice guidance. A range of response options may be available, from telephone or email triage through to onsite assistance as required. Where such services are not available within the organisation, the SOC will know where and how to procure appropriate services from third parties[85]."*

74. Security Operations Centres are specialised, so provision is only likely to come from well-established companies, operating in an active cyber security industry market.

Office Location	Non-CREST Accredited	CREST Accredited	Total
In-country	0	1	1
Regional	1	1	2
International	2	8	10
Total	**3**	**10**	**13**

75. Security Operations Centres are specialised, so provision of this service is only likely to come from well-established companies, operating in an active cyber security industry market.

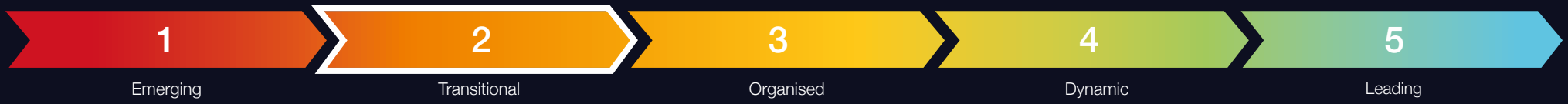
76. There are **13 companies that can provide Security Operations services into Tanzania.** Just **one is based in-country,** and it is a CREST-accredited international organisation. The remainder were internationally based organisations, a majority of which were CREST accredited.



Of **10 international companies**, **8 are CREST-accredited companies** which offer their services into Tanzania at clients' request.

Cyber Security Service Provision

Indicator 3.5 Incident Response Providers



Assessment – *Maturity Level 2*

No locally-registered CREST member companies but a strong presence from international CREST members with local offices. There are some locally registered providers, but these are not benchmarked against international standards. There is competition, and international providers view the market as being mature enough for investment.

Incident Response Providers

76. Incident response to a cyber security incident is defined by CREST as: "*An information (or IT) security incident that could be classified as a cyber security incident ranges from serious cyber security attacks on critical national infrastructure and major organised cybercrime, through hacktivism and basic malware attacks, to internal misuse of systems and software malfunction*[86]."

77. Responding to a cyber incident is challenging, as many organisations will not have effective cyber security controls in place. **Depending on size, not all organisations will have a dedicated IT team with cyber security professionals employed in house.** Companies providing incident response services to clients are a vital component of the cyber industry and the fight against cybercrime. **The number of Incident Response service providers based in-country is critical to the overall cyber maturity of the cyber industry in Tanzania.**

Office Location	Non-CREST Accredited	CREST Accredited	Total
In-country	4	3	7
Regional	0	1	1
International	3	28	31
Total	**7**	**32**	**39**

78. In total, there are **39 companies offering Incident Response services into Tanzania.** Of the **seven companies based in-country, one is TZ-CERT and three are CREST accredited international organisations.** There is **only one regionally based company.** The remainder are internationally based, and a majority are CREST accredited. It is not known how often the services of these regionally or internationally based companies are called upon from Tanzania.

Dimension 4

Cyber Security Professional Development

Cyber Security Professional Development

Overall Dimension Assessment: *Maturity Level 2*

79. Education and professional development are critical in providing students with the skills and knowledge to thrive in the modern workplace. Without ICT and cyber security being taught in the national education system, academia, and then available as professional development, it is difficult to attract young people into the cyber security industry and to train as professionals.

    The continued pace of technological advancement and increased use of the internet generates an increase in threat from cybercriminals. Unprotected digital money is an easy target for them, and unprotected data is equally valuable. To combat the threat, a country needs a vibrant cyber security industry with well-trained professionals.

80. To determine the health of cyber security professional development, there is a need to identify which higher education establishments and professional training providers offer cyber security qualifications and certifications - and what qualifications and certifications are available. CREST examined what professional membership organisations were undertaking to improve the cyber profession. Researchers studied recruitment channels to identify advertised cyber security roles and cyber security freelancers promoting themselves, to ascertain the vibrancy of the cyber security job market.

81. As a result of the National ICT Policy, the ICT Commission encourages registration of all ICT professionals at four levels: ICT Consultant, ICT Professional, ICT Graduate and ICT Technician, with the aim of improving professional standards - and giving market reassurance that their ICT professionals are of the highest standards[87].

82. In 2016, the TCRA offered ICT Scholarships for Tanzanian students studying ICT courses[88]. The Ministry of Education, Science and Technology has an ICT training programme for secondary school teachers, implemented in 2010[89]. It was initially developed as a response to the National ICT Policy 2003 but has been modified since publication of the 2016 National ICT Policy. There is a manual to this programme (not found during research), which aims to address the following gaps[90]:

    - Lack of awareness on the importance of ICT use in teaching and learning
    - Lack of basic skills in using ICT facilities
    - Lack of basic technical skills in ICT equipment maintenance
    - Lack of basic technical skills in management of hardware and software
    - Lack of skills of integrating ICT in teaching and learning.[91]

83. These initiatives, if successfully implemented, will have a positive effect on ICT professional development.

Overall Assessment

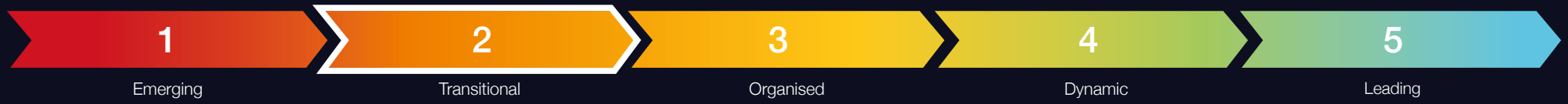
84. All six review areas within professional development are assessed as being at Maturity Level 2. The implementation plan of the 2016 National ICT Policy[92] recognised the need to focus on certification - and establishing professional bodies - which may have been met by the ICT Commission's ICT Professional registration scheme.

Development Approach

85. Investment in certifications and local chapters of professional bodies should be considered a priority. Partnering between local and international universities could improve cyber security education opportunities.

Cyber Security Professional Development

Indicator 4.1 Academia & Higher Education



Assessment – *Maturity Level 2*
In addition to computer science degrees, evidence of some cyber security degrees (BSc, MSc, and PhD) and some research.

Academia and Higher Education

86. Higher education takes place after secondary schools usually in further education colleges or universities. It aims to equip people with the skills and qualifications needed in their future workplace or careers. Academia is the pursuit of research, higher level education and scholarship.

87. CREST's research sought to identify universities and colleges offering ICT or cyber courses and modules to their students, and at what level – diploma, degree, or Master's, for example. The more students graduating with ICT- or cyber-related degrees, the more people may potentially follow an ICT related career.

	Cert	Diploma	BA/BSc	MSc	PhD	Total
ICT Courses	23	12	7	2	0	44
Cyber Cources	1	0	1	2	0	4
Total	**24**	**12**	**8**	**4**	**0**	**48**

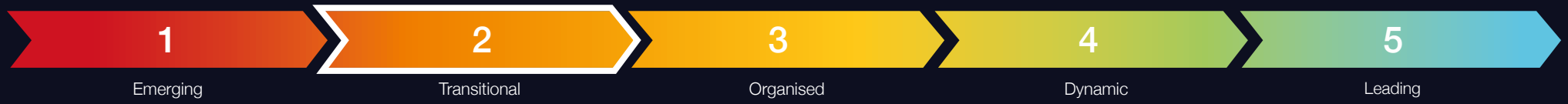
88. The table to the left shows approximate numbers of courses offered from the 20 higher education institutions, universities and colleges researched. Information on courses provided was taken from the institutions' websites. Where information was offered, it was not all shown in the same level of detail, hence numbers are approximate.

89. 48

Of the **20 institutions researched, there were a total of 48 ICT courses offered, some with cyber content and a few specific cyber courses.** Most courses are certification/diploma level and the number with cyber content is low. There is plenty of scope for increasing the number of cyber courses available to students as demand requires.

Cyber Security Professional Development

Indicator 4.2 Training Providers



Assessment – *Maturity Level 2*
Remote (online) delivery of training is supplemented with some regional instructor-led provision and a few local providers. No CREST International training provider members with local offices. Some competition but with no measure of quality of service.

Training Providers

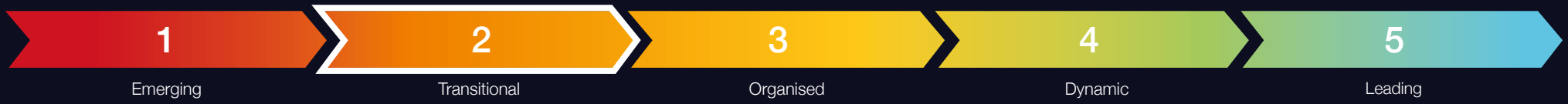
90. Training providers are qualified to deliver training via established courses to clients in a particular subject. CREST's research sought to identify the number of training providers, where they were located and what cyber courses they were providing.

91. 16

Some **16 training providers were found during research.** A small number of local providers offer some cyber security related training alongside a wider portfolio of ICT training. **These local offerings are supplemented by a few regional providers.** The non-traditional training offered via the CyberStars Competition and through the Digital Opportunities Tanzania initiative are a useful addition to the mix.

Cyber Security Professional Development

Indicator 4.3 Professional Certifications



Assessment – *Maturity Level 2*

Some International Certification Bodies operate in country but take up is low. Some local institutions and professional associations in operation.

Professional Certifications

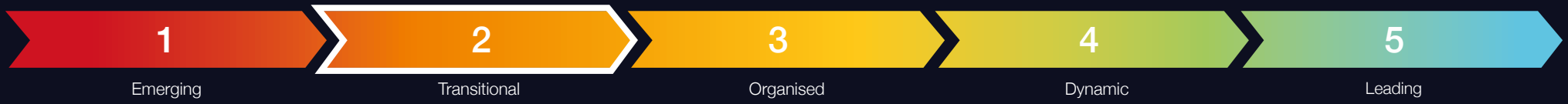
92. Professional certifications provide evidence of the holder's skills in that subject area at the time of certification. In the cyber security industry, a multitude of different cyber certifications can be attained, provided by a growing number of professional training providers. More detail of these training providers and the certifications that they provide can be found in **Appendix C.**

93. During CREST's research, **15 professional certification bodies were found. Most offer certifications with online exams or in-person in Tanzania through Pearson Vue or PSI test centres.** Some certifications requiring practical exams offer this element online or through connection to a remote network. Some bodies require attendance at a physical testing site, which have limited availability in Africa.

Take up of certifications is low, even with the ICT Commission encouraging professional registration. There was one body with an active chapter in Tanzania. It runs events such as webinars, training sessions and an outreach programme at Mzumbe University. A few other certification bodies organise training in Tanzania, either themselves or with accredited training partners. **There was low recruitment activity by the certification bodies.** Only a handful of information security jobs were available in online searches, featuring a small number of certifications.

Cyber Security Professional Development

Indicator 4.4 Professional Cyber Membership Organisations



Assessment – *Maturity Level 2*

Some evidence of international cyber security membership bodies representing individuals and/or companies having local chapters/branches.

Professional Cyber Membership Organisations or Associations

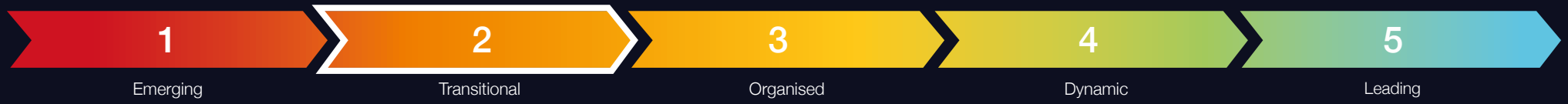
94. **Professional membership organisations or associations usually focus on furthering the profession they represent.** They provide membership by subscription. Membership benefits range from gaining access to further professional development and training, access to discounted products and events, networking, and collaboration with like-minded people, and increasing professional credibility because of membership. **These organisations are frequently not-for-profit.**

95. Several international professional membership organisations operate in the cyber security industry, some with chapters based in individual countries and regions. The existence of chapters in a country/region is direct evidence of an appetite for membership of that organisation, and indirect evidence of a more general appetite for community and professional ethos.

96. One of the strands of the government's 2016 ICT Policy was development of professional bodies, due to be delivered in 2018. - There is no clear evidence that it has yet delivered. **Only two professional membership organisations were found operating in Tanzania at the time of research. There is significant scope for improvement.**

Cyber Security Professional Development

Indicator 4.5 Specialist Recruitment



Assessment – *Maturity Level 2*
Some evidence of in-country cyber security recruitment.

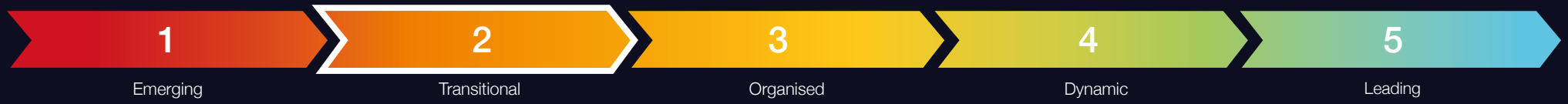
Specialist Cyber Recruitment

97. The presence and activity levels of recruitment companies and platforms provides evidence of how vibrant the job market is in a particular geographical area and/or industry sector. CREST's research looked for companies, online or with a physical in-country presence, that were either recruiting specifically for cyber security roles in Tanzania, or marketed cyber qualified freelance professionals registered with them.

98. 5 **Five recruiting organisations were identified in Tanzania.** While none were specific to the cyber-security profession, some had cyber security- or ICT-related posts available.

Cyber Security Professional Development

Indicator 4.6 Events & Exhibitions



Assessment – *Maturity Level 2*
Occasional cyber security events/exhibitions being run in-country, usually organised by an external entity.

Events and exhibitions

99. **Events and exhibitions take a great deal of commitment, finances, advanced planning, and organisation to bring to life.** There needs to be an appetite from the target audience to pay the ticket price and attend. CREST's research looked for cyber or information security events recently held in Tanzania, what level the events were, and how frequently they were held. This provides evidence for the appetite for both cyber security knowledge and services in country. The impact of these events can be far reaching, as they are effective hubs for networking, collaboration, and information sharing, which helps sow seeds of cyber security inspiration in their audience.

