Ministry of ICT, Postal and Courier Services

NATIONAL CYBER SECURITY STRATEGY (NCSS) DRAFT 1.0

2025-2030

Table of Contents

List of Abbreviations

CI	Critical Infrastructure
CII	Critical Information Infrastructure
C IIP	Critical Information Infrastructure Protection Government of Zimbabwe
CSL	Cyber Security Landscape (CSL)
CTL	Cyber Threat Landscape (CTL)
NCSIG	National Cyber Security Institutions and Governance (NCSIG)
NCSCT	National Cybersecurity Strategy Coordination Taskforce (NCSCT)
CSMIC	Minister’s responsible Cyber security and monitoring of interception communication centre (CSMIC)
CSC	Cyber Security Committee (CSC)
CSD	Cyber Security Directorate (CSD)
DPA	Data Protection Authority (DPA)
ZICOP	Zimbabwe Child Online Protection Committee (ZICOP)
ZISAC	Zimbabwe Information Sharing and Analysis Centre (ZISAC)
NSOC	National Network Security Centre (NSOC)
ZIM-CIRT	Computer Incident Response Team (ZIM-CIRT)

PRESIDENT’S REMARKS

PRESIDENT ‘S REMARKS

MINISTER’S REMARKS

Minister’s Remarks

PART 1

Introduction

Vision, Mission and Objectives for Cyber Security

1.1 INTRODUCTION

Working towards attainment of **'Vision 2030'** in an era where digital transformation is rapidly reshaping economies and societies, the need for robust cyber security measures has never been more critical. Zimbabwe, as a participant in the global digital landscape, recognizes the imperative to safeguard its information infrastructure, protect its citizens, and ensure the integrity of national systems against an ever-evolving array of cyber threats.

In contrast to land, air, sea and space, cyberspace poses the following unique difficulties: First, due to the global reach of ubiquitous networks, threat actors can launch distressing attacks far from victims and often in jurisdictions with weak laws and/or no enforcement. Second, fast connection speeds give victims little time to defend against attacks. Thus, at best, States and organisations only know about an attack when it is in process. At worst, victims do not discover the compromise of their critical systems. Third, whereas States pursue national interests through a rules-based international system, cyberspace does not have accepted norms and principles of proportionality. Indeed, whilst a country typically requires the approval of the United Nations to participate in the activities of the community of nations, any actor can setup in cyberspace and do whatever they please. Actors such organised criminals, insurgents and terrorists do not worry about norms and do not fear retaliation mainly due to the difficulty of attributing an attack to a given actor. The lack of accepted norms in cyberspace is reducing confidence in the use of ICTs (ITU, 2011)

The National Cyber Security Strategy (NCSS) for Zimbabwe serves as a comprehensive framework aimed at enhancing the country's cyber resilience. It outlines a proactive approach to identify, prevent, and respond to cyber incidents while fostering a culture of cyber awareness among citizens and organizations alike. By aligning with international best practices and standards, this strategy not only seeks to protect national interests but also to promote confidence in the digital economy, thereby facilitating economic growth and development.

This strategy emphasizes collaboration among government agencies, private sector stakeholders, and civil society to create a unified front against cyber threats. It aims to establish clear roles and responsibilities, enhance capacity building, and promote information sharing to strengthen the national cyber security posture. In doing so, Zimbabwe will strive to create a secure and resilient digital environment that empowers its citizens and businesses to thrive in the digital age.

As we embark on this critical journey, the NCSS will serve as a guiding beacon, driving efforts to protect our nation's digital assets and ensuring a secure future
for all Zimbabweans to and beyond **'Vision 2030'.**

1.2 VISION, MISSION AND OBJECTIVES OF NCSS

1.2.1 Vision:

A secure and resilient cyberspace that fosters trust and innovation.

1.2.2 Mission:

To protect national interests, enhance cybersecurity awareness, and promote stakeholder collaboration.

1.2.3 Objectives

a. Strengthen the cybersecurity framework and governance.
b. Enhance the capacity of institutions and individuals to respond to cyber threats.
c. Promote public-private partnerships in cybersecurity.
d. Foster cybersecurity awareness and education.
e. Develop incident response capabilities.
f. Promote innovation in the field of cyber security Improve the nations cyber resilience and risk management posture.

1.3 BACKGROUND

The rapid advancement of technology has ushered in a new era of connectivity and digital innovation across the globe, including Zimbabwe. As the nation embraces digital transformation, the integration of technology into various sectors such as finance, healthcare, education, and governance has become increasingly pronounced. However, with these advancements come significant risks and challenges posed by cyber threats that can undermine national security, economic stability, and public safety. Zimbabwe has witnessed a growing incidence of cyber-related incidents, including data breaches, ransomware attacks, and phishing schemes, which have highlighted vulnerabilities in its cyber landscape. The increasing reliance on digital platforms for both governmental and private sector operations necessitates a strategic response to mitigate these risks.

Recognizing the potential impact of cyber threats on its development goals, the government of Zimbabwe has prioritized the establishment of a comprehensive cyber security framework. In recent years, various initiatives have been undertaken to enhance national cyber security capabilities, including the formation of specialized cyber security units, the development of legal frameworks, and participation in international cyber security collaborations. However, the fragmented nature of these efforts underscores the need for a cohesive National Cyber Security Strategy that aligns resources, policies, and stakeholders towards a unified goal.

The enactment of the Cyber and Data Protection Act [Chapter 12:07] in 2021 marked a significant legislative milestone, underscoring the nation's commitment to fostering a secure and resilient digital ecosystem. The Act establishes a comprehensive framework for data protection, addressing the growing concerns of privacy and cyber threats. With that in mind and taking into consideration our capabilities, needs, threats and national values as the basis of this strategy. We take heed of ITU’s perspective that culture and national interests shape risk perception and the success of cyber defences. Our strategy is based on national values to ensure maximum buy-in from all stakeholders.

The National Cyber Security Strategy for Zimbabwe aims to address these challenges by providing a structured approach to enhance the nation's cyber resilience. It seeks to create a secure digital environment that fosters innovation, protects critical infrastructure, and safeguards the rights of citizens in the digital space. By establishing clear objectives, promoting public-private partnerships, and encouraging awareness and education on cyber security issues, this strategy will lay the foundation for a safer and more secure cyber ecosystem in Zimbabwe.

Ultimately, the strategy is not only a response to the current cyber threat landscape but also a proactive measure to position Zimbabwe as a competitive player in the global digital economy. Through concerted efforts and collaboration, Zimbabwe aims to build a robust cyber security framework that protects its national interests and promotes sustainable growth in the digital age.