100. 5

Seven different annual or ad-hoc cyber security events were identified during research. The last year has seen a welcome growth in planned cyber security events in Tanzania, but sadly COVID-19 curtailed some of the plans. The involvement of the Bank of Tanzania in the TZ-CERT Capacity Building event at the start of 2020 is a good omen. The Tanzania Youth Digital Summit 2020 and CyberStars competition in December 2019 were both a further step in the right direction. With targeted support and encouragement, Tanzania could rapidly reach Maturity Level 3.

Dimension 5

Banking Sector Cyber Security Posture

Banking Sector Cyber Security Posture

Overall Dimension Assessment: *Maturity Level 3*

1	2	3	4	5
Emerging	Transitional	Organised	Dynamic	Leading

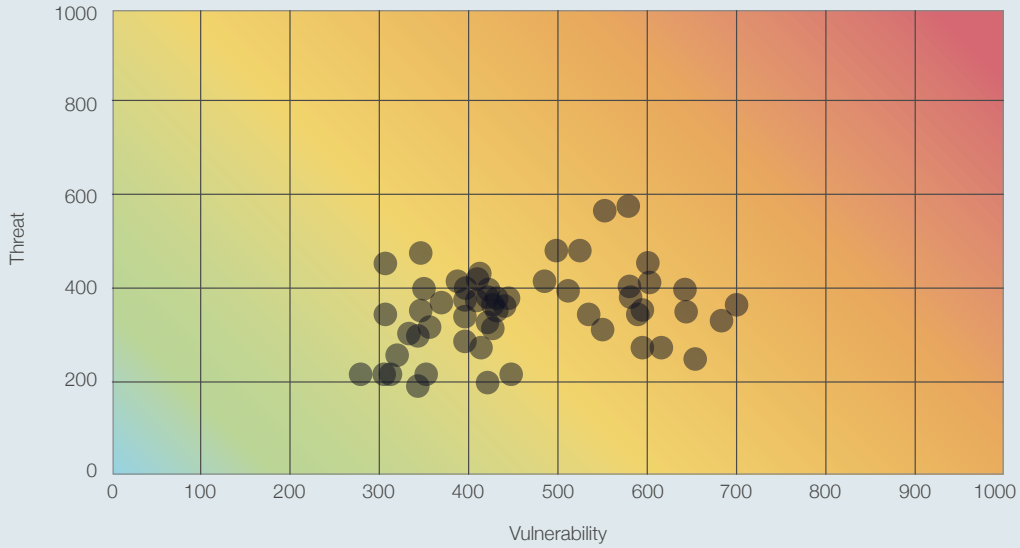
101. To assess the current cyber security posture of the Ugandan banking sector, CREST commissioned a leading cyber threat intelligence service provider, Orpheus Cyber, to undertake passive (non-intrusive) external assessments of the public-facing IT infrastructure from a sample of financial institutions. Its brief was to examine the cyber security risk rating of each financial institution against a series of non-intrusive metrics, including:

- The presence of vulnerabilities on public-facing IT infrastructure
- The presence of open ports on internet-facing servers
- The adoption of anti-phishing mechanisms
- Availability of breached employee credentials on online forums and marketplaces frequented by cybercriminals.

102. The results of research into these four metrics are explained in more detail in **Indicators 5.2 to 5.5**. For each institution, the results were fed into an Orpheus cyber proprietary assessment tool to measure vulnerability against threat and determine comparative risk ratings. The anonymised results of the assessments have been plotted on a scatter diagram, right, where very low risk is bottom left and very high risk is top right. These results are covered in more detail in **Indicator 5.1.**

Comparative Risk Rating

Figures represent CREST's cyber risk rating of each financial institution against a series of non-intrusive metrics



103. In determining the financial institutions to be assessed, the first source was the list of supervised institutions maintained by the Bank of Tanzania[93]. This information was cross-checked against the membership list of Tanzania Bankers Association[94], Wikipedia[95] and the websites of the financial institutions themselves, to generate a representative sample of national and international banks and microfinance institutions operating in Tanzania. The website addresses and email domains of 57 financial institutions were passed on to Orpheus Cyber for initial assessment. The results contained in this report relate to assessments undertaken on these institutions in October 2020. For ethical reasons, all results have been anonymised throughout.

Banking Sector Cyber Security Posture

Indicator 5.1 Banking Sector Cyber Risk Profile

Assessment – *Maturity Level 3*
Banking sector cyber risk profile is assessed as average; 10% or fewer of the surveyed financial institutions received a cyber risk rating of Very High and 40% or fewer received a rating of High or Very High.

Banking Sector Cyber Risk Profile

104. The totality of cyber risk faced by individual financial institutions is formed by a complex array of threats and vulnerabilities. No modern-day organisation can be completely immune to cyber risk. The trick is to systematically address risks in terms of severity and impact – starting with highest risks. The same approach applies when taking a sectoral approach.

105. The scale that CREST uses for rating cyber risk ranges **between 0 (very lowest risk)** and **1000 (very highest risk)** and falls into **five different rating bands**:

Very Low	Low	Medium	High	Very High
(0 – 354)	(355 – 408)	(409 – 467)	(468 – 522)	(523 – 1000)

106. As visible in the scatter diagram on the previous page, assessed financial institutions have been found to have **individual vulnerability scores (X-axis) ranging between 281 and 697**. The **average cyber risk score** for the sample is **400**, which corresponds to a national average risk rating of '**Low**'.

107. Note that no active (intrusive) assessment was undertaken, nor assessment made of those elements of the IT infrastructure that are not internet-facing. If a comprehensive assessment were made of entire IT infrastructures, internet-facing and otherwise, results may have differed. However, the levels of access that would have been required for such an undertaking are far beyond the scope of this report. For research purposes, the cyber risk rating of the public-facing infrastructure is considered sufficient to indicate the general security posture of the whole financial services sector.

There appears to be significant room for improvement in cyber security posture of some of the individual financial institutions, particularly in those with a 'High' or 'Very High' risk rating.

Banking Sector Cyber Security Posture

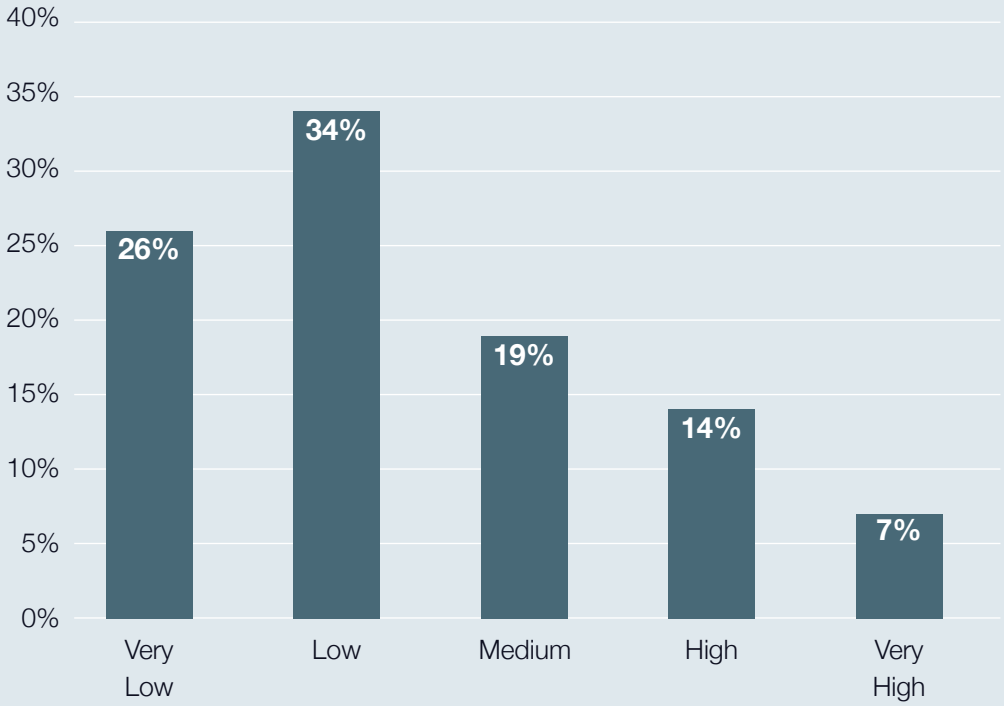
Indicator 5.1 Banking Sector Cyber Risk Profile (continued)

1 Emerging | 2 Transitional | 3 Organised | 4 Dynamic | 5 Leading

Assessment – *Maturity Level 2*

Banking sector cyber risk profile is assessed as poor; 30% or fewer of the surveyed financial institutions received a cyber risk rating of Very High and 55% or fewer received a rating of High or Very High.

Breakdown of Uganda's Financial Institutions by Category of Risk Rating



122. A breakdown by category of risk rating of the assessed sample of financial institutions is shown here, and the results anonymised. **Encouragingly, 60% of the financial institutions have an overall cyber risk rating of 'Very Low' or 'Low'.** On the other hand, **21% have an overall cyber risk rating of 'Very High' or 'High'.**

Institutions in these latter two categories are not implementing good cyber hygiene practices and/or operating vulnerable infrastructures. Consequently, they face higher levels of cyber risk.

Banking Sector Cyber Security Posture

Indicator 5.2 Infrastructure Vulnerability Risk

Assessment – *Maturity Level 3*
Infrastructure vulnerability risk is assessed as average; 10% or fewer of the surveyed financial institutions had critical known vulnerabilities on their IT infrastructure and 40% or fewer had any known vulnerabilities.

Infrastructure Vulnerability Risk

109. Software patching and other routine housekeeping activities are essential tasks which need to be carried out frequently and methodically to reduce the opportunities for attackers. **They are a good indicator of an organisation's enduring commitment to security.** Ethically, research was limited to carrying out non-intrusive examinations of those infrastructure elements directly connected to the internet. Formally, the results are similarly constrained. But it is reasonable to assume the results are typical of the state of patching across each financial institution's complete IT infrastructure.

110. Vulnerabilities, often referred to as CVEs[96], (Common Vulnerabilities and Exposures) are flaws in software and hardware that cybercriminals seek to exploit when attempting to gain access to the IT infrastructure of a chosen victim. To look for CVEs, they routinely scan portions of the internet. **CREST's researchers followed a similar approach, scanning the public-facing IT infrastructure of the 57 Tanzanian financial institutions being assessed.**

    By restricting themselves to passive reconnaissance only, researchers were unable to confirm if the vulnerabilities they detected actually existed. There is a possibility that in some cases they were false positives.

111. 31%

    The investigation revealed that 31% of Tanzania's financial institutions operate unsecure internet-facing infrastructure featuring at least one known vulnerability. The vulnerabilities detected mostly have patches available. Their presence on an internet-facing infrastructure suggests lax patching practices.

112. Each CVE is analysed and assigned a severity score ranging from 0 to 10, with 10 being the most severe. This score is known by the acronym CVSS[97] (Common Vulnerability Scoring System). Vulnerabilities with a score of 9 or more are classed as critical. Critical vulnerabilities are often prioritised by those with malicious intent, because of the ease with which they can be exploited, or the access they provide when successfully exploited.

7%

CREST's research identified only 7% of Tanzania's assessed financial institutions are operating internet-facing IT infrastructure with at least one critical vulnerability. In those financial institutions with critical vulnerabilities, these results are indicative of a failure to adopt an 'attacker's eye perspective' and prioritise critical CVEs for remediation.

Banking Sector Cyber Security Posture

Indicator 5.3 Architecture & Access Risk

Assessment – *Maturity Level 3*
Architecture & Access risk is assessed as average; 25% or fewer of the financial institutions were identified as having potential remote access vulnerabilities and 25% or fewer were identified as having potential database vulnerabilities.

Architecture & Access Risk

113. Security architecture and access management are the most common means of securing networks and information. "Security by design" is the essential foundation upon which all other cyber defences are built. Insufficient segregation between key assets, and unguarded routes to gain unauthorised access are examples of gaps that can be exploited by attackers. Ethically, researchers were limited to examine only those assets directly connected to the internet. They focused on the remote access and database ports of internet-facing servers as a simple indicator of the configuration management underpinning the network and, by inference, the likely approach taken to security by design.

114. In the context of computer infrastructure, ports are the gateways through which computers communicate with each other. By design, computer servers have multiple logical communication pathways, tailored to facilitate communications relating to a particular service. When a port is 'open,' the server can receive packets of data related to a particular service, when it is closed, it cannot. Certain ports need to be configured as 'open' to allow the server to perform. Traffic [data] going in and out of these ports can be guarded by mechanisms such as firewalls.

115. If a server is misconfigured and one or more ports are unintentionally left open (and unguarded), then cybercriminals can potentially gain access and compromise the computer network. In the same way cybercriminals scan for CVEs (see **Indicator 5.2**), they routinely scan the internet to identify open ports which they can target to gain a foothold into corporate networks.

116.

Cybercriminals frequently look to **scan ports associated with remote access services** – hardware and software that allow authorised users to remotely access a computer or a network from a distinct network connection.

Cybercriminals favour **targeting remote access services** because, once compromised, they can easily move within a network and gain access to systems containing valuable information they can steal and/or encrypt.

Certain specialised cybercriminals also look to target remote access services and **gain access to bank networks**, with a view to **selling-on this access in online criminal forums and marketplaces**.

Banking Sector Cyber Security Posture

Indicator 5.3 Architecture & Access Risk (continued)

CREST's research showed that 7% of the assessed financial institutions maintain at least one port associated with remote access services open to the internet.

117. In most cases, these ports will have been configured to accept incoming data packets from the internet for a valid business requirement, with adequate security measures in place. Although banks with open remote access ports on their IT infrastructure remain susceptible to a potential compromise, they are a small subset. Evidence suggests Tanzania's financial services sector is not highly vulnerable to the threat emanating from ports associated with remote access services.

118. Another set of ports on computer servers that cybercriminals often deliberately target are those used by database services.

19%

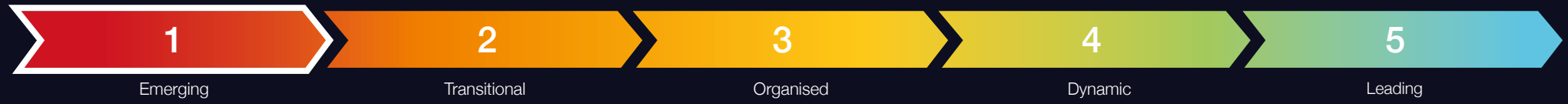
CREST's research showed 19% of the assessed financial institutions have at least one database-related port open on their public-facing infrastructure. Although some of these internet-accessible database services are in place to meet valid business requirements and configured with adequate security controls, others could be incorrectly configured and susceptible to targeting by cybercriminals.

119. While remote access ports left open to the internet can allow cybercriminals to reach a bank's internal network and steal valuable information, exposed databases place customer data and other sensitive information at even more direct and imminent risk. This is mainly because the database services associated with the ports often lack authentication protocols by default, allowing unauthorised third parties to easily access and retrieve their content.

120. Understanding the threat associated with exposed database instances - reducing the possibility of suffering a data leak - also reduces the risk of contravening Tanzania's embryonic data protection regulations.

Banking Sector Cyber Security Posture

Indicator 5.4 Email Authentication Risk



Assessment – *Maturity Level 1*
Email authentication risk is assessed as very poor; more than 15% of the surveyed financial institutions had not correctly enabled basic email authentication measures (SPF) and/or more than 70% had not correctly enabled advanced email authentication measures (DMARC).

Email Authentication Risk

121. **Having an inherent susceptibility to social engineering and phishing campaigns is human nature.** While training and education can help prevent successful attacks, using email authentication mechanisms can further reduce the threat. As an outside observer, it has not been possible to comment directly on staff training. But by passively detecting if email authentication mechanisms are in place, an indication of an organisation's commitment to reducing the effectiveness of phishing attacks and similar hazards can be gained.

122. **Sender Policy Framework (SPF)** and **Domain-based Message Authentication, Reporting & Conformance (DMARC)** are authentication mechanisms organisations can use to secure email traffic. They work together to ensure email domains are not used fraudulently, preventing the risk of spoofing, and helping block spam messages, malware and phishing attempts.

123. SPF is regarded as the minimum (basic) standard to safeguard against spoofing and impersonation. DMARC is a more advanced security mechanism that, when correctly enabled, signals a strong cybersecurity posture. While it is still not as commonly implemented as SPF, recent global statistics confirm DMARC implementation rates are growing, with a corresponding decline in domain spoofing[98].

124. Having SPF and DMARC correctly enabled does not entirely negate the threat from phishing. However, it reduces the chance of falling victim to impersonation attempts and **business email compromise (BEC) scams**. Both are common threats in the financial services sector[99].

125. In a BEC scam, cybercriminals frequently target victims with spear-phishing emails devised to impersonate the company's CEO, an employee with the authority to approve money transfers, or key suppliers, for example. The aim is to trick recipients into wiring funds to bank accounts under the cybercriminal's control or revealing highly sensitive information that could prove useful in further malicious operations. BEC scams continue proving highly profitable for cybercriminals - **in its 2019 Internet Crime Report, the FBI estimated that BEC scams cost businesses approximately USD 1.8 billion[100] globally.**

126.

48%

CREST's research revealed that **48% of the sample of financial institutions had not implemented basic email authentication measures (SPF).**

85%

85% of the sampled institutions had not implemented advanced email authentication measures (DMARC).
These results suggest there is still significant room for improving the financial service sector's defences against phishing and similar threats.

Banking Sector Cyber Security Posture

Indicator 5.5 Information Leakage Risk

Assessment – *Maturity Level 3*

Information leakage risk is assessed as average; fewer than half of the surveyed financial institutions had been identified as having had some employee credentials compromised in recent years by third-party breaches.

Information Leakage Risk

127. **The more sensitive information about an organisation is publicly available, the greater the risk of successful cyber-attacks**. Employees often expose information via social and professional platforms, which may be openly viewed by cybercriminals as a starting point for crafting phishing attacks. Alternatively, cybercriminals often gain access to login credentials via the dark web because of third-party website hacks. While the level of information leakage via employee's use of social and professional platforms is hard to quantify, it is easier to spot instances of login credential exposure, and this is often used as a measure of the problem.

128. **Employees often use their work email address to sign-up for third-party websites** – not only professional platforms but also leisure-oriented services. However, these platforms and services can expose users' sensitive information in data breaches caused by either a malicious external compromise or internal negligence.

> **73%** CREST's research revealed that **33% of the assessed financial institutions in Tanzania** had had at least some of their **employees' credentials leaked online** after unconnected attacks on third-party website-based service providers.

129. As a minimum, **work email addresses have been exposed.** In the worst case, plaintext passwords and other log-in information disclosed via third-party breaches have the potential to allow cybercriminals to directly hijack employees' corporate accounts.

    Leaked credentials may allow for more tailored and enhanced brute force attacks, providing adversaries with patterns and common combinations employees might follow when choosing passwords. Third party breaches might also lead to more sophisticated phishing efforts, with cybercriminals using the exposed information to craft highly convincing malicious messages, luring recipients into providing access or revealing additional data.

130. It has not been possible to verify how many of the assessed financial institutions follow good hygiene practices and enforce strong password best practices. These measures may help mitigate the threat associated with third-party leaked credentials. **However, the high percentage of financial institutions which have fallen victim to third-party breaches suggests the sector remains vulnerable to such threats.**

Banking Sector Cyber Security Posture

Mitigation Measures

147. **Ethically, having identified potential vulnerabilities in the financial services sector, it is good practice to outline mitigation measures that, where appropriate and proportional, financial institutions should consider adopting, including:**

Infrastructure Vulnerability

- Implement an effective patching and software update routine and ensure vulnerabilities of the highest severity and those that cybercriminals actively seek to identify and exploit are prioritised.
- Adopt an attacker's-eye perspective on your organisation to see which vulnerabilities could appear to potential adversaries.

Architecture & Access

- Review open server ports and assess whether there is a business requirement for them to be open. Close those that are not required.
- For those instances required to be internet accessible, ensure appropriate security settings, controls or authentication mechanisms are in place.

Email Authentication

- Create a Sender Policy Framework (SPF) record so it can be determined which IP addresses and hostnames are authorised to send emails from your domain.
- Implement a Domain Message Authentication, Reporting & Conformance (DMARC) policy to monitor and prevent any third parties from attempting to send emails on your behalf.

Information Leakage

- Educate employees on potential threats of using business email accounts on third-party services.
- Establish and enforce a strong password policy to reduce chances of password re-use.
- Implement additional security measures, such as multi-factor authentication.

Appendices

Appendix A

Glossary

Anti-phishing	Mechanisms and processes to defend against phishing attacks: see phishing
BEC	Business Email Compromise: a form of scam in which the cybercriminal seeks to obtain an unauthorised money transfer into an account which they control
CERT	Computer Emergency Response Team
CMAGE	Cyber Security Maturity Assessment for Global Ecosystems
CSIRT	Computer Security Incident Response Team
Dimension	The top-level partitioning of the cyber security ecosystem into five distinct areas of study: covers one or more Indicators to which metrics can be applied
DMARC	Domain-based Message Authentication, Reporting & Conformance: an advanced form of email authentication
Ecosystem	A description of the community of interacting elements which together describe the whole enterprise: in the context of this maturity model it consists of five Dimensions
Ethical Hacking	An alternative name for Penetration Testing: see PenTest
FIRST	Forum of Incident Response & Security Teams: an international association of CERTs/CSIRTs
Indicator	The lower-level partitioning of the cyber security ecosystem into manageable research topics for assessment purposes: one or more indicators build into Dimensions of the ecosystem
Information Exchange	A semi-formal mechanism for experts in different organisations to exchange information on observed cyber security threats, vulnerabilities and incidents
International (service provider)	A cyber security service provider headquartered elsewhere with offices in multiple countries which offers the service remotely or through a visiting employee
IR	Incident Response: a category of cyber security service
Local (service provider)	A cyber security service provider with one or more in-country office(s): company may additionally be classed as international, regional or locally registered
Locally registered (service provider)	A cyber security service provider which is registered and headquartered in the country
Malware	Malicious software intentionally designed to cause damage to a computer or network

Appendix A

Glossary (continued)

Multi-factor authentication	An automated process by which a user is granted access to hardware/software only after successfully presenting two or more pieces of evidence (factors) to an authentication mechanism
PenTest	Penetration Testing: a category of cyber security service in which a security tester carries out an authorised simulated attack on a system to evaluate security
Phishing	A process by which a cybercriminal attempts to obtain sensitive information, such as usernames, passwords and credit card details, by disguising themselves as trustworthy
Port	A physical or virtual connection to a computer server through which different categories of information or instructions are sent and received
Public-facing / Internet-facing	Those elements of a computer system software (and/or hardware) to which there is (paid or free) public access, often via an internet connection: distinct from those elements of a computer system which can only be accessed by authorised internal staff
Regional (service provider)	A cyber security service provider with an office in an adjacent country which offers the service remotely or through a visiting employee
Scam	A deceptive scheme or trick used to cheat an organisation or individual out of something, especially money
SFP	Sender Policy Framework; a basic form of email authentication
SOC	Security Operations Centre: a facility in which a team monitors an organisation's cyber security on an ongoing basis: facility can be in-house or outsourced to a cyber security service provider
Spear-Phishing	A highly targeted attempt at phishing in which the cybercriminal often uses known information to add authenticity to a malicious communication
Spoofing	Masking the origin of a malicious email (or other communication) to trick the recipient into believing that it is genuine: used in support of a phishing attack
Third-party breach	Occurs when a cybercriminal uses a third-party system with a trusted connection to your system (typically a supplier) to indirectly gain access to your network or steals your data directly from a (trusted) third-party
TI	(Cyber) Threat Intelligence; a category of cyber security service
VA	Vulnerability Analysis; a category of cyber security service

Appendix B

Summary of Maturity Level Definitions

The comprehensive list of maturity level definitions for each indicator is as follows:

Indicator 1.1
Government Strategy & Policy

Level 5	Level 4	Level 3	Level 2	Level 1
A coordinated cyber security delivery programme underpinned by regular reviews of strategies and policies; across all aspects of the cyber security lifecycle - awareness, education, training, development, standards, risk management, incident response and law enforcement.	Active participation in cyber security implementation and policy development by key Government departments and regulatory bodies, including the Central Bank.	Evidence of substantive actions to implement strategies and policies aimed at improving the country's cyber security posture and/or capabilities.	Some evidence of up-to-date strategies and policies aimed at improving the country's cyber security posture and/or capabilities.	No evidence of up-to-date strategies or policies aimed at improving the country's cyber security posture and/or capabilities.

Indicator 1.2
Regulator/Government Operated Assurance Schemes

Level 5	Level 4	Level 3	Level 2	Level 1
Strong evidence of successful financial services assurance scheme in operation, leading to security improvements. Evidence of best practice also across other sectors.	Evidence of financial services assurance scheme in operation. Strong evidence of regulators operating in other sectors and strategy/policy being developed in respect of assurance schemes.	Strong evidence of good regulation of financial services sector. Evolving strategy/policy in respect of financial services assurance scheme. Some evidence of regulators operating in other sectors.	Central Bank (and/or other financial services regulators) maintain accurate records. Some evidence of good regulation of financial services sector. Little evidence of regulators operating in other sectors.	No regulator operated assurance schemes identified. Limited financial services regulation by Central Bank. Little evidence of regulators operating in other sectors.

Appendix B

Summary of Maturity Level Definitions (continued)

Indicator 1.3
Law Enforcement & Cyber Defence Capabilities

Level 5	Level 4	Level 3	Level 2	Level 1
Broad spectrum of coordinated national responses to cybercrime - strategy, legal, reporting, investigation, international collaboration, awareness, education, technical measures. Credible and coordinated cyber defence posture.	National focus for reporting and specialist investigation of cybercrime. Significant investment in law enforcement and cyber defence capabilities. Strong public awareness campaigns. Widespread adoption of technical measures. Some evidence of regional/ international coordination. Strong intervention measures to divert potential cybercriminals into cyber security careers (e.g. Cyber Choices, Cyber First).	Good reporting and investigation of cybercrime. Heathy investment in law enforcement capabilities to counter cybercrime. Awareness of cybercrime within the business community and the public. Some adoption of technical measures. Some investment in cyber defence capabilities. Adoption of some intervention measures to divert potential cybercriminals into cyber security careers (e.g. Cyber Choices).	Some reporting of cybercrime and its impact. Evidence of investment in law enforcement capabilities to tackle cybercrime and some strategy/policy/legal support for tackling cybercrime. Some public awareness. Evidence of some government and military interest in cyber defence matters. Little evidence of specific measures within the financial services sector to tackle cybercrime.	Little evidence of the reporting of cybercrime and its impact. Little evidence of law-enforcement capabilities to tackle cybercrime. Little evidence of public awareness. Little evidence of interest in cyber defence matters.

Appendix B

Summary of Maturity Level Definitions (continued)

Indicator 2.1
CERTs & Information Sharing

Level 5	Level 4	Level 3	Level 2	Level 1
Fully implemented information exchange arrangements in operation across all sectors. Meets ENISA CERT Maturity Model Tier 3 requirements (more details can be found at **https://www.enisa.europa.eu/publications/study-on-csirt-maturity).**	Evidence of sector-specific CERTs and information exchanges in operation.	Evidence that National CERT has international links (FIRST etc) and is following international standards. Meets ENISA CERT Maturity Model Tier 2 requirements.	National CERT established. Meets ENISA CERT Maturity Model Tier 1 requirements.	Limited evidence of cyber incident reporting or coordinated response.