1.4 RATIONALE

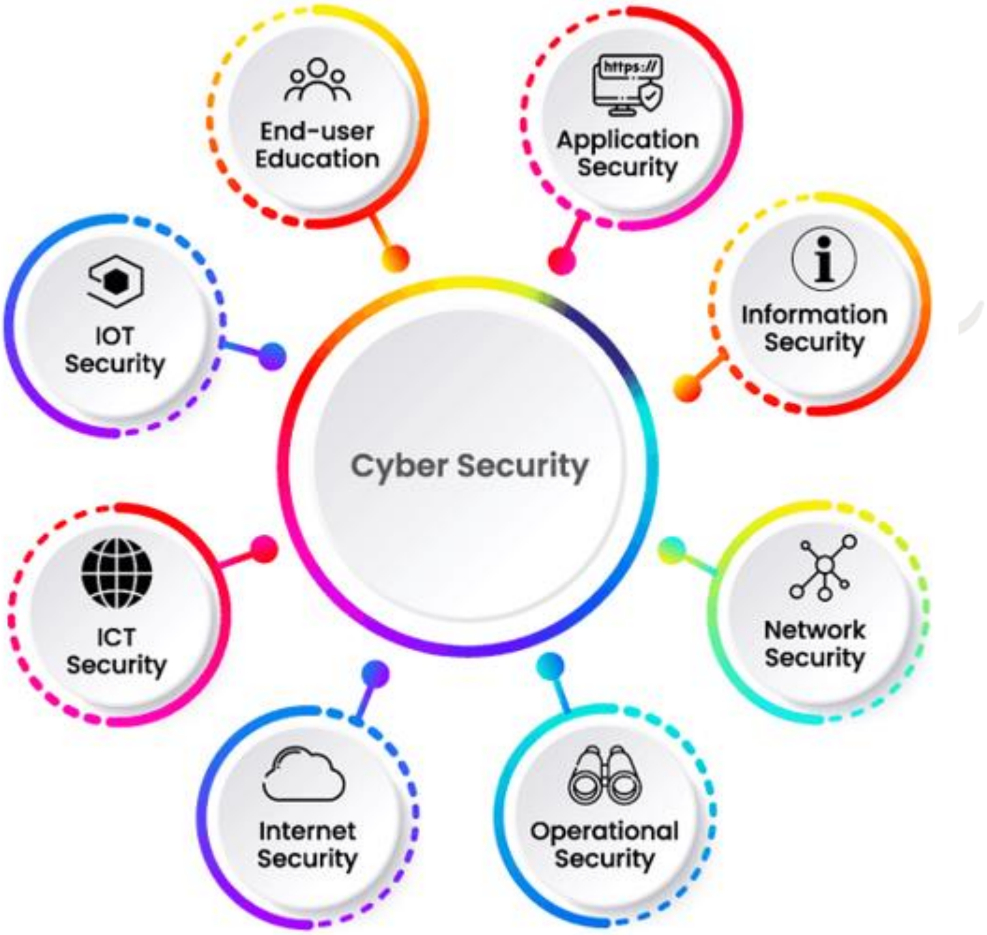
The Republic of Zimbabwe identifies cybersecurity as a national economic and security challenge. The most prevalent cybersecurity challenges in Zimbabwe include exploitation of the new operating environment by adversaries to conduct war like activities such as disruption of operations of critical infrastructure. Most ICT infrastructure and users in the Republic of Zimbabwe have prioritized efficiency, cost and convenience and overlooked security during development and implementation. As many organisation join the automation train, data safety has taken centre stage. Interconnected ICTs have inherent vendor/manufacturer vulnerabilities that can be exploited by adversaries and expose the Zimbabwean citizens, businesses and government to global threats. Despite a growing number of incidents, governance of cyberspace has remained uncoordinated with no clear structure.

Cyber resilience and compliance issues have been growing and need deliberate attention. While Zimbabwe has enacted some laws and formulated policies, there remains need for regular review in order to effectively address emerging risks and threats.

Additionally, cybersecurity awareness of citizens is evolving with changes of the threat landscape thus increasing susceptibility to cyber threats. On the other hand, Zimbabwe increasingly continues to face cybersecurity threats leveraging on the above-mentioned challenges. There have been instances where the notorious threat actors and corporate entities have used cyber espionage to gain access to sensitive/classified data for financial gain, political reasons and to gain competitive advantage.

Furthermore, as ICTs become more interconnected, systems become susceptible to sabotage through deliberate and malicious acts that may disrupt normal processes and functions or destroy/damage equipment and information. Similarly, cyber subversion through propaganda, fake news and misinformation may undermine trust in the government, authority and competence of leaders thus posing a threat to Zimbabwe’s stability.

In addition, terror groups continue to leverage on ICTs (virtual private networks, internet, global applications, social media platforms and websites) for recruitment, radicalization, incitement, financing, training, planning and execution of attacks. Also, there has been an increase in cyber fraud cases through banking/finance, sim swaps and online scams such as digital Ponzi schemes, job scams, fake websites & lotteries, crypto and forex scams, hawala and chop chop schemes among others



Cybersecurity domains (includes these/but not limited)

1.5 CYBER SECURITY AND THREAT LANDSCAPE IN ZIMBABWE

The cyber security landscape in Zimbabwe is shaped by a combination of technological advancements, regulatory frameworks, and emerging threats. Understanding this landscape requires an examination of key components such as the current threat environment, institutional responses, challenges faced, and opportunities for improvement. Zimbabwe as any other connected country has seen an increase in cyber threats, including data breaches, ransomware attacks, and phishing scams. The shift towards digital services, especially during the COVID-19 pandemic, has made organizations more vulnerable to these attacks. Critical sectors such as finance, healthcare, and government are primary targets due to the sensitive data they handle.

The financial sector, in particular, has reported incidents of fraud and cyber attacks that threaten consumer trust and financial stability. Criminals and Employees with access to sensitive information pose a risk, whether intentionally or through negligence. This highlights the need for robust internal security measures and training programs. Cyber threat actors are on rise as the threat landscape is increasing. Cybercriminals seeking financial gain through illegal activities like ransomware and fraud have been identified and prosecuted in the country. Hacktivists using hacking to promote political or social causes, terrorists, script-kiddies and organized crime groups coordinating cyber crimes as part of broader criminal enterprises and state-sponsored actors are issues the country is dealing with as any other county. Understanding these diverse actors is crucial for developing effective cyber defense strategies.

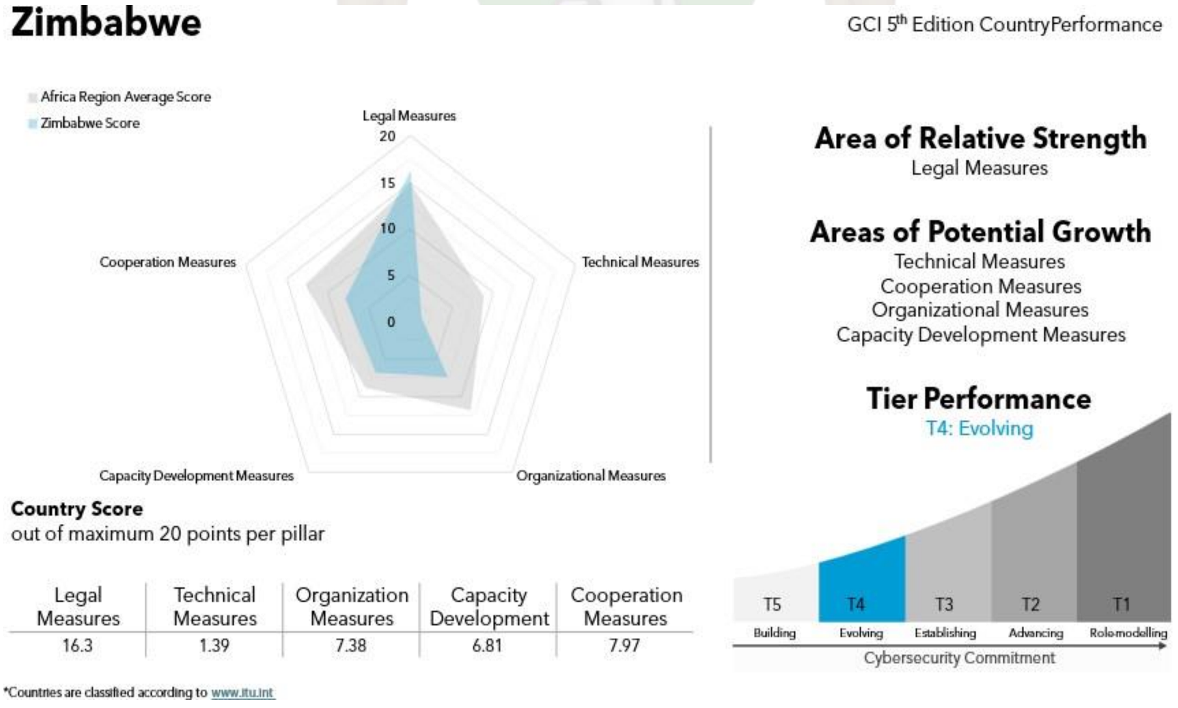
The enactment of the Cyber Security and Data Protection Act in 2021 marked a significant step towards establishing a legal framework for cyber security in Zimbabwe. This Act provides mechanisms for data protection, incident response, and the prosecution of cyber offenses. The Act also aims to foster collaboration between government, private sector, and civil society.