Indicator 3.1
Threat Intelligence Providers

Level 5	Level 4	Level 3	Level 2	Level 1
CREST Chapter (voluntary or self-sustaining) established with a mix of locally-registered members and international members with local offices. Strong local and international benchmarked provision of service with a self-sustaining industry representation.	Some locally-registered CREST member companies (invested or no CREST Chapter). Strong local and international benchmarked provision of service but not yet a self-sustaining industry representation.	No locally/regionally-registered CREST member companies but a strong presence from international CREST members with local offices. There are some locally registered providers, but these are not benchmarked against international standards. There is competition and international providers view the market as being mature enough for investment.	Some local/regional providers and a few CREST International members with local offices. Some competition but with no measure of quality of service for local providers.	Virtually no providers. Any that exist are likely to be small boutiques with no measure of quality. Market is not mature enough for international businesses to be active.

Appendix B

Summary of Maturity Level Definitions (continued)

Indicator 3.2
Vulnerability Assessment Providers

Level 5	Level 4	Level 3	Level 2	Level 1
CREST Chapter (voluntary or self-sustaining) established with a mix of locally-registered members and international members with local offices. Strong local and international benchmarked provision of service with a self-sustaining industry representation.	Some locally-registered CREST member companies (invested or no CREST Chapter). Strong local and international benchmarked provision of service but not yet a self-sustaining industry representation.	No locally-registered CREST member companies but a strong presence from international CREST members with local offices. There are some locally registered providers, but these are not benchmarked against international standards. There is competition and international providers view the market as being mature enough for investment.	Some local providers and a few CREST International members with local offices. Some competition but with no measure of quality of service for local providers.	Virtually no providers. Any that exist are likely to be small boutiques with no measure of quality. Market is not mature enough for international businesses to be active.

Appendix B

Summary of Maturity Level Definitions (continued)

Indicator 3.3
Penetration Testing Providers

Level 5	Level 4	Level 3	Level 2	Level 1
CREST Chapter (voluntary or self-sustaining) established with a mix of locally-registered members and international members with local offices. Strong local and international benchmarked provision of service with a self-sustaining industry representation.	Some locally-registered CREST member companies (invested or no CREST Chapter). Strong local and international benchmarked provision of service but not yet a self-sustaining industry representation.	No locally-registered CREST member companies but a strong presence from international CREST members with local offices. There are some locally registered providers, but these are not benchmarked against international standards. There is competition and international providers view the market as being mature enough for investment.	Some local providers and a few CREST International members with local offices. Some competition but with no measure of quality of service for local providers.	Virtually no providers. Any that exist are likely to be small boutiques with no measure of quality. Market is not mature enough for international businesses to be active.

Appendix B

Summary of Maturity Level Definitions (continued)

Indicator 3.4
Security Operation Centre Providers

Level 5	Level 4	Level 3	Level 2	Level 1
CREST Chapter (voluntary or self-sustaining) established with a mix of locally-registered members and international members with local offices. Strong local and international benchmarked provision of service with a self-sustaining industry representation.	Some locally-registered CREST member companies (invested or no CREST Chapter). Strong local and international benchmarked provision of service but not yet a self-sustaining industry representation.	No locally/regionally-registered CREST member companies but a strong presence from international CREST members with local offices. There are some locally registered providers, but these are not benchmarked against international standards. There is competition and international providers view the market as being mature enough for investment.	Some local/regional providers and a few CREST International members with local offices. Some competition but with no measure of quality of service for local providers.	Virtually no providers; any that exist are likely to be small boutiques with no measure of quality. Market is not mature enough for international businesses to be active.

Appendix B

Summary of Maturity Level Definitions (continued)

Indicator 3.5
Incident Response Service providers

Level 5	Level 4	Level 3	Level 2	Level 1
CREST Chapter (voluntary or self-sustaining) established with a mix of locally-registered members and international members with local offices. Strong local and international benchmarked provision of service with a self-sustaining industry representation.	Some locally-registered CREST member companies (invested or no CREST Chapter). Strong local and international benchmarked provision of service but not yet a self-sustaining industry representation.	No locally-registered CREST member companies, but a strong presence from international CREST members with local offices. There are some locally registered providers, but these are not benchmarked against international standards. There is competition and international providers view the market as being mature enough for investment.	Some local providers and a few CREST International members with local offices. Some competition but with no measure of quality of service for local providers.	Virtually no providers; any that exist are likely to be small boutiques with no measure of quality. Market is not mature enough for international businesses to be active.

Appendix B

Summary of Maturity Level Definitions (continued)

Indicator 4.1
Academia & Higher Education

Level 5	Level 4	Level 3	Level 2	Level 1
Professional bodies and government-influencing academia.	Wider academic engagement and outreach in the cyber security ecosystem.	Academia active in cyber security teaching and research. Significant local choice of cyber security degrees at BSc, MSc, and PhD. Apprenticeship (or similar) programmes available.	In addition to computer science degrees, evidence of some cyber security degrees (BSc, MSc, and PhD) and some research.	Limited evidence of an interest in cyber security within academia (teaching or research). Some computer science degrees available, but with little security content. Apprenticeship programmes not identified.

Indicator 4.2
Training Providers

Level 5	Level 4	Level 3	Level 2	Level 1
CREST Chapter (Voluntary or self-sustaining) established with locally-headquartered and international members. Strong local and international benchmarked provision of services with a self-sustaining industry representation.	Some locally-headquartered CREST member providers (invested or no CREST Chapter). Strong local and international benchmarked provision of services, but not yet a self-sustaining industry representation.	A good balance between online and local instructor-led training. No local/regional CREST training provider member companies, but strong presence from International CREST training provider member companies with local offices. There are in-country providers, but these are not benchmarked against international standards. There is competition and international providers view the market as being mature enough for investment.	Remote (online) delivery of training supplemented with some regional instructor-led provision and a few local providers. No CREST International training provider members with local offices. Some competition but with no measure of quality of service.	Mainly remote (online) delivery with virtually no instructor-led in-country/regional provision. While there may a small number of providers, they are likely to be small boutiques with no measure of quality. The market is not mature enough for international businesses to be active.

Appendix B

Summary of Maturity Level Definitions (continued)

Indicator 4.3
Professional Certifications

Level 5	Level 4	Level 3	Level 2	Level 1
All International Certification Bodies operate in-country and take up is strong. Recruitment and access to government and regulated markets demand professional certifications.	All International Certification Bodies operate in-country and take up is strong. Recruitment and access to government and regulated markets does not actively utilise professional certifications.	Most International Certification Bodies (technical, management and audit) operate in-country; take-up is developing but would not be classed as strong.	Some International Certification Bodies operate in-country, but take-up is low. Some local institutions and professional associations in operation.	Virtually no professional certifications available or taken in-country; while there may a small number of certification bodies, take-up of certification is very low. The market may not be mature enough for international businesses to be active.

Indicator 4.4
Professional Cyber Membership Organisations

Level 5	Level 4	Level 3	Level 2	Level 1
Active membership organisation(s) for individuals and companies, setting professional standards and applying enforceable codes of conduct/ethics.	Active membership organisation(s) for individuals and companies, making significant contributions to in-country events and exhibitions.	Some evidence of local cyber security membership organisations for individuals and/or companies.	Some evidence of international cyber security membership bodies representing individuals and/or companies having local chapters/branches.	No evidence of local cyber security membership organisations or local chapters/ branches of international membership bodies.

Appendix B

Summary of Maturity Level Definitions (continued)

Indicator 4.5
Specialist Recruitment

Level 5	Level 4	Level 3	Level 2	Level 1
Active specialist cyber security recruitment market. Salary and other information made publicly available. CERIS-style association available.	Active general cyber security recruitment market from generic technology recruiters. Role and job description standards encouraged. NIST and CIISEC actively encouraged.	Evidence of organised cyber security recruitment. Evidence of recruitment outreach to academia and schools, talent-spotting initiatives, and growth in the market.	Some evidence of in-country cyber security recruitment.	No evidence of in-country cyber security recruitment.

Indicator 4.6
Events & Exhibitions

Level 5	Level 4	Level 3	Level 2	Level 1
An active programme of cyber security events and exhibitions attracting local and international audiences/speakers/exhibitors.	Regular locally-organised cyber security events and exhibitions being run in-country with mix of local/international speakers/exhibitors.	Evidence of regular locally-organised dedicated cyber security events and exhibitions being run in-country.	Occasional cyber security events and exhibitions being run in-country, usually organised by an external entity.	No evidence of cyber security events and exhibitions being run in-country.

Appendix B

Summary of Maturity Level Definitions (continued)

Indicator 5.1
Banking Sector Cyber Risk Profile

Level 5	Level 4	Level 3	Level 2	Level 1
Banking sector cyber risk profile is assessed as excellent; no surveyed financial institutions received a cyber risk rating of Very High and 10% or fewer received a rating of High.	Banking sector cyber risk profile is assessed as good. 5% or fewer of the surveyed financial institutions received a cyber risk rating of Very High and 25% or fewer received a rating of High or Very High.	Banking sector cyber risk profile is assessed as average. 10% or fewer of the surveyed financial institutions received a cyber risk rating of Very High and 40% or fewer received a rating of High or Very High.	Banking sector cyber risk profile is assessed as poor. 30% or fewer of the surveyed financial institutions received a cyber risk rating of Very High and 55% or fewer received a rating of High or Very High.	Banking sector cyber risk profile is assessed as very poor. More than 30% of the surveyed financial institutions received a cyber risk rating of Very High and/or more than 55% received a rating of High or Very High.

Indicator 5.2
Infrastructure Vulnerability Risk

Level 5	Level 4	Level 3	Level 2	Level 1
Infrastructure vulnerability risk is assessed as excellent. No surveyed financial institutions had critical known vulnerabilities on their IT infrastructure and 10% or fewer had any known vulnerabilities.	Infrastructure vulnerability risk is assessed as good. 5% or fewer of the surveyed financial institutions had critical known vulnerabilities on their IT infrastructure and 25% or fewer had any known vulnerabilities.	Infrastructure vulnerability risk is assessed as average. 10% or fewer of the surveyed financial institutions had critical known vulnerabilities on their IT infrastructure and 40% or fewer had any known vulnerabilities.	Infrastructure vulnerability risk is assessed as poor. 20% or fewer of the surveyed financial institutions had critical known vulnerabilities on their IT infrastructure and 55% or fewer had any known vulnerabilities.	Infrastructure vulnerability risk is assessed as very poor. More than 20% of the surveyed financial institutions had critical known vulnerabilities on their IT infrastructure and/or more than 55% had any known vulnerabilities.

Appendix B

Summary of Maturity Level Definitions (continued)

Indicator 5.3
Architecture & Access Risk

Level 5	Level 4	Level 3	Level 2	Level 1
Architecture and Access risk is assessed as excellent. No financial institutions were identified as having potential remote access vulnerabilities and 5% or fewer were identified as having potential database vulnerabilities.	Architecture and Access risk is assessed as good. 5% or fewer of the financial institutions were identified as having potential remote access vulnerabilities and 10% or fewer were identified as having potential database vulnerabilities.	Architecture and Access risk is assessed as average. 10% or fewer of the financial institutions were identified as having potential remote access vulnerabilities and 20% or fewer were identified as having potential database vulnerabilities.	Architecture and Access risk is assessed as poor. 20% or fewer of the financial institutions were identified as having potential remote access vulnerabilities and 40% or fewer were identified as having potential database vulnerabilities.	Remote access and database risk is assessed as very poor. More than 20% of the financial institutions were identified as having potential remote access vulnerabilities and/or more than 40% were identified as having potential database vulnerabilities.

Indicator 5.4
Email Authentication Risk

Level 5	Level 4	Level 3	Level 2	Level 1
Email authentication risk is assessed as excellent. All surveyed financial institutions have correctly enabled basic email authentication measures (SPF) and 10% or fewer had not yet enabled advanced email authentication measures (DMARC).	Email authentication risk is assessed as good; 5% or fewer of the surveyed financial institutions had not correctly enabled basic email authentication measures (SPF) and 25% or fewer had not correctly enabled advanced email authentication measures (DMARC).	Email authentication risk is assessed as average; 10% or fewer of the surveyed financial institutions had not correctly enabled basic email authentication measures (SPF) and 40% or fewer had not correctly enabled advanced email authentication measures (DMARC).	Email authentication risk is assessed as poor; 15% or fewer of the surveyed financial institutions had not correctly enabled basic email authentication measures (SPF) and 70% or fewer had not correctly enabled advanced email authentication measures (DMARC).	Email authentication risk is assessed as very poor; more than 15% of the surveyed financial institutions had not correctly enabled basic email authentication measures (SPF) and/or more than 70% had not correctly enabled advanced email authentication measures (DMARC).

Appendix B

Summary of Maturity Level Definitions (continued)

Indicator 5.5
Information Leakage Risk

Level 5	Level 4	Level 3	Level 2	Level 1
Information leakage risk is assessed as excellent. 15% or fewer of the surveyed financial institutions had been identified as having had some employee credentials compromised in recent years by third-party breaches	Information leakage risk is assessed as good. 30% or fewer of the surveyed financial institutions had been identified as having had some employee credentials compromised in recent years by third-party breaches.	Information leakage risk is assessed as average. Between 31% and 50% of the surveyed financial institutions are identified as having had some employee credentials compromised in recent years by third-party breaches.	Information leakage risk is assessed as poor. More than half of the surveyed financial institutions have had at least some employee credentials compromised in recent years by third-party breaches.	Information leakage risk is assessed as very poor. More than 80% of the surveyed financial institutions have been identified as having had at least some employee credentials compromised in recent years by third-party breaches.

Appendix C

Professional Certifications and Member Organisations

Background

1. Knowledge, skills and experience are three factors used by companies when determining who to hire or promote. These factors are also used by a buyer when selecting which service provider to award a contract to. Experience is a matter of record and can be underpinned by endorsements from former employers or clients.

   In a mature marketplace, certifications are the common currency used to express an individual's knowledge and skills. Employers can quickly filter potential candidates by certifications they hold. Buyers can also use certifications as a benchmark when looking to award a contract. The availability and use of certifications in both scenarios are a useful indicator of the maturity of a marketplace.

Career progression model

2. For ease of evaluation, various cyber security certifications have been categorised into a career progression model using a five-tier hierarchy denoting approximate skill level equivalence;
   - Foundation (New Entrant)
   - Practitioner (Intermediate)
   - Senior Practitioner (Subject Matter Expert/Advanced)
   - Principle Advanced (Subject Matter Expert/Senior Management/Chartered)
   - Lead Practitioner (Fellow/Recognised Industry Expert)

   In some career progression models there are two tiers below Foundation (often referred to as the 'Transition Boundary' into the industry).

Certification bodies

3. During CREST's research, fifteen organisations were identified as offering one or more certification of relevance to the cyber security profession. Together, they offer 142 different certifications, including 118 with differing degrees of technical content (grouped as 'Technical Certificates of Relevance') and 24 more focused on security management and other skillsets (grouped at 'Other Certificates of Relevance'). In some cases, certification organisations also act as professional membership organisations, holding events and contributing to through-career development of members.

4. Most certification bodies offer certifications with online exams or through Pearson Vue or PSI test centres. Some certifications requiring practical exams offer this element online, or through connection to a remote network, although some bodies need a physical testing site, which have limited availability in Africa.

5. Certification bodies and individual certifications are shown in the following table by assessed tier level. Exam delivery options are also shown. For brevity, the abbreviation for each certification has been used; the full title of each certification and more details on the exam delivery options are shown on the awarding body's website (also shown in the associated endnote in **Appendix F**).

Appendix C

Professional Certifications and Member Organisations (continued)

Certification Body	CERTIFICATION TIER					EXAM DELIVERY				
	Foundation	Practitioner	Senior Practitioner	Principle Advanced	Lead Practitioner	Online	Pearson Vue Centre	PSI Test Centre	Training Classroom	Specialist Test Centre
TECHNICAL CERTIFICATES OF RELEVANCE										
CREST[101]		CPSA CPIA CPTIA	CRT CRTIA CRTSA CRIA CC NIA CCHIA CCMRE	CCSAS CCSAM CCTIM, CCIM CCT Inf CCT App CCWS	Fellow		✓			✓
EC Council[102]	CEH CND ECSS	ECSA ECIH EDRP CASE-Java CASE-.Net ECES CTIA	APT LPT CHFI CAST CEH(Master) CSA	ECDA ECTI		✓	✓		✓	
ISACA[103]		CSX-P	CISA CRISC CISM		CGEIT	✓		✓		
(ISC)2[104]		HCISPP SSCP CAP	CISSP CCSP CSSLP		CISSP-AP CISSP-EP CISSP-MP		✓			
SANS[105]		GSEC GPEN GWAPT GICSP GCIP GCWN GCUX GAWN GPYC GWEB GCIH GCFE GASF GREM GCFA GNFA GSSP-Java GSSP-.Net GICSP GMOB GBFA GCSA	GXPN GCCC GSED GPPA GMON GCIA GRID GCDA GCTI GCED GPPA GDSA GDAT GEVA GNSA		GSE	✓	✓			
CompTIA[106]	Pentest+ Security+	CySA+	CASP+			✓	✓			
Offensive Security[107]		OSCP OSWP	OSCE OSWE	OSEE		✓				
Cloud Security Alliance[108]		CCSK				✓				

Appendix C

Professional Certifications and Member Organisations (continued)

Certification Body	CERTIFICATION TIER					EXAM DELIVERY				
	Foundation	Practitioner	Senior Practitioner	Principle Advanced	Lead Practitioner	Online	Pearson Vue Centre	PSI Test Centre	Training Classroom	Specialist Test Centre
TECHNICAL CERTIFICATES OF RELEVANCE										
PCI[109]		PCIP PCI-DSS QPA	PCI-DSS ISA PCI-DSS AQSA		PCI-DSS QSA PA-QSA PCI-DSS 3DS PCI-DSS P2PE PCI-DSS Secure Software Lifecycle Assessor PCI-DSS Secure Software Assessor PCI-DSS CPSA	✓	✓			
Cisco[110]		CCNA CC CyberOps Associate	CCNP Security CC CyberOps Professional	CCIE Security			✓			✓
Microsoft[111]	MTA: Security Fundamentals	Azure Security Engineer Associate Microsoft 365 Security Administrator Associate				✓	✓			
Amazon Web Services[112]	AWS Certified Security					✓	✓	✓		
OTHER CERTIFICATES OF RELEVANCE										
EC Council	CNDA CSCU			CCISO		✓	✓		✓	
ISACA		Cybersecurity Audit Scheme COBIT Program	CDPSE			✓		✓		
(ISC)2	Associate of (ISC)2						✓			
SANS	GISF	GLEG GSNA	GISP GCPM	GSLC	GSTRT	✓	✓			
IRCA (ISMS)[113]	Associate Auditor	Internal Auditor	Auditor	Lead Auditor	Principle Auditor				✓	
BCS[114]	CiSMP	BCM CIAA	CIRM				✓		✓	✓
IET[115]	ICTTech									✓

Appendix D

Country Context

Geography

1. Tanzania is the largest country in East Africa. It is situated with Uganda and Kenya to the North, the Indian Ocean to the East, Mozambique to the Southeast, Zambia and Malawi to the Southwest and Rwanda, Burundi, and the DRC to the West[116]. Tanzania's capital is Dodoma, though Dar es Salam is the largest city and port[117]. Tanzania is home to Mount Kilimanjaro, and has the largest animal population per square mile than any other country in the world[118].
2. After the death of President John Magufuli, President Samia Suluhu Hassan was sworn in on March 19, 2021 as the United Republic of Tanzania's sixth, and first female, presiden.[119]

Natural resources

3. Gold is one of the most important natural resources and most valuable export for Tanzania. Diamonds, kaolin, gypsum, tin, and various gemstones, including tanzanite, are also mined[120]. Power is provided by imported petroleum, hydroelectric power, and coal, which is also mined in-country[121].

Population

4. According to the World Population Review, as of 2021, the current population of Tanzania is 61,112,037, based on projections United Nations data and the population is projected to reach 282.67 million by the end of the century[122]. Tanzania's population growth rate is 2.98%, due to Tanzania's high fertility rate of 4.8 births per woman, and a high birth rate of 36.2 births per 1,000 people[123].

Economy

5. According to Serianu's 2017 "Demystifying Africa's Cyber Security Poverty Line" report, Tanzania's GDP in 2017 was US$47bn[124]. Encyclopaedia Britannica states Tanzania's 2017 GNI was $50,361 USD, and per capita GNI in 2017 was US$910.[125]
6. The World Bank reports that Tanzania has had a strong income growth over the past decade, and that in July 2020 Tanzania's gross national income (GNI) per capita increased from $1,020 in 2018 to $1,080 in 2019, exceeding the threshold for lower-middle income status[126]. The World Bank commented on the Tanzania Development Vision 2025, and aspirations to become a middle-income country by 2025[127], with high quality living, peace, stability, and good governance, for example. It states that while increased GNI per capita is impressive, it is not enough to reach these goals, and that investment into human development and physical capital is key[128].
7. The World Bank also comments on the number of Tanzanians living below the national poverty line. While GNI has grown, so has the population. This rapid population growth has caused the number of people living below the poverty line to increase. In 2020, the COVID-19 pandemic-induced economic slowdown caused the poverty rate to rise to an estimated 27.2%, compounding the effect of population growth on those living in poverty[129].

Appendix D

Country Context (continued)

Internet connectivity

8. Serianu's 2017 "Demystifying Africa's Cyber Security Poverty Line" report stated that internet penetration for Tanzania in 2017 was at 39% of the population[130].
9. In the Ministry of Finance and Planning's Implementation Strategy for the National Plan 2016-2021, Vol 1 – The Action Plan[131], as at 2018, it states Tanzania had completed a National ICT Infrastructure Backbone Project - after laying 25,954 kilometres of optical fibre cable covering 24 regions of mainland Tanzania. Connectivity to submarine cables (EASSy & SEACOM) and cross-border connectivity with neighbouring countries (Kenya, Uganda, Rwanda, Malawi, Burundi, and Zambia) had been successfully implemented[132].

Cyber crime

10. According to Serianu's 2017 "Demystifying Africa's Cyber Security Poverty Line" report, which studied 10 African countries including Tanzania, the estimated cost of cybercrime to the country was US$99m[133].
11. The World Bank reports Tanzania's situation has deteriorated or been stagnant in most governance areas between 2012 and 2019. The strongest decline, according to the Bank, is in terms of the rule of law, governance effectiveness, and accountability, where it notes that political, media and civil societies freedoms have shrunk[134].
12. In the 2019 ACME article, Tanzania's 'worrying decline of media freedom', it reports the arrest of a journalist and that the arrest represents a further clamp down on critical reporting, a free media and free speech. The article also reported that Tanzania ranks 118th out of 180 countries in Reporters Without Borders (RSF) World Press Freedom Index this year, 25 positions below its 2018 ranking[135]. There are more articles on a similar theme on the ACME website[136].
13. In an Article on the CIPESA website (2020), "Tanzania Tramples Digital Rights in Fight Against Covid-19"[137], it comments that in July 2020 the Tanzania government repealed the 2018 Tanzania's Electronic and Postal Communications (Online Content) Regulations, replacing it with the Tanzania Electronic and Postal Communications (Online Content) Regulations 2020. The latter aggravate the crackdown on free speech as it requires the registration of bloggers, online discussion forums, radio, and television webcasters. The new regulations are reported to be so vague in their definitions that their application could be open to interpretation - and so boundless. The more recent regulations prohibit publication of any "content with information with regards to the outbreak of a deadly or contagious disease in the country or elsewhere without the approval of the respective authorities." The article goes onto give more examples where freedom of speech has been curtailed[138].
14. Another article from CIPSEA (2019), UN Human Rights Council Called to Address Deterioration of Freedoms in Tanzania, reports on the draconian legislation enacted since 2015 that restricts freedom of opinion, speech and enables harassment of human rights defenders[139].
15. While the above examples are not cybercrime examples, they show how cyber space is being used and controlled by the authorities.
16. Directly related to cybercrime, one of the more recent articles found was in Tanzania's The Guardian Reporter (2017), which revealed that Tanzania was one of 150 countries targeted in a huge global cyber-attack. The TCRA issued a warning to all computer users to keep their operating systems up to date[140].

Appendix D

Country Context (continued)

Cyber Security Professional Development

17. Tanzania follows a 6-4-2-3 system of education, so primary school takes six years, followed by four years of secondary school, two years of high school (advanced level), and three years of first-degree university education[141]. According to an ICT in Education in Tanzania (2007) report there were a total of 14,700 primary schools, 2,289 secondary schools, 20 tertiary colleges (vocational training centres), and 53 teacher-training colleges[142].

18. According to the 2017 Serianu Africa Cyber Security Report, there were an estimated 300 cyber security professionals working in Tanzania.

Other maturity models

19. Oxford University's Global Cyber Security Capacity Centre (GCSCC) and the Commonwealth Telecommunications Organisation (CTO) have not yet published their report on Tanzania. The report research seems to have been conducted in 2016[143].

Appendix E

Bibliography

This bibliography is the list of all articles and the main websites accessed for qualitative research. Some references will also be listed in the endnotes where specific information had been used in writing this report. Details of individual websites of the numerous organisations accessed during the initial stages of quantitative research for each individual dimension and indicator is held seperately, and can be made available upon request to CREST.

Africa CERT, 2020,
https://www.africacert.org/about-us/
(accessed July and 27 Oct 2020)

African Centre for Media Excellence,
https://acme-ug.org/
(accessed July and Oct 2020)

African Centre for Media Excellent (ACME) (2019). Tanzania's 'worrying decline of media freedom'. Uganda: *Author* (available from)
https://acme-ug.org/2019/08/19/tanzanias-worrying-decline-of-media-freedom/ (accessed April 2021)

After School Africa (2016). TCRA ICT Scholarships for Tanzania Students in Tanzania 2016/2017. Nigeria: *Author* (avail online)
https://www.afterschoolafrica.com/4508/tcra-ict-scholarships-for-tanzania-students-in-tanzania/
(accessed Mar 21)

Bank of England and CBEST, CBEST Intelligence Led Testing, Understanding Cyber Threat Intelligence Operations, V2, UK, *Bank of England*, 2016,
https://www.bankofengland.co.uk/-/media/boe/files/financial-stability/financial-sector-continuity/understanding-cyber-threat-intelligence-operations.pdf (accessed Nov 2020)

Bank of Tanzania (2012). Call for Tender for Provision of Consultancy Services to perform Technology Vulnerability Assessments and Establish Adequacy of ICT Asset Controls. Tender no PA/082/2012-13/ HQ/C/04. Tanzania: *Author.* (available online)
https://www.bot.go.tz/Adverts/CallsforTender/en/20200107005645971136.pdf (accessed Mar 2021)

CIPESA Writer (2020). Tanzania Tramples Digital Rights in Fight Against Covid-19. Uganda: *Collaboration on International ICT Policy in East and Southern Africa* (CIPESA). (available from)
https://cipesa.org/2020/10/tanzania-tramples-digital-rights-in-fight-against-covid-19-as-elections-loom/
(accessed April 2021)

CIPESA (2019). UN Human Rights Council Called to Address Deterioration of Freedoms in Tanzania. Uganda: *Author* (available from)
https://cipesa.org/2019/05/un-human-rights-council-called-to-address-deterioration-of-freedoms-in-tanzania/ (accessed April 2021)

Courses Eye,
https://www.courseseye.com
(accessed April 2021)

Collaboration on International ICT Policy in East and Southern Africa (CIPESA),
https://cipesa.org/about-us/ (accessed April 2021)

CREST, UK,
https://www.crest-approved.org/
(accessed Nov 2020)

CREST, 'Cyber Security Incident Response Guide V1', 2013, UK, *Author,*
https://www.crest-approved.org/wp-content/uploads/2014/11/CSIR-Procurement-Guide.pdf
(accessed Nov 2020)

European Union Agency for Network and Information Security (ENISA), 'ENISA CSIRT Maturity Assessment Model,' 30 April 2019, *Author.*
https://www.enisa.europa.eu/publications/study-on-csirt-maturity (Accessed 4 Nov 2020)

Forum of Incident Response and Security Teams (FIRST), 2015-2020,
https://www.first.org/about/mission
(accessed April 2021)

Global Cyber Security Capacity Centre, (2021). CMM Reviews Around the World. Oxford.
https://gcscc.ox.ac.uk/cmm-reviews#/
(accessed 1 April 2021)