Despite the establishment of some cybersecurity institutions, a fragmented approach to cyber security exists, with varying levels of engagement and capacity among different sectors and stakeholders. Efforts to raise awareness about cyber security risks among citizens and businesses are being implemented, though more extensive campaigns are needed to ensure widespread understanding and preparedness. Many organizations, especially in the public sector, face budget constraints that hinder their ability to invest in comprehensive cyber security measures, personnel training, and technology upgrades. There is a shortage of skilled professionals in the field of cyber security in Zimbabwe, making it challenging to build capable teams to manage and mitigate cyber threats effectively.

The rapid evolution of cyber threats requires continuous adaptation and updating of strategies, which can be difficult for organizations to manage effectively. There is an opportunity to invest in training and capacity-building programs to develop a skilled workforce in cyber security. Collaboration with educational institutions and international organizations can facilitate this process. Strengthening collaboration between the government and the private sector can lead to more effective information sharing, joint initiatives, and resource pooling to combat cyber threats. Zimbabwe can benefit from adopting international best practices and standards in cyber security, which can help organizations enhance their security postures and resilience against threats. Promoting basic cyber hygiene practices among individuals and organizations can significantly reduce vulnerabilities. This includes training on recognizing phishing attempts, securing passwords, and maintaining software updates.

Zimbabwe's cyber security landscape is characterized by both significant challenges and opportunities. While the country faces a growing array of cyber threats, the establishment of a legal framework and dedicated institutions marks progress in addressing these issues. Continued efforts to enhance capacity, promote collaboration, and raise awareness will be essential for building a robust cyber security posture that can protect the nation's digital assets and ensure a secure environment for all citizens.

According to the ITU 2024 Global Cyber Security Index Zimbabwe is in 'Tier 4 (T4) Evolving' representing countries that obtained an overall score of at least 20/100 by demonstrating a basic cybersecurity commitment to government-driven actions that encompass evaluating, establishing, or implementing certain generally accepted cybersecurity measures in at least one pillar or several indicators and/or sub-indicators.



Zimbabwe

GCI 5th Edition CountryPerformance

Area of Relative Strength

Legal Measures

Areas of Potential Growth

Technical Measures
Cooperation Measures
Organizational Measures
Capacity Development Measures

Tier Performance

T4: Evolving

Country Score
out of maximum 20 points per pillar

Legal Measures	Technical Measures	Organization Measures	Capacity Development	Cooperation Measures
16.3	1.39	7.38	6.81	7.97

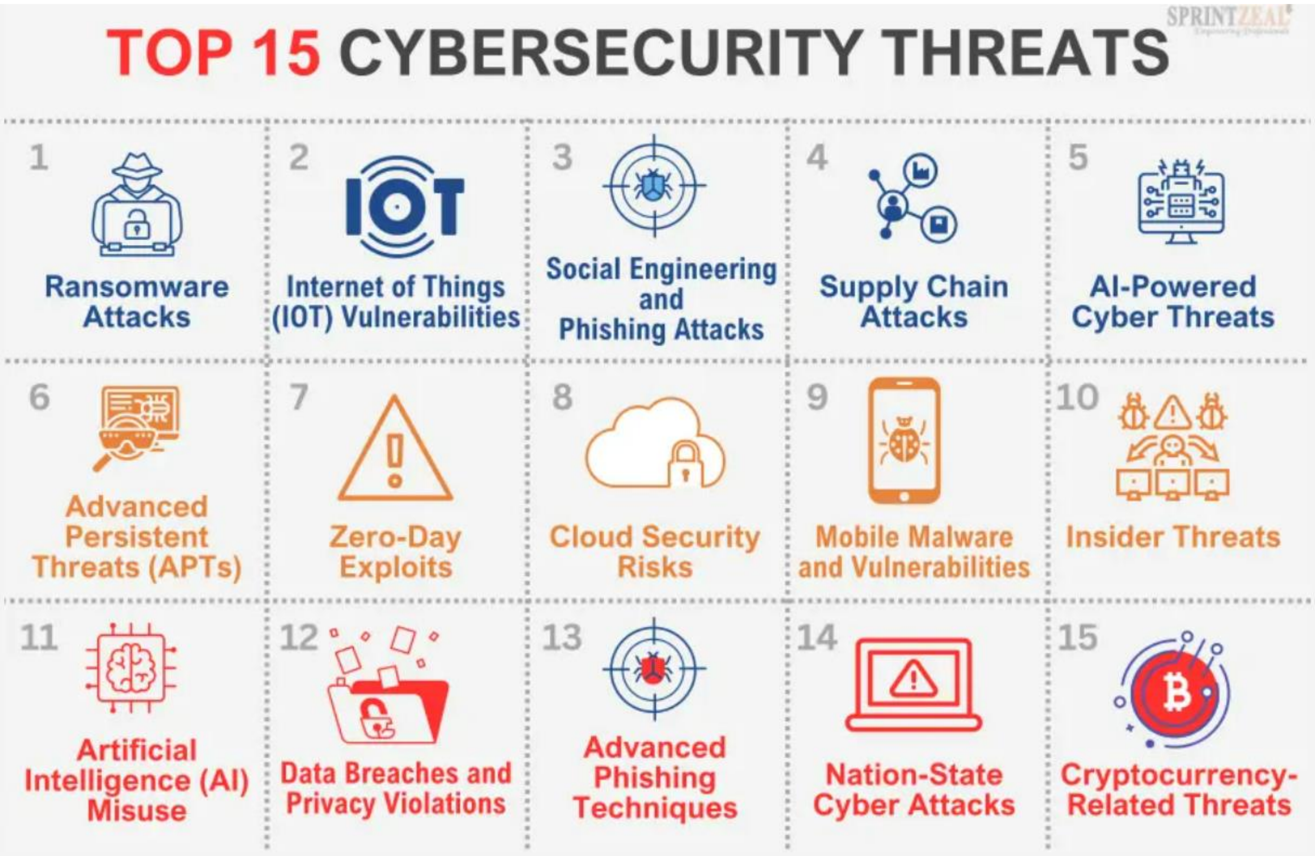
*Countries are classified according to www.itu.int

Source: ITU Global Cybersecurity Index 2024

> “In contrast to land, air, sea and space, cyberspace poses unique difficulties...”

ITU 2011

Top 15 Cyber Threats of 2024



TOP 15 CYBERSECURITY THREATS

1 Ransomware Attacks

2 Internet of Things (IOT) Vulnerabilities

3 Social Engineering and Phishing Attacks

4 Supply Chain Attacks

5 AI-Powered Cyber Threats

6 Advanced Persistent Threats (APTs)

7 Zero-Day Exploits

8 Cloud Security Risks

9 Mobile Malware and Vulnerabilities

10 Insider Threats

11 Artificial Intelligence (AI) Misuse

12 Data Breaches and Privacy Violations

13 Advanced Phishing Techniques

14 Nation-State Cyber Attacks

15 Cryptocurrency-Related Threats

Source: https://www.sprintzeal.com/blog/top-cybersecurity-threats

PART 2

Cyber Security Principles, Norms & Pillars

“Nyika Inovakwa Nevene vayo, Ilizwe Lakhiwa Ngabanikazi Balo”.

H.E. Cde Dr E.D. Mnangagwa

2.1 GUIDING PRINCIPLES:

We adopt and domesticate the international principles:

a. Principle of Constitutionality and Legality – Actions undertaken in order to enhance cyber security must be based on the provisions provided for in the Constitution of the Republic of Zimbabwe, legislation in force and international agreements.

b. Principle of National Security – Cyber security is an integral part of national security, it supports the functioning of the state and society, the competitiveness of the economy and innovation. This principle means ensuring the right to security and protection for all citizens through cybercrime prevention.

c. Principle of Subsidiarity – Because of the diverse ownership and operation of various ICT systems, the State cannot assume sole responsibility for protecting cyberspace and the rights of citizens online. The owners and operators of information and communication technology are primarily responsible for protecting their systems and the information of their customers.

d. Principle of Holistic Approach - It is crucial to develop a holistic approach to face threats in cyberspace,

e. Principle of Public and Private Partnership - Cyber security is ensured in a coordinated manner through cooperation between the public and private sectors, taking into account the interconnectedness and interdependence of existing infrastructure and services in cyberspace.

f. Principle of Continuity – Activities should be seen as part of a continuous strategy. This is especially important because administrative/procedural and time limits will be imposed, and because different initiatives and activities will need to be linked with actions that will continue for several years.

g. Principle of Confidentiality - Institutions with responsibility to prevent and combat cybercrime should seek to establish trust in protecting investigation, data and information integrity from misuse by those with access to them.

h. Principle of Human Rights and Freedoms - Cyber security is guaranteed by respecting fundamental rights and freedoms as well as by protecting individual liberties, personal information, and identity regardless of ethnicity, gender, age, religion throughout all stages.

i. Principle of International Cooperation - Cyber security is enhanced via international cooperation with international partners and allies. Through cooperation, Zimbabwe will play a substantial role in promoting global cyber security and at the same time enhancing its own competences.

2.2 GUIDING NORMS

We adopt and domesticate the following international norms:

a. **Responsible State Behavior**: - State and non state players should act responsibly in cyberspace, refraining from attacks on critical infrastructure.

b. **Human Rights Protection**: - Respect for human rights and privacy should be upheld online as they are offline.

c. **Non-Interference**: - State to refrain from interference with the internal affairs of other states through cyber means.

d. **Cooperation and Assistance**: Collaboration between states and other stakeholders is crucial for tackling cyber threats effectively.

e. **Transparency and Confidence-Building**: Sharing information about cybersecurity policies and incidents can build trust and reduce misunderstandings.

f. **Accountability**: Actors in cyberspace should be held accountable for their actions, with appropriate legal frameworks in place.

g. **Capacity Building**: Strengthening the cybersecurity capabilities of all countries, especially developing ones, is essential for global security.

h. **Protection of Critical Infrastructure**: Measures should be taken to protect essential services and infrastructures from cyber attacks.

2.3 FIVE (5) PILLARS OF THE ITU GLOBAL CYBERSECURITY AGENDA (GCA)

We adopt and domesticate the ITU Pillars:

a. Pillar 1 - Legal Measures Strategy

This Pillar seeks to elaborate strategies for the development of model globally applicable and interoperable cybercrime legislation. The overall goal of the Pillar is to develop advice and internationally compatible processes for handling crime committed over ICTs. Zimbabwe needs to strengthen their capacity to regulate cyberspace. The executive, law enforcement, the judiciary, the private sector, and other stakeholders must support and follow national laws. Due to transnational nature of cyber threats, Global harmonisation is important because gaps in national legislation abet cybercrime.

b. Pillar 2 – Technical and Procedural Measures

This Pillar focuses on measures for addressing vulnerabilities in software products. The pillar aims to devise globally acceptable accreditation schemes, protocols and standards.

c. Pillar 3 – Organizational Structures

The Pillar aims to create organisational structures and strategies to help prevent, detect and respond to attacks against critical information infrastructures.

d. Pillar 4 – Capacity Building

This Pillar seeks to elaborate strategies for enhancing knowledge and expertise to boost cybersecurity on the national policy agenda.