Hare Harry, (2007). SURVEY OF ICT AND EDUCATION IN AFRICA: Tanzania Country Report - ICT in Education in Tanzania. *Info Dev.org:* (available from)
https://www.infodev.org/infodev-files/resource/InfodevDocuments_432.pdf (accessed April 2021)

Appendix E

Bibliography (continued)

Information Communication Technologies (ICT) Commission (2021).
https://www.ictc.go.tz/index.php
(accessed Aug 20 and Mar 21)

Internet Authority, (2021). Tanzania:
https://www.ega.go.tz/what-we-do
(accessed April 21)

Ingham, K, Bryceson, DF, Mascarenhas, AC. and Chiteji, FM. (2021). Tanzania. *Encyclopaedia Britannica*.
https://www.britannica.com/place/Tanzania
(Accessed 1 April 2021)

Macroeconomic and Financial Management Institute of Eastern and Southern Africa (MEFMI), *Author,*
http://mefmi.org/ (Accessed Oct 2020)

Ministry of Finance and Planning, (no date) Tanzania Development Plan, Vision, and Investment Priorities to Achieve Middle Income Status by 2025.
Tanzania: *Tanzania Investment Centre.* Available from:
https://www.mcci.org/media/154357/tanzania-developemnt-plan-booklet.pdf (accessed Mar 21)

Ministry of Finance and Planning (2018). Implementation Strategy for the National Five-Year Development Plan 2016/17-2020/21 Volume 1 The Action Plan.
Tanzania: *Author.*
http://www.mof.go.tz/docs/The%20Action%20Plan%20of%20Implementation%20of%20the%202nd%20FYDP.pdf (accessed Mar 21)

Ministry of Finance and Planning (2021). Policy and Strategies.
Tanzania: *Author*
http://www.mof.go.tz/index.php/policy/policy-and-strategies (accessed Mar 21)

Ministry of Education Science and Technology (2016). ICT Training Program.
Tanzania: *Author.* (Avail online)
http://www.moe.go.tz/en/project/ict-training-programme (accessed April 21)

Ministry for Works and Transport (2018), The Electronic and Postal Communications (Computer Emergency Response Team) Regulations 2018.
Tanzania: *Author* (avail online)
https://www.tcra.go.tz/document/The%20Electronic%20and%20Postal%20Communications%20(Computer%20Emergency%20Response%20Team)%20Regulations,%202018
(accessed April 2021)

Ministry of Works, Transport and Communications (2016). National Information Communications Technology Policy 2016. Tanzania: *Author.* Available from:
https://www.ictc.go.tz/index.php/about-us/national-ict-policy (Accessed Mar 21)

Ministry of Works, Transport and Communications (MWTC) (2016). National Information and Communications Technology Policy (NICP) 2016 – Implementations Strategy 2016/17-2020/21.
Tanzania: *Author.* Available from:
https://www.ictc.go.tz/index.php/component/phocadownload/category/4-policies?download=48:107
(accessed Aug 20 and Mar 21)

National Cyber Security Centre (NCSC), *Author,* UK,
https://www.ncsc.gov.uk/ (accessed Nov 2020)

National Cyber Security Index, "National Cyber Security Index 2018", *Estonia, e-Governance Academy,* 2018,
https://ega.ee/wp-content/uploads/2018/05/ncsi_digital_smaller.pdf (accessed Oct 2020)

National Tanzania Computer Emergency Response Team (TZ-CERT) (2021)
https://www.tzcert.go.tz/about-us/
(accessed Aug 20 and Mar 21)

Omar Hayla (2020) Tanzania: Cybercrime Related Cases Drop Drastically – Police.
Tanzania: *Tanzania Daily News.* (available online from)
https://allafrica.com/stories/202003170618.html
(accessed April 210)

Serianu, 'Africa Cyber Security Report 2017 - Demystifying Africa's Cyber Security Poverty Line' Kenya, *Author,* 2017,
https://www.serianu.com/downloads/AfricaCyberSecurityReport2017.pdf
(Accessed July 2020)

Appendix E

Bibliography (continued)

Tanzania Communications Regulatory Authority (TCRA) (2021)
https://www.tcra.go.tz/about-tcra/tcra-profile
(accessed Aug 20 and April 21)

Tanzania Industrial Research and Development Organisation (TIRDO) (2017). Information and Communication Technologies Division.
Tanzania: *Author.* (available online)
https://www.tirdo.or.tz/ict.php (accessed April 2021)

Tanzanian Police Force (2021).
Resources. (Available online)
https://www.polisi.go.tz/resources/
(accessed Aug 20 and April 21)

The African Network Information Centre (AFRINIC),
https://afrinic.net/about
(accessed April 2021)

The Guardian Reporter (2017). Tanzania targeted by Huge Global Cybercrime Attack.
Tanzania: *IPP Media.* (available from)
https://www.ippmedia.com/en/news/tanzania-targeted-huge-global-cyber-crime-attack
(accessed April 2021)

The United Republic of Tanzania (2015)
The Cybercrime Act 2015.
Tanzania: *The Gazette of the United Republic of Tanzania* No 22 Vol 96 22 May 2015. (avail online)
https://www.tcra.go.tz/document/The%20Cybercrimes%20Act,%202015
(accessed Aru 20 and April 21)

The United Republic of Tanzania (2010) Electronic and Postal Communications Act No 3, 2010.
Tanzania: *Author* (Avail Online) Part VI, para 124.
https://www.tcra.go.tz/document/The%20Electronic%20and%20Postal%20Communications%20Act,%202010%20(Act%20No.%203%20out%20of%2010) (accessed April 21)

The United Republic of Tanzania Planning Commission (no date). The Tanzania Development Vision 2025.
Tanzania: *Ministry of Finance and Planning*.
(Avail Online from):
http://www.mof.go.tz/mofdocs/overarch/vision2025.htm#1.0%20DEVELOPMENT%20VISION
(accessed April 21)

The United Republic of Tanzania, Planning Commission (no date). Tanzania Development Vision 2025.
Tanzania: *Author.* Ch 4, para 4.3, p20-21. (pdf format available from)
https://www.extractiveshub.org/servefile/getFile/id/1826 (accessed April 21)

The World Bank, (2021). The World Bank in Tanzania – Economic Overview. *Author*, 23 March 2021,
https://www.worldbank.org/en/country/tanzania/overview (accessed April 2021)

UN, (2020). UNDIR Cyber Security Portal – Tanzania.
Author. (avail from)
https://unidir.org/cpp/en/states/unitedrepublicoftanzania (accessed April 2021)

World Population Review (2021) Tanzania Population 2021. *Author.* (avail from)
https://worldpopulationreview.com/countries/tanzania-population (accessed April 2021)

Appendix F

Endnotes

Endnotes have been used to reference specific information instead of footnotes to prevent the sheer quantity of references from interrupting the report flow. If you are reading this electronically, endnotes can be read without flipping to this Appendix. By rolling over the endnote number within the text, the reference will then appear.

1. Further information available on the Bill & Melinda Gates Foundation, Financial Services for the Poor programme website, **https://www.gatesfoundation.org/What-We-Do/Global-Growth-and-Opportunity/Financial-Services-for-the-Poor** (accessed 29 Oct 2020)
2. Further information available on the CREST International website, **https://crest-approved.org/** (accessed 29 Oct 2020)
3. Further information available on the Orpheus Cyber website, **https://orpheus-cyber.com/** (accessed 29 Oct 2020)
4. The United Republic of Tanzania Planning Commission (no date). The Tanzania Development Vision 2025. Tanzania: *Ministry of Finance and Planning.* Avail from: **http://www.mof.go.tz/mofdocs/overarch/vision2025.htm#1.0%20DEVELOPMENT%20VISION** (accessed April 21)
5. The United Republic of Tanzania, Planning Commission (no date). Tanzania Development Vision 2025. Tanzania: *Author.* Ch 4, para 4.3, p20-21. (pdf format available from) **https://www.extractiveshub.org/servefile/getFile/id/1826** (accessed April 21)
6. Ministry of Finance and Planning, (no date). Tanzania Development Plan, Vision and Investment Priorities to Achieve Middle Income Status by 2025. Tanzania: *Tanzania Investment Centre.* pp6-7. Available from: **https://www.mcci.org/media/154357/tanzania-developemnt-plan-booklet.pdf** (accessed Mar 21)
7. Ministry of Finance and Planning, (no date). Tanzania Development Plan, Vision and Investment Priorities to Achieve Middle Income Status by 2025. Tanzania: *Tanzania Investment Centre.* Ch3 p13. Available from: **https://www.mcci.org/media/154357/tanzania-developemnt-plan-booklet.pdf** (accessed Mar 21)
8. Ministry of Finance and Planning, (no date). Tanzania Development Plan, Vision and Investment Priorities to Achieve Middle Income Status by 2025. Tanzania: *Tanzania Investment Centre.* Ch5 p28. Available from: **https://www.mcci.org/media/154357/tanzania-developemnt-plan-booklet.pdf** (accessed Mar 21)
9. Ministry of Finance and Planning, (no date). Tanzania Development Plan, Vision and Investment Priorities to Achieve Middle Income Status by 2025. Tanzania: *Tanzania Investment Centre.* Ch1 pp5-7. Available from: **https://www.mcci.org/media/154357/tanzania-developemnt-plan-booklet.pdf** (accessed Mar 21)
10. Ministry of Finance and Planning (2021). Policy and Strategies. Tanzania: *Author* **http://www.mof.go.tz/index.php/policy/policy-and-strategies** (accessed Mar 21)
11. Ministry of Finance and Planning (2018). Implementation Strategy for the National Five-Year Development Plan 2016/17-2020/21 Volume 1 The Action Plan. Tanzania: *Author.* **http://www.mof.go.tz/docs/The%20Action%20Plan%20of%20Implementation%20of%20the%202nd%20FYDP.pdf** (accessed Mar 21)
12. Information Communication Technologies (ICT) Commission (2021). **https://www.ictc.go.tz/index.php** (accessed Aug 20 and Mar 21)
13. Information Communication Technologies (ICT) Commission (2021). ICT Professionals About Registration. **https://www.ictc.go.tz/index.php/3/about-registration** (accessed Aug 20 and Mar 21)

Appendix F

Endnotes (continued)

14. Information Communication Technologies (ICT) Commission (2021). National ICT Policy. Tanzania. *Author* **https://www.ictc.go.tz/index.php/about-us/national-ict-policy** (accessed Mar 21)

15. Internet Authority, (2021). Tanzania: **https://www.ega.go.tz/what-we-do** (accessed April 21)

16. The United Republic of Tanzania (2019). eGovernment Act no 10 of 2019. Tanzania: *The Gazette of the United Republic of Tanzania* No 39 Vol 100 20th September 2019. Tanzania: (Available online) **https://www.ega.go.tz/uploads/publications/en-1574849310-eGov%20act,%202019.pdf** (accessed April 21)

17. Internet Authority, (2021). Tanzania: **https://www.ega.go.tz/what-we-do** (accessed April 21)

18. Internet Authority, (2021). Tanzania: **https://www.ega.go.tz/what-we-do** (accessed April 21)

19. Internet Authority, (2021). Our Systems and Services. Tanzania: **https://www.ega.go.tz/products-services** (accessed April 21)

20. Tanzania Industrial Research and Development Organisation (TIRDO) (2017). Information and Communication Technologies Division. Tanzania: *Author*. (available on line) **https://www.tirdo.or.tz/ict.php** (accessed April 2021)

21. Ministry of Works, Transport and Communications (2016). National Information Communications Technology Policy 2016. Tanzania: *Author*. Available from: **https://www.ictc.go.tz/index.php/about-us/national-ict-policy** (Accessed Mar 21)

22. Ministry of Works, Transport and Communications (MWTC) (2016). National Information and Communications Technology Policy (NICP) 2016 – Implementations Strategy 2016/17-2020/21. Tanzania: *Author*. Available from: **https://www.ictc.go.tz/index.php/component/phocadownload/category/4-policies?download=48:107** (accessed Aug 20 and Mar 21)

23. The United Republic of Tanzania Planning Commission (no date). The Tanzania Development Vision 2025. Tanzania: *Ministry of Finance and Planning*. Avail from: **http://www.mof.go.tz/mofdocs/overarch/vision2025.htm#1.0%20DEVELOPMENT%20VISION** (accessed April 21)

24. Ministry of Finance and Planning (2021). Policy and Strategies. Tanzania: *Author* **http://www.mof.go.tz/index.php/policy/policy-and-strategies** (accessed Mar 21)

25. The United Republic of Tanzania (2015) The Cybercrime Act 2015. Tanzania: *The Gazette of the United Republic of Tanzania* No 22 Vol 96 22 May 2015. (avail online) **https://www.tcra.go.tz/document/The%20Cybercrimes%20Act,%202015** (accessed Aru 20 and April 21)

26. Ministry for Works and Transport (2018), The Electronic and Postal Communications (Computer Emergency Response Team) Regulations 2018. Tanzania: *Author* (avail online) **https://www.tcra.go.tz/document/The%20Electronic%20and%20Postal%20Communications%20(Computer%20Emergency%20Response%20Team)%20Regulations,%202018** (accessed April 2021)

27. The United Republic of Tanzania (2019). eGovernment Act no 10 of 2019. Tanzania: *The Gazette of the United Republic of Tanzania* No 39 Vol 100 20th September 2019. Tanzania: (Available online) **https://www.ega.go.tz/uploads/publications/en-1574849310-eGov%20act,%202019.pdf** (accessed April 21)

28. Ministry of Works, Transport and Communications (2016). National Information Communications Technology Policy 2016. Tanzania: *Author*. pp vi. Available from: **https://www.ictc.go.tz/index.php/about-us/national-ict-policy** (Accessed Mar 21)

Appendix F

Endnotes (continued)

29. Ministry of Works, Transport and Communications (2016). National Information Communications Technology Policy 2016. Tanzania: *Author*. Ch3 pp15-33. Available from: **https://www.ictc.go.tz/index.php/about-us/national-ict-policy** (Accessed Mar 21)