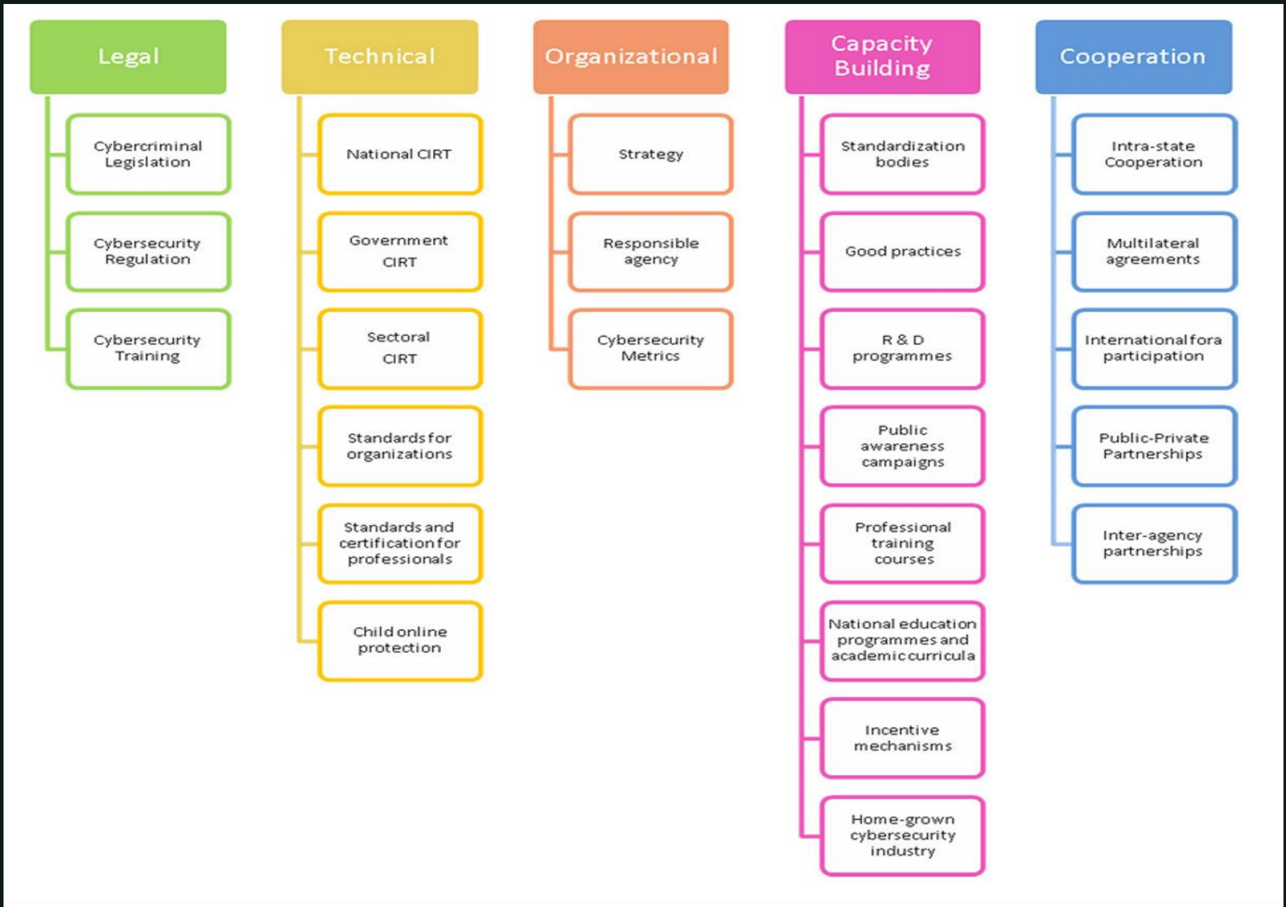
e. Pillar 5 – International Cooperation

The Pillar focuses on strategies for international cooperation, dialogue and coordination

Legal
Technical
Organizational
Capacity development
Cooperation

FIVE (5) PILLARS OF THE ITU GLOBAL CYBERSECURITY AGENDA (GCA)

FIVE (5) PILLARS OF THE ITU GLOBAL CYBERSECURITY AGENDA (GCA)



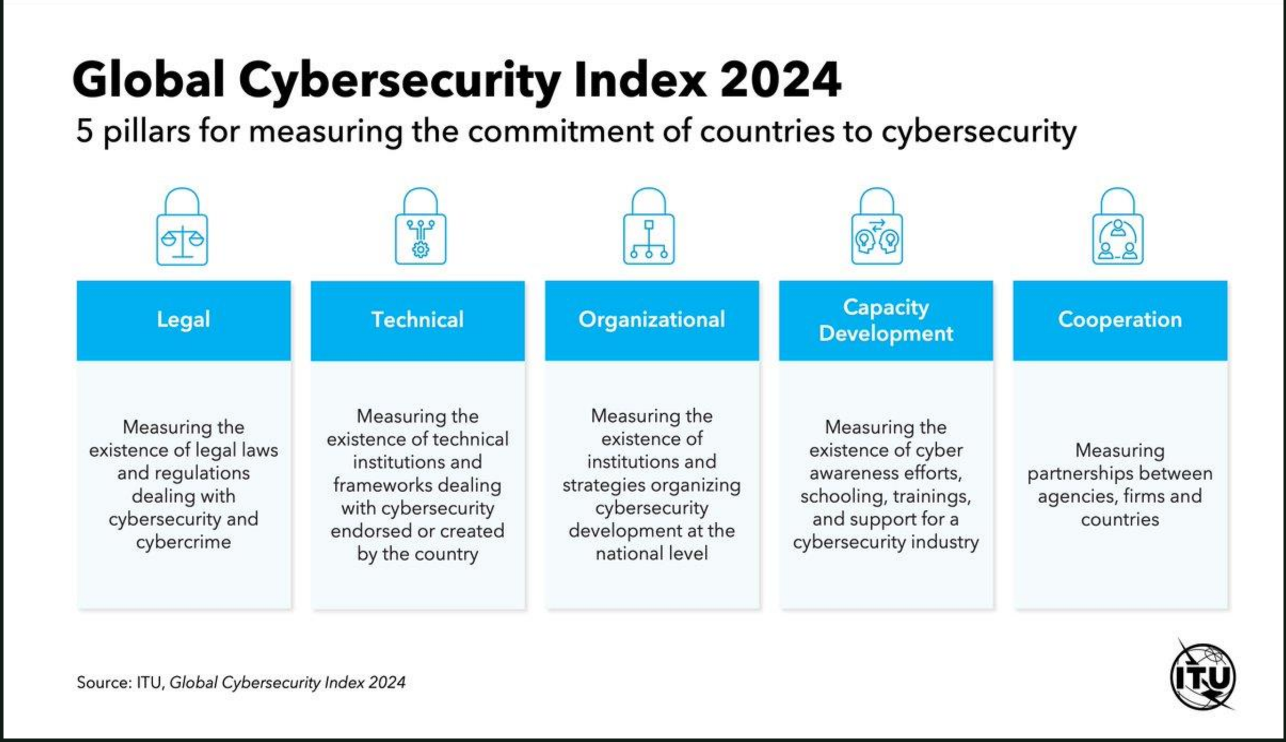
Legal
- Cybercriminal Legislation
- Cybersecurity Regulation
- Cybersecurity Training

Technical
- National CIRT
- Government CIRT
- Sectoral CIRT
- Standards for organizations
- Standards and certification for professionals
- Child online protection

Organizational
- Strategy
- Responsible agency
- Cybersecurity Metrics

Capacity Building
- Standardization bodies
- Good practices
- R & D programmes
- Public awareness campaigns
- Professional training courses
- National education programmes and academic curricula
- Incentive mechanisms
- Home-grown cybersecurity industry

Cooperation
- Intra-state Cooperation
- Multilateral agreements
- International fora participation
- Public-Private Partnerships
- Inter-agency partnerships



Global Cybersecurity Index 2024

5 pillars for measuring the commitment of countries to cybersecurity

Legal	Technical	Organizational	Capacity Development	Cooperation
Measuring the existence of legal laws and regulations dealing with cybersecurity and cybercrime	Measuring the existence of technical institutions and frameworks dealing with cybersecurity endorsed or created by the country	Measuring the existence of institutions and strategies organizing cybersecurity development at the national level	Measuring the existence of cyber awareness efforts, schooling, trainings, and support for a cybersecurity industry	Measuring partnerships between agencies, firms and countries

Source: ITU, *Global Cybersecurity Index 2024*

PART 3

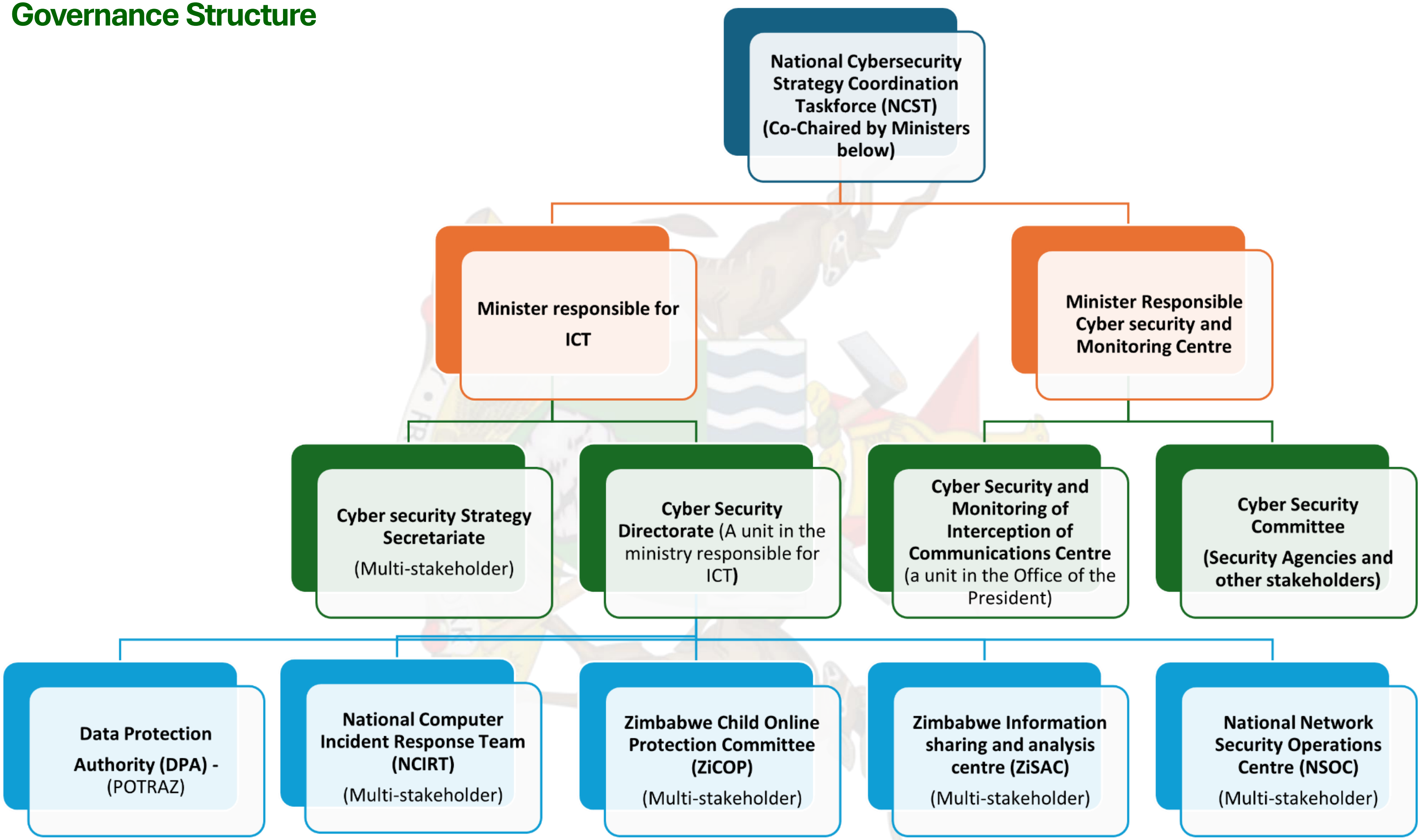
National Cyber Security Institutional and Governance Framework

3.1 NATIONAL CYBER SECURITY INSTITUTIONAL FRAMEWORK

Securing Zimbabwe’s national information assets requires an adequate and comprehensive governance structure for effective focus and coordination of national cyber security initiatives. It is necessary therefore to establish an efficient coordination mechanism for effective cyber security and resilience.

In line with Zimbabwe current laws, best practices and ITU National Cybersecurity Strategy Guide and the, the following governance structure will be utilised:

National Cyber Security Governance Structure


National Cybersecurity Strategy Coordination Taskforce (NCST) (Co-Chaired by Ministers below)
Minister responsible for ICT
Minister Responsible Cyber security and Monitoring Centre
Cyber security Strategy Secretariate (Multi-stakeholder)
Cyber Security Directorate (A unit in the ministry responsible for ICT)
Cyber Security and Monitoring of Interception of Communications Centre (a unit in the Office of the President)
Cyber Security Committee (Security Agencies and other stakeholders)
Data Protection Authority (DPA) - (POTRAZ)
National Computer Incident Response Team (NCIRT) (Multi-stakeholder)
Zimbabwe Child Online Protection Committee (ZiCOP) (Multi-stakeholder)
Zimbabwe Information sharing and analysis centre (ZiSAC) (Multi-stakeholder)
National Network Security Operations Centre (NSOC) (Multi-stakeholder)

3.2 INSTITUTIONS AND GOVERNANCE FROM STRACTURE ABOVE

1. National Cybersecurity Strategy Coordination Taskforce (NCST):
2. Minster responsible for ICT and Minister Responsible Cyber Security and Monitoring
3. Centre Cyber Security and Monitoring of Interception of Communications Centre (a unit in the Office of the President)
4. Cyber Security Committee (CSC)
5. Cyber Security Directorate (A unit in the ministry responsible for ICT)
6. Data Protection Authority (DPA) - POTRAZ
7. National Computer Incident Response Team (NCIRT)
8. Zimbabwe Child Online Protection Committee (ZiCOP)
9. Zimbabwe Information sharing and analysis centre (ZiSAC)
10. National Network Security Operations Centre (NSOC)
11. Stakeholders
12. Cyber Security National secretariate

3.3 NATIONAL CYBERSECURITY STRATEGY COORDINATION TASKFORCE (NCST)

Establish **National Cybersecurity Strategy Coordination Taskforce (NCST):**

A high-level taskforce for:

a. Cyber Security Coordination: The NCST coordinates the activities of various stakeholder and/or institutions for effective and efficient strategy and operations.

b. Crisis Management: It plays a crucial role in managing national cyber related and other emergencies, by coordinating responses and deploying resources as needed.

c. Risk Management: The NCST is involved in information sharing, gathering and analyzing cyberthreat to identify potential threats to national security and advise stakeholders on appropriate actions.

d. Strategic Planning: It is responsible for developing and implementing strategic plans related to cyber defense and security, ensuring the country's preparedness against internal and external threats.

e. Advisory Role: The NCST advises the President and other senior government officials on security matters, helping to shape national cyber defense policies and strategies.

f. Operational Oversight: Oversee implementation and monitoring and evaluation of the cyber security strategy, ensuring they are conducted efficiently and in alignment with national objectives.

g. Resource Mobilization: Mobilize financial and human resource for cyber security

3.3.1. MEMBERSHIP – 14 MEMBERS AS FOLLOWS:

- Minister responsible for ICT and Minister Responsible Cyber Security and Monitoring of Interception of Communications Centre (CSMIC) (Co-chairs):

i. 2 members from Cyber security committee (established under Cyber and Data Protection Act) (CSC Chair and Vice Chair)

ii. Ministry of Finance (Permsec)

iii. Consumer APEX board (Head)

iv. 2 representatives of Private Sector

v. Ministry of ICTPCS (Permsec)

vi. Attorney General

vii. Public Service Commission – (Permsec)

viii. Cyber security directorate head (Min of ICT) and CSMIC head as Ex-Officio(s) (Technical Advisors)

iix. Civil society – Head of Zimbabwe Association of NGOs

ix. Academia – Head of Association of VCs

3.4 MINSTER RESPONSIBLE FOR ICT AND MINISTER RESPONSIBLE CYBER SECURITY AND MONITORING OF INTERCEPTION OF COMMUNICATIONS CENTRE

Role and responsibilities

i. Link between cyber security stakeholders and the Office of the President and Cabinet.

ii. Co-chair the NCST

iii. Perform roles and responsibilities as per Cyber and Data Protection Act.