30. Ministry of Works, Transport and Communications (MWTC) (2016). National Information and Communications Technology Policy (NICP) 2016 – Implementations Strategy 2016/17-2020/21. Tanzania: *Author.* Available from: **https://www.ictc.go.tz/index.php/component/phocadownload/category/4-policies?download=48:107** (accessed Aug 20 and Mar 21)

31. Ministry of Works, Transport and Communications (MWTC) (2016). National Information and Communications Technology Policy (NICP) 2016 – Implementations Strategy 2016/17-2020/21. Tanzania: *Author.* Ch2,2.1.2, p7. Available from: **https://www.ictc.go.tz/index.php/component/phocadownload/category/4-policies?download=48:107** (accessed Aug 20 and Mar 21)

32. Ministry of Works, Transport and Communications (MWTC) (2016). National Information and Communications Technology Policy (NICP) 2016 – Implementations Strategy 2016/17-2020/21. Tanzania: *Author.* Available from: **https://www.ictc.go.tz/index.php/component/phocadownload/category/4-policies?download=48:107** (accessed Aug 20 and Mar 21)

33. Ministry of Works, Transport and Communications (MWTC) (2016). National Information and Communications Technology Policy (NICP) 2016 – Implementations Strategy 2016/17-2020/21. Tanzania: *Author*. Available from: **https://www.ictc.go.tz/index.php/component/phocadownload/category/4-policies?download=48:107** (accessed Aug 20 and Mar 21)

34. Ministry of Works, Transport and Communications (MWTC) (2016). National Information and Communications Technology Policy (NICP) 2016 – Implementations Strategy 2016/17-2020/21. Tanzania: *Author*. Ch4, 4.1, p25. Available from: **https://www.ictc.go.tz/index.php/component/phocadownload/category/4-policies?download=48:107** (accessed Aug 20 and Mar 21)

35. Ministry of Works, Transport and Communications (MWTC) (2016). National Information and Communications Technology Policy (NICP) 2016 – Implementations Strategy 2016/17-2020/21. Tanzania: *Author.* Ch4, 4.1, p26. Available from: **https://www.ictc.go.tz/index.php/component/phocadownload/category/4-policies?download=48:107** (accessed Aug 20 and Mar 21)

36. Ministry of Works, Transport and Communications (MWTC) (2016). National Information and Communications Technology Policy (NICP) 2016 – Implementations Strategy 2016/17-2020/21. Tanzania: *Author.* Ch4, 4.1, p30. Available from: **https://www.ictc.go.tz/index.php/component/phocadownload/category/4-policies?download=48:107** (accessed Aug 20 and Mar 21)

37. Ministry of Works, Transport and Communications (MWTC) (2016). National Information and Communications Technology Policy (NICP) 2016 – Implementations Strategy 2016/17-2020/21. Tanzania: *Author.* Ch4, p56. Available from: **https://www.ictc.go.tz/index.php/component/phocadownload/category/4-policies?download=48:107** (accessed Aug 20 and Mar 21)

Appendix F

Endnotes (continued)

38. Ministry of Works, Transport and Communications (MWTC) (2016). National Information and Communications Technology Policy (NICP) 2016 – Implementations Strategy 2016/17-2020/21. Tanzania: *Author*. Ch4, 4.1, p31. Available from: **https://www.ictc.go.tz/index.php/component/phocadownload/category/4-policies?download=48:107** (accessed Aug 20 and Mar 21)

39. Ministry of Works, Transport and Communications (MWTC) (2016). National Information and Communications Technology Policy (NICP) 2016 – Implementations Strategy 2016/17-2020/21. Tanzania: *Author*. Ch4, p57. Available from: **https://www.ictc.go.tz/index.php/component/phocadownload/category/4-policies?download=48:107** (accessed Aug 20 and Mar 21)

40. Ministry of Finance and Planning (2018). Implementation Strategy for the National Five-Year Development Plan 2016/17-2020/21 Volume 1 The Action Plan. Tanzania: *Author.* **http://www.mof.go.tz/docs/The%20Action%20Plan%20of%20Implementation%20of%20the%202nd%20FYDP.pdf** (accessed Mar 21)

41. Ministry of Finance and Planning (2021). Policy and Strategies. Tanzania: *Author* **http://www.mof.go.tz/index.php/policy/policy-and-strategies** (accessed Mar 21)

42. Ministry of Finance and Planning (2018). Implementation Strategy for the National Five-Year Development Plan 2016/17-2020/21 Volume 1 The Action Plan. Ch 2 Para 2.3.1.5 pp24. Tanzania: *Author.* **http://www.mof.go.tz/docs/The%20Action%20Plan%20of%20Implementation%20of%20the%202nd%20FYDP.pdf** (accessed Mar 21)

43. Ministry of Finance and Planning (2018). Implementation Strategy for the National Five-Year Development Plan 2016/17-2020/21 Volume 1 The Action Plan. Ch 2 Para 2.3.6.1 pp48. Tanzania: *Author.* **http://www.mof.go.tz/docs/The%20Action%20Plan%20of%20Implementation%20of%20the%202nd%20FYDP.pdf** (accessed Mar 21)

44. Ministry of Finance and Planning (2018). Implementation Strategy for the National Five-Year Development Plan 2016/17-2020/21 Volume 1 The Action Plan. Annexes, Table B XII ICT, pp194. Tanzania: *Author*. **http://www.mof.go.tz/docs/The%20Action%20Plan%20of%20Implementation%20of%20the%202nd%20FYDP.pdf** (accessed Mar 21)

45. Ministry of Finance and Planning (2018). Implementation Strategy for the National Five-Year Development Plan 2016/17-2020/21 Volume 1 The Action Plan. Ch 2 Para 2.3.6.2 pp49. Tanzania: Author. **http://www.mof.go.tz/docs/The%20Action%20Plan%20of%20Implementation%20of%20the%202nd%20FYDP.pdf** (accessed Mar 21)

46. Ministry of Finance and Planning (2018). Implementation Strategy for the National Five-Year Development Plan 2016/17-2020/21 Volume 1 The Action Plan. Annexes, Table B XIII E-Government, pp195. Tanzania: *Author.* **http://www.mof.go.tz/docs/The%20Action%20Plan%20of%20Implementation%20of%20the%202nd%20FYDP.pdf** (accessed Mar 21)

47. Ministry of Finance and Planning (2018). Implementation Strategy for the National Five-Year Development Plan 2016/17-2020/21 Volume 1 The Action Plan. Annexes, Table B XII ICT, pp194, Table B XIII E-Government, pp195. Tanzania: *Author.* **http://www.mof.go.tz/docs/The%20Action%20Plan%20of%20Implementation%20of%20the%202nd%20FYDP.pdf** (accessed Mar 21)

Appendix F

Endnotes (continued)

48. Ministry of Finance and Planning (2018). Implementation Strategy for the National Five-Year Development Plan 2016/17-2020/21 Volume 1 The Action Plan. Annexes, Table B XIII E-Government, pp195. Tanzania: *Author.* **http://www.mof.go.tz/docs/The%20Action%20Plan%20of%20Implementation%20of%20the%202nd%20FYDP.pdf** (accessed Mar 21)

49. Internet Authority, (2021). Our Systems and Services. Tanzania: **https://www.ega.go.tz/products-services** (accessed April 21)

50. The United Republic of Tanzania (2019). eGovernment Act no 10 of 2019. Tanzania: The Gazette of the United Republic of Tanzania No 39 Vol 100 20th September 2019. Tanzania: (Available online) **https://www.ega.go.tz/uploads/publications/en-1574849310-eGov%20act,%202019.pdf** (accessed April 21)

51. Bank of Tanzania (2012). Call for Tender for Provision of Consultancy Services to perform Technology Vulnerability Assessments and Establish Adequacy of ICT Asset Controls. Tender no PA/082/2012-13/HQ/C/04. Tanzania: *Author*. (avail online) **https://www.bot.go.tz/Adverts/CallsforTender/en/20200107005645971 36.pdf** (accessed Mar 2021)

52. Internet Authority, (2021). Our Systems and Services. Tanzania: **https://www.ega.go.tz/products-services** (accessed April 21)

53. The United Republic of Tanzania (2019). eGovernment Act no 10 of 2019. Tanzania: The Gazette of the United Republic of Tanzania No 39 Vol 100 20th September 2019. Tanzania: (Available online) **https://www.ega.go.tz/uploads/publications/en-1574849310-eGov%20act,%202019.pdf** (accessed April 21)

54. The United Republic of Tanzania (2015) The Cybercrimes Act 2015. Tanzania: *The Gazette of the United Republic of Tanzania* No 22 Vol 96 22 May 2015. (avail online) **https://www.tcra.go.tz/document/The%20Cybercrimes%20Act,%202015** (accessed Aru 20 and April 21)

55. The United Republic of Tanzania (2010) Electronic and Postal Communications Act No3, 2010. Tanzania: *Author* (Avail Online) Part VI, para 124. **https://www.tcra.go.tz/document/The%20Electronic%20and%20Postal%20Communications%20Act,%202010%20(Act%20No.%203%20out%20of%2010)** (accessed April 21)

56. National Tanzania Computer Emergency Response Team (TZ-CERT) (2021) **https://www.tzcert.go.tz/about-us/** (accessed Aug 20 and Mar 21)

57. Tanzania Communications Regulatory Authority (TCRA) (2021) **https://www.tcra.go.tz/about-tcra/tcra-profile** (accessed Aug 20 and April 21)

58. Tanzania Communications Regulatory Authority (TCRA) (2021) **https://www.tcra.go.tz/about-tcra/tcra-profile** (accessed Aug 20 and April 21)

59. Ministry for Works and Transport (2018), The Electronic and Postal Communications (Computer Emergency Response Team) Regulations 2018. Tanzania: *Author* (avail online) **https://www.tcra.go.tz/document/The%20Electronic%20and%20Postal%20Communications%20(Computer%20Emergency%20Response%20Team)%20Regulations,%202018** (accessed April 2021)

60. Ministry for Works and Transport (2018), The Electronic and Postal Communications (Computer Emergency Response Team) Regulations 2018. Tanzania: *Author* (avail online) **https://www.tcra.go.tz/document/The%20Electronic%20and%20Postal%20Communications%20(Computer%20Emergency%20Response%20Team)%20Regulations,%202018** (accessed April 2021)

61. Ministry for Works and Transport (2018), The Electronic and Postal Communications (Computer Emergency Response Team) Regulations 2018. Tanzania: *Author* (avail online) **https://www.tcra.go.tz/document/The%20Electronic%20and%20Postal%20Communications%20(Computer%20Emergency%20Response%20Team)%20Regulations,%202018** (accessed April 2021)

Appendix F

Endnotes (continued)

62. The United Republic of Tanzania (2019). eGovernment Act no 10 of 2019. Tanzania: *The Gazette of the United Republic of Tanzania* No 39 Vol 100 20th September 2019. Part II Sect 4 p7, Part III Sect 7 p10. Tanzania: (Available online) **https://www.ega.go.tz/uploads/publications/en-1574849310-eGov%20act,%202019.pdf** (accessed April 21)

63. Internet Authority, (2021). Our Systems and Services. Tanzania: **https://www.ega.go.tz/products-services** (accessed April 21)

64. The United Republic of Tanzania (2019). eGovernment Act no 10 of 2019. Tanzania: *The Gazette of the United Republic of Tanzania* No 39 Vol 100 20th September 2019. Tanzania: (Available online) **https://www.ega.go.tz/uploads/publications/en-1574849310-eGov%20act,%202019.pdf** (accessed April 21)

65. The United Republic of Tanzania (2019). eGovernment Act no 10 of 2019. Tanzania: *The Gazette of the United Republic of Tanzania* No 39 Vol 100 20th September 2019. Part II sect 5 p 7-9. Tanzania: (Available online) **https://www.ega.go.tz/uploads/publications/en-1574849310-eGov%20act,%202019.pdf** (accessed April 21)

66. The United Republic of Tanzania (2019). eGovernment Act no 10 of 2019. Tanzania: *The Gazette of the United Republic of Tanzania* No 39 Vol 100 20th September 2019. Tanzania: (Available online) **https://www.ega.go.tz/uploads/publications/en-1574849310-eGov%20act,%202019.pdf** (accessed April 21)

67. Ministry of Finance and Planning (2021). Policy and Strategies. Tanzania: *Author* **http://www.mof.go.tz/index.php/policy/policy-and-strategies** (accessed Mar 21)

68. Tanzanian Police Force (2021). Resources. (Available online) **https://www.polisi.go.tz/resources/** (accessed Aug 20 and April 21)

69. Omar Hayla (2020) Tanzania: Cybercrime Related Cases Drop Drastically – Police. Tanzania: *Tanzania Daily News*. (available online from) **https://allafrica.com/stories/202003170618.html** (accessed April 210)

70. Ministry of Works, Transport and Communications (MWTC) (2016). National Information and Communications Technology Policy (NICP) 2016 – Implementations Strategy 2016/17-2020/21. Tanzania: *Author.* Ch4, 4.1, p26. Available from: **https://www.ictc.go.tz/index.php/component/phocadownload/category/4-policies?download=48:107** (accessed Aug 20 and Mar 21)

71. National Tanzania Computer Emergency Response Team (TZ-CERT) (2021) **https://www.tzcert.go.tz/about-us/** (accessed Aug 20 and Mar 21)

72. Forum of Incident Response and Security Teams (FIRST), 2015-2020, **https://www.first.org/about/mission** (accessed April 2021)

73. Africa CERT, 2020, **https://www.africacert.org/about-us/** (accessed July 2020 and April 21)

74. Ministry for Works and Transport (2018), The Electronic and Postal Communications (Computer Emergency Response Team) Regulations 2018. Tanzania: *Author* (avail online) **https://www.tcra.go.tz/document/The%20Electronic%20and%20Postal%20Communications%20(Computer%20Emergency%20Response%20Team)%20Regulations,%202018** (accessed April 2021)

75. European Union Agency for Network and Information Security (ENISA), 'ENISA CSIRT Maturity Assessment Model', 30 April 2019, *Author.* **https://www.enisa.europa.eu/publications/study-on-csirt-maturity** (Accessed 4 Nov 2020)