3.5 CYBER SECURITY AND MONITORING OF INTERCEPTION OF COMMUNICATIONS CENTRE (A UNIT IN THE OFFICE OF THE PRESIDENT)

The functions of the Cyber Security and Monitoring Centre shall be to—

(a) be the sole facility through which authorised interceptions shall be effected;

(b) advise Government and implement Government policy on cybercrime and cyber security;

(c) identify areas for intervention to prevent cybercrime;

(d) coordinate cyber security and establish a national contact point available daily around-the-clock;

(e) establish and operate a protection-assured whistle-blower system that will enable members of the public to confidentially report to the Committee cases of alleged cybercrime;

(f) promote and coordinate activities focused on improving cyber security and preventing cybercrime by all interested parties in the public and private sectors;

(g) provide guidelines to public and private sector interested parties on matters relating to awareness, training, enhancement, investigation, prosecution and combating cybercrime and managing cyber security threats;

(h) oversee the enforcement of the Cyber and Data Protection Act to ensure that it is enforced reasonably and with due regard to fundamental human rights and freedoms;

(i) provide technical and policy advice to the responsible Minister;

(j) advise the responsible Minister on the establishment and development of a comprehensive legal framework governing cyber security matters.

3.6 CYBER SECURITY COMMITTEE

(1) There is hereby established a committee to be known as the Cyber Security Committee which shall be an ad hoc advisory body to the Minister responsible for CSMIC.

(2) The Cyber Security Committee shall consist of eleven members appointed by the Minister for their knowledge in computer and telecommunications, law and policy and skills in respect of any aspect dealt with enabling Act as follows—

(a) one representative nominated by each of the following—

(i) the Postal and Telecommunications Regulatory Authority of Zimbabwe;

(ii) the ministry responsible for information and communications technologies;

(iii) the ministry responsible for science and technology;

(iv) the ministry responsible for justice;

(v) the Zimbabwe Republic Police;

(vi) the National Prosecution Authority;

(vii) the ministry responsible for defence;

(viii) the Central Intelligence Organisation;

(ix) the Prisons and Correctional Service;

(b) one representative from the cyber security and monitoring centre;

(c) any representative from any sector of the economy or any other person who may be necessary to the deliberations in respect of a particular warrant, appointed on an ad hoc basis.

(3) From among the appointed members, the Minister shall appoint the Chairperson of the Cyber Security Committee.

(4) The Committee shall, at its first meeting, elect a Vice-Chairperson of the Committee from among its members: Provided that the Chairperson and the Vice Chairperson shall be of different genders.

(5) The provisions of the Schedule apply to the Cyber Security Committee.

(6) The Cyber Security Committee may, with the approval of the Minister, issue such guidelines as may be necessary for the carrying out of the provisions of the enabling Act as it relates to its functions under the Act

3.7 CYBER SECURITY DIRECTORATE (A UNIT IN THE MINISTRY RESPONSIBLE FOR ICT)

Roles and responsibilities:

1. Technical lead and advisor to the minister responsible for ICT on cyber security matters

2. Coordinate cyber security efforts of:

a. National Computer Incident Response Team (NCIRT) (Multi-stakeholder)

b. Zimbabwe Child Online Protection Committee (ZiCOP) (Multi-stakeholder)

c. Zimbabwe Information sharing and analysis centre (ZiSAC) (Multi-stakeholder)

d. National Network Security Operations Centre (NSOC) (Multi-stakeholder)

3. Coordinate cyber security and awareness drive done through or by the Ministry responsible for ICT.

4. Cyber Security focal point for the Ministry of ICT.

5. Advising and representing the Ministry on technical, policy, legislative and regulatory matters relating to Cyber Security

6. Collaborate with DPA on data protection issues

3.8 DATA PROTECTION AUTHORITY (DPA) – POTRAZ

The Postal and Telecommunications Regulatory Authority established in terms of the Postal and Telecommunications Act [Chapter 12:05] was designated as the Data Protection Authority.

Functions of Data Protection Authority

(a) to regulate the manner in which personal information may be processed through the establishment of conditions for the lawful processing of data;

(b) to promote and enforce fair processing of data in accordance with this Act;

(c) to issue its opinion either of its own accord, or at the request of any person with a legitimate interest, on any matter relating to the application of the fundamental principles of the protection of privacy, in the context of this Act;

(d) to submit to any Court any administrative act which is not compliant with the fundamental principles of the protection of the privacy in the framework of the enabling Act as well as any law containing provisions regarding the protection of privacy in relation to the processing of data in consultation with Minister responsible for Information, Publicity and Broadcasting Services;

(e) to advise the Minister on matters relating to right to privacy and access to information;

(f) to conduct inquiries or investigations either of its own accord or at the request of the data subject or any interested person, and in relation thereto may call upon the assistance of experts to carry out its functions and may request the disclosure of any documents that may be of use for their inquiry or investigation;

(g) to receive, by post or electronic means or any other equivalent means, the complaints lodged against data processing and give feed-back to the claimants or complainants;

(h) to investigate any complaint received in terms of the Act howsoever received;

(i) to conduct research on policy and legal matters relating to the development of international best practices on the protection of personal information in Zimbabwe and advise the Minister accordingly;

(j) in consultation with the Minister, to facilitate cross border cooperation in the enforcement of privacy laws and participating at national, regional and international forums mandated to deal with the protection of personal information initiatives.

3.9 ZIMBABWE CHILD ONLINE PROTECTION COMMITEE (ZICOP)

ZICOP is a multi-stakeholder committee to facilitate and coordinate child online safety and protection through technical, legal, policy and financial capacity mobilisation and development in Zimbabwe. It brings in all stakeholders in Zimbabwe to safeguard the rights of children online. It facilities international cooperation and support for Zimbabwe towards a safer internet for the children.

1. To coordinate of Child Online Protection (COP) activities throughout the country.
2. To advocate for establishment of COP policy and its attendant legislation;
3. To mobilise resources including ; human , financial, material, technical;
4. To coordinate of child online protection training and capacity building activities;
5. To facilitate monitoring and evaluation exercises on child online protection;
6. To establish working groups to spearhead COP activities;
7. To facilitate country – wide awareness raising campaigns;
8. To engage multi stakeholders for consultations on child online protection;
9. To promote research, data gathering, analysis, information sharing and subsequent developments are undertaken;
10. To promote regional and international cooperation and collaboration;
11. To promote disclosure and reporting of child online abuses and related crimes

3.10 ZIMBABWE INFORMATION SHARING AND ANALYSIS CENTRE (ZISAC)

A non-profit membership-based organizations that provide a central resource for gathering information on cyber threats.

Members receive direct access to a suite of services and informational products including

a. cybersecurity advisories and alerts,

b. vulnerability assessments,

c. incident response support,

d. secure information sharing,

e. tabletop exercises,

f. malicious domains/IP report, and more.

Roles and responsibilities :

(Based on best practice and other established Information Sharing and Analysis Centre (ISACs)

a. sharing of information, knowledge, standards and tools,

b. Threat intelligence gathering and sharing.

c. Development of Guidelines and best practices on incident handling, cyber security management (processes, tools).

d. Incident management : technical details, response and mitigation, operating experience feedback and, to a certain extent, operational/business consequences. Infrastructures and tools:

e. Cyber security services proposed via the platform (e.g. vulnerability analysis, pen-testing, personalised audit, staff training, etc.).

f. Common validation, qualification and certification tools, standards and methodologies.

g. Data samples (large, representative, shared, real, exploitable, with privacy clearance) enabling to assess the performance of security solutions in a non-biased way.

h. Develop industry specific Information sharing and analysis centers.