76. National Tanzania Computer Emergency Response Team (TZ-CERT) (2021) **https://www.tzcert.go.tz/about-us/** (accessed Aug 20 and Mar 21)

Appendix F

Endnotes (continued)

77. The United Republic of Tanzania (2010) Electronic and Postal Communications Act No3, 2010. Tanzania: *Author* (Avail Online) Part VI, para 124. **https://www.tcra.go.tz/document/The%20Electronic%20and%20Postal%20Communications%20Act,%202010%20(Act%20No.%203%20out%20of%2010)** (accessed April 21)

78. Ministry for Works and Transport (2018), The Electronic and Postal Communications (Computer Emergency Response Team) Regulations 2018. Tanzania: *Author* (avail online) **https://www.tcra.go.tz/document/The%20Electronic%20and%20Postal%20Communications%20(Computer%20Emergency%20Response%20Team)%20Regulations,%202018** (accessed April 2021)

79. Africa CERT, 2020. African Teams. **https://www.africacert.org/african-csirts/** (accessed July 2020 and April 21)

80. Forum of Incident Response and Security Teams (FIRST), (2015-2020). FIRST Teams. **https://www.first.org/members/teams/** (accessed April 2021)

81. European Union Agency for Network and Information Security (ENISA), 'ENISA CSIRT Maturity Assessment Model', 30 April 2019, *Author.* **https://www.enisa.europa.eu/publications/study-on-csirt-maturity** (Accessed 4 Nov 2020)

82. Bank of England and CBEST, CBEST Intelligence Led Testing, Understanding Cyber Threat Intelligence Operations, V2, UK, *Bank of England,* 2016, Para2.2.2 p 9, **https://www.bankofengland.co.uk/-/media/boe/files/financial-stability/financial-sector-continuity/understanding-cyber-threat-intelligence-operations.pdf** (accessed Nov 2020)

83. CREST, 'Accredited Companies Providing Vulnerability Assessment Services', 2020, **https://service-selection-platform.crest-approved.org/accredited_companies/vulnerability_assessment/** (accessed Nov 2020)

84. National Cyber Security Centre (NCSC), "Penetration Testing", UK, Author, 8 Aug 2017, **https://www.ncsc.gov.uk/guidance/penetration-testing** (accessed Nov 2020)

85. CREST, 'Accredited Companies providing Security Operations Centres (SOC)' 2020, *Author*, **https://service-selection-platform.crest-approved.org/accredited_companies/soc/** (accessed Nov 2020)

86. CREST, 'Cyber Security Incident Response Guide V1', 2013, UK, Author, Part 2, p11, **https://www.crest-approved.org/wp-content/uploads/2014/11/CSIR-Procurement-Guide.pdf** (accessed Nov 2020)

87. Information Communication Technologies (ICT) Commission (2021). ICT Professionals About Registration. **https://www.ictc.go.tz/index.php/3/about-registration** (accessed Aug 20 and Mar 21)

88. After School Africa (2016). TCRA ICT Scholarships for Tanzania Students in Tanzania 2016/2017. Nigeria: *Author* (avail online) **https://www.afterschoolafrica.com/4508/tcra-ict-scholarships-for-tanzania-students-in-tanzania/** (accessed Mar 21)

89. Ministry of Education Science and Technology (2016). ICT Training Program. Tanzania: *Author.* (Avail online) **http://www.moe.go.tz/en/project/ict-training-programme** (accessed April 21)

90. Ministry of Education Science and Technology (2016). ICT Training Program. Tanzania: *Author.* (Avail online) **http://www.moe.go.tz/en/project/ict-training-programme** (accessed April 21)

91. Ministry of Education Science and Technology (2016). ICT Training Program. Tanzania: *Author.* (Avail online) **http://www.moe.go.tz/en/project/ict-training-programme** (accessed April 21)

Appendix F

Endnotes (continued)

92. Ministry of Works, Transport and Communications (MWTC) (2016). National Information and Communications Technology Policy (NICP) 2016 – Implementations Strategy 2016/17-2020/21. Tanzania: *Author.* Available from: **https://www.ictc.go.tz/index.php/component/phocadownload/category/4-policies?download=48:107** (accessed Aug 20 and Mar 21)

93. Bank of Tanzania, Supervised Institutions, **https://www.bot.go.tz/BankSupervision/Institutions** (accessed 29 May 20)

94. Tanzania Bankers Association, **http://tanzaniabankers.org/** (accessed 29 May 20)

95. Wikipedia, List of Banks in Tanzania, **https://en.wikipedia.org/wiki/List_of_banks_in_Tanzania** (accessed 29 May 20)

96. Common Vulnerabilities & Exposures (CVE) is a publicly available list of disclosed flaws, each is assigned a unique identification number, **https://cve.mitre.org** (accessed 29 Oct 20)

97. Further information on CVSS available on Wikipedia, **https://en.wikipedia.org/wiki/Common_Vulnerability_Scoring_System** (accessed on 29 Oct 20)

98. Valimail report on DMARC, 2019, **https://www.valimail.com/resources/domain-spoofing-declines-as-protective-measures-grow/** (accessed 30 Oct 2020)

99. Finance Digest Report, 2019, **https://www.financedigest.com/rise-sophisticated-bec-scams-finance-industry** (accessed 30 Oct 2020)

100. FBI Internet Crime Report, 2019, **https://www.ic3.gov/Media/Y2019/PSA190910** (accessed 31 Oct 2020)

101. CREST International, **https://www.crest-approved.org/** (accessed Aug 20)

102. EC Council, **https://www.eccouncil.org/** (accessed Aug 20)

103. ISACA, **https://www.isaca.org/** (accessed Aug 20)

104. (ISC)2, **https://www.isc2.org/** (accessed Aug 20)

105. SANS, **https://www.sans.org/** (accessed Aug 20)

106. CompTIA, **https://www.comptia.org/** (accessed Aug 20)

107. Offensive Security, **https://www.offensive-security.com/** (accessed Aug 20)

108. Cloud Security Alliance, **https://cloudsecurityalliance.org/education/** (accessed Aug 20)

109. PCI, **https://www.pcisecuritystandards.org/program_training_and_qualification/** (accessed Aug 20)

110. Cisco, **https://www.cisco.com/c/en/us/training-events/training-certifications/certifications/security.html** (accessed Aug 20)

111. Microsoft, **https://www.microsoft.com/en-us/learning/browse-all-certifications.aspx** (accessed Aug 20)

112. Amazon Web Services, **https://aws.amazon.com/training/path-security/?nc2=sb_lp_se** (accessed Aug 20)

113. IRCA(ISMS), **https://www.quality.org/** (accessed Aug 20)

114. BCS, **https://www.bcs.org/get-qualified/certifications-for-professionals/information-security-and-ccp-scheme-certifications/** (accessed Aug 20)

115. IET, **https://www.theiet.org/career/professional-registration/ict-technician/** (accessed Aug 20)

Appendix F

Endnotes (continued)

116. Ingham, K, Bryceson, DF, Mascarenhas, AC. and Chiteji, FM. (2021). Tanzania – Introduction and Quick Facts. *Encyclopaedia Britannica.* **https://www.britannica.com/place/Tanzania** (Accessed 1 April 2021)

117. Ingham, K, Bryceson, DF, Mascarenhas, AC. and Chiteji, FM. (2021). Tanzania – Introduction and Quick Facts. *Encyclopaedia Britannica*. **https://www.britannica.com/place/Tanzania** (Accessed 1 April 2021)

118. Ingham, K, Bryceson, DF, Mascarenhas, AC. and Chiteji, FM. (2021). Tanzania – Introduction and Quick Facts. *Encyclopaedia Britannica.* **https://www.britannica.com/place/Tanzania** (Accessed 1 April 2021)

119. The World Bank, (2021). The World Bank in Tanzania – Economic Overview. *Author,* 23 March 2021, **https://www.worldbank.org/en/country/tanzania/overview** (accessed April 2021)

120. Ingham, K, Bryceson, DF, Mascarenhas, AC. and Chiteji, FM. (2021). Tanzania – Resources and Power. *Encyclopaedia Britannica.* **https://www.britannica.com/place/Tanzania** (Accessed 1 April 2021)

121. Ingham, K, Bryceson, DF, Mascarenhas, AC. and Chiteji, FM. (2021). Tanzania – Resources and Power. *Encyclopaedia Britannica.* **https://www.britannica.com/place/Tanzania** (Accessed 1 April 2021)

122. World Population Review (2021) Tanzania Population 2021. *Author.* (avail from) **https://worldpopulationreview.com/countries/tanzania-population** (accessed April 2021)

123. World Population Review (2021) Tanzania Population 2021. *Author.* (avail from) **https://worldpopulationreview.com/countries/tanzania-population** (accessed April 2021)

124. Serianu, (2017). Africa Cyber Security Report 2017 - Demystifying Africa's Cyber Security Poverty Line – Key Highlights. Kenya, *Author*. p11 **https://www.serianu.com/downloads/AfricaCyberSecurityReport2017.pdf** (Accessed April 2021)

125. Ingham, K, Bryceson, DF, Mascarenhas, AC. and Chiteji, FM. (2021). Tanzania – Introduction and Quick Facts. *Encyclopaedia Britannica*. **https://www.britannica.com/place/Tanzania** (Accessed 1 April 2021)

126. The World Bank, (2021). The World Bank in Tanzania – Economic Overview. *Author*, 23 March 2021, **https://www.worldbank.org/en/country/tanzania/overview** (accessed April 2021)

127. The United Republic of Tanzania Planning Commission (no date). The Tanzania Development Vision 2025. Tanzania: *Ministry of Finance and Planning*. Avail from: **http://www.mof.go.tz/mofdocs/overarch/vision2025.htm#1.0%20DEVELOPMENT%20VISION** (accessed April 21)

128. The World Bank, (2021). The World Bank in Tanzania – Economic Overview. *Author*, 23 March 2021, **https://www.worldbank.org/en/country/tanzania/overview** (accessed April 2021)

129. The World Bank, (2021). The World Bank in Tanzania – Economic Overview. *Author*, 23 March 2021, **https://www.worldbank.org/en/country/tanzania/overview** (accessed April 2021)

130. Serianu, (2017). Africa Cyber Security Report 2017 - Demystifying Africa's Cyber Security Poverty Line – Key Highlights. Kenya, *Author*. p11 **https://www.serianu.com/downloads/AfricaCyberSecurityReport2017.pdf** (Accessed April 2021)

131. Ministry of Finance and Planning (2018). Implementation Strategy for the National Five-Year Development Plan 2016/17-2020/21 Volume 1 The Action Plan. Ch 2.3.6.1 p 48. Tanzania: *Author.* **http://www.mof.go.tz/docs/The%20Action%20Plan%20of%20Implementation%20of%20the%202nd%20FYDP.pdf** (accessed Mar 21)

132. Ministry of Finance and Planning (2018). Implementation Strategy for the National Five-Year Development Plan 2016/17-2020/21 Volume 1 The **Action Plan. Ch 2.3.6.1 p 48. Tanzania: Author. http://www.mof.go.tz/docs/The%20Action%20Plan%20of%20Implementation%20of%20the%202nd%20FYDP.pdf** (accessed Mar 21)

Appendix F

Endnotes (continued)

133. Serianu, (2017). Africa Cyber Security Report 2017 - Demystifying Africa's Cyber Security Poverty Line – Key Highlights. Kenya, *Author.* p11 **https://www.serianu.com/downloads/AfricaCyberSecurityReport2017.pdf** (Accessed April 2021)

134. The World Bank, (2021). The World Bank in Tanzania – Economic Overview. *Author*, 23 March 2021, **https://www.worldbank.org/en/country/tanzania/overview** (accessed April 2021)

135. African Centre for Media Excellent (ACME) (2019). Tanzania's 'worrying decline of media freedom'. Uganda: *Author* (available from) **https://acme-ug.org/2019/08/19/tanzanias-worrying-decline-of-media-freedom/** (accessed April 2021)

136. African Centre for Media Excellent (ACME) (2019). Tanzania. Uganda: (available from) **https://acme-ug.org/?s=Tanzania** (accessed April 2021)

137. CIPESA Writer (2020). Tanzania Tramples Digital Rights in Fight Against Covid-19. Uganda: *Collaboration on International ICT Policy in East and Southern Africa (CIPESA)*. (available from) **https://cipesa.org/2020/10/tanzania-tramples-digital-rights-in-fight-against-covid-19-as-elections-loom/** (accessed April 2021)

138. CIPESA Writer (2020). Tanzania Tramples Digital Rights in Fight Against Covid-19. Uganda: *Collaboration on International ICT Policy in East and Southern Africa (CIPESA)*. (available from) **https://cipesa.org/2020/10/tanzania-tramples-digital-rights-in-fight-against-covid-19-as-elections-loom/** (accessed April 2021)

139. CIPESA (2019). UN Human Rights Council Called to Address Deterioration of Freedoms in Tanzania. Uganda: *Author* (available from) **https://cipesa.org/2019/05/un-human-rights-council-called-to-address-deterioration-of-freedoms-in-tanzania/** (accessed April 2021)

140. The Guardian Reporter (2017). Tanzania targeted by Huge Global Cybercrime Attack. Tanzania: *IPP Media*. (available from) **https://www.ippmedia.com/en/news/tanzania-targeted-huge-global-cyber-crime-attack** (accessed April 2021)

141. Hare Harry, (2007). SURVEY OF ICT AND EDUCATION IN AFRICA: Tanzania Country Report - ICT in Education in Tanzania. Info Dev.org: (available from) **https://www.infodev.org/infodev-files/resource/InfodevDocuments_432.pdf** (accessed April 2021)

142. Hare Harry, (2007). SURVEY OF ICT AND EDUCATION IN AFRICA: Tanzania Country Report - ICT in Education in Tanzania. Info Dev.org: (available from) **https://www.infodev.org/infodev-files/resource/InfodevDocuments_432.pdf** (accessed April 2021)

143. Global Cyber Security Capacity Centre, (2021). CMM Reviews Around the World. Oxford. **https://gcscc.ox.ac.uk/cmm-reviews#/** (accessed 1 April 2021)