3.11 NATIONAL NETWORK SECURITY OPERATIONS CENTRE (NSOC)

3.12.1 Roles and responsibilities

24/7 multi-stakeholder collaborative SOC data aggregation center providing

a. detection, analysis and response to security incidents in real-time.

b. monitoring and analysis of traffic and events,

c. cyber data aggregation, correlation and investigation

3.12.2 Membership

- SOCs in Zimbabwe and
- SOCs serving Zimbabwe entities

3.12 Zim-CIRT

Key functions:

1. Incident Response: National CIRT shall be primary responders to cybersecurity incidents. They coordinate efforts to mitigate the impact of cyber attacks and assist affected organizations in recovery processes.
2. Threat Analysis and Intelligence Sharing: Collect, analyze, and disseminate information about cybersecurity threats and vulnerabilities to help organizations prepare and defend against potential attacks.
3. Coordination and Communication: Act as a central point for communication and coordination among various stakeholders, including government agencies, private sector companies, and international partners during cyber incidents.
4. Awareness and Training: They provide training and awareness programs to improve cybersecurity knowledge and skills among individuals and organizations, promoting best practices in cybersecurity.
5. Policy Development and Advising: Contribute to the development of national cybersecurity policies and strategies, advising government on potential improvements and regulatory measures.
6. Vulnerability Management: Identify and assess vulnerabilities in software and hardware systems and coordinate with vendors to address these issues, reducing the risk of exploitation.
7. Research and Development: Engage in research to develop new tools and techniques for cybersecurity defense and incident management.
8. Collaboration with International CIRTs: They work with other national and international CIRTs to share information, strategies, and resources, enhancing global cybersecurity resilience.

13.13 CYBER SECURITY STAKEHOLDERS – ROLES AND RESPONSIBILITIES

Stakeholder	Roles and Responsibilities
Ministry of ICT, Postal and Courier Services **& Minister responsible for cyber security and monitoring centre** **& cyber security and monitoring of interception of communications centre**	Develops national ICT policies, including cybersecurity strategies, and oversees their implementation and other functions as provided by the laws of Zimbabwe.
Professional Boards, Associations and organisations	Promotes ICT development and coordinates cybersecurity efforts across different sectors and other functions as provided by the laws of Zimbabwe.
Line Ministries, Regulators, Commissions, AG and Government agencies and other government related creatures of statute	Coordinates national cybersecurity efforts, including monitoring threats and managing incidents within there legal spheres of influence as per the laws of Zimbabwe, and other functions as provided by the laws of Zimbabwe.
Zimbabwe Republic Police (ZRP), ZACC, NPA and other investigative agencies.	Investigates and prosecute cyber-crimes and enforces laws related to cybersecurity and cybercrime as provided by the laws of Zimbabwe.
Zimbabwe Defense Forces (ZDF), Intelligence, Prison service and other national security organisations.	Protects national security from cyber threats, including safeguarding networks and data and national sovereignty and other functions as provided by the laws of Zimbabwe.
Financial Institutions (e.g., Banks)	Implement cybersecurity measures to protect customer data and financial transactions and other functions as provided by the laws of Zimbabwe.
Internet Service Providers (ISPs)	Provide secure internet services and collaborate on threat detection and response efforts and other functions as provided by the laws of Zimbabwe.
Private Sector Companies, SMEs and State-owned enterprises	Invest in cybersecurity infrastructure and practices to protect business operations and data and other functions as provided by the laws of Zimbabwe.
Academic and Research Institutions	Conduct research and provide education on cybersecurity trends, technologies, and best practices.
Civil Society Organizations	Promote cyber security and digital rights as per laws of Zimbabwe.
Judiciary	Judiciary role on issues of cyber security as per Zimbabwe laws
Users	Protect their information and systems they use
Legislature	Legislative on cyber security issues as per laws of Zimbabwe

13.14 CYBER SECURITY NATIONAL SECRETARIATE

There shall be a multi-stakeholder secretariate for implementation of the strategy, serving as an administrative office that handles the secretarial operations and coordination of the strategy. It serves as the backbone of the strategy, ensuring that its functions and activities are carried out smoothly and efficiently.

Key roles and responsibilities of a secretariate:

1. Administrative Support: Provides administrative services such as scheduling meetings, handling correspondence, and maintaining records.
2. Coordination: Facilitates communication and coordination among different departments or units within the organization to ensure cohesive operations.
3. Documentation: Manages and archives important documents, reports, and records, ensuring they are accessible and organized.
4. Meeting Management: Organizes and manages meetings, including preparing agendas, distributing materials, and recording minutes.
5. Policy Implementation: Assists in the implementation of policies and procedures set by the governing body or leadership.
6. Communication Hub: Acts as a central point for internal and external communication, disseminating information to relevant stakeholders.
7. Resource Management: Assists in oversing the allocation and use of resources, including finances, personnel, and equipment, to support the organization's objectives.
8. Support to Leadership: Provides support to the leadership by preparing briefing materials, conducting research, and assisting in decision-making processes.

PART 4

National Cyber Security Strategies

4.1 CYBERSECURITY POLICIES, LAWS, REGULATIONS & STANDARDS

Laws, regulations, policies and standard need to be crafted in such a way the that they support the vision and strategic objective of the country in general and specifically cyber security aspirations of the country. The threat landscape is changing rapidly hence the measure need to be able to versatile and strike a balance between over and under regulations.

4.1.1 Goal:

Strengthen cybersecurity policies, laws, regulations and standards.

4.1.2 Objective:

Have up-to-date and harmonised cybersecurity policies, laws, regulations, and standards.

4.1.3 Interventions:

a. Review cybersecurity policies, laws, regulations and standards.
b. Amend/update cybersecurity policies, laws, regulations and standards.
c. Establish new cybersecurity policies, laws and regulations for the adoption of new and emerging technologies.
d. Establish national cybersecurity standards/architecture.
e. Ratification of any relevant and applicable reginal and internal instruments.
f. Domesticate and Legislate of HIPSSA model law

4.1.4 Outcome

Up-to-date and hamonised polices and laws, regulations and standards

4.2 CYBERSECURITY CAPACITY DEVELOPMENT AND ORGANISATIONAL MEASURE

Cyber security is dependent on the whole system, in which the human element and institutional tone plays a critical link. We are as secure as our weakest link, hence there is need to for continuous evaluation and monitoring of capacity with the view of closing any capacity gaps and institutional inefficiencies.

4.2.1 Goal:

Strengthen cybersecurity capability and capacity

4.2.3 Objective:

Increase cybersecurity expertise, education, and awareness.

4.2.4 Interventions:

a. Establish a cybersecurity professional certification/accreditation and career progression framework.

b. Develop MOU for collaboration of institutions in the strategy

c. Support the establishment/ enhancement of Cybersecurity Operations Centers (CSOCs) in CIIs.

d. Operationalize institutions in the Cyber and data protection Act.

e. Establish a Cybersecurity Centre of Excellence (CCoE).

f. Develop more local specialized experts in cybersecurity and

g. Establish mechanism for licencing of penetration testers and digital forensic practitioners.

h. Accreditation of cyber security service providers and companies.

i. Develop and implement a cybersecurity basic education curriculum.

j. Develop and implement a cybersecurity awareness raising programme.

k. Promote cybersecurity Research &Development of in-country secure, competitive, cost-effective, and tailor-made cybersecurity solutions.

4.2.5 Outcome:

Increased cybersecurity capacity and improved cybersecurity culture and develop strong institutions.

4.3 CO-OPERATION & COLLABORATION

Cyber knows no geographical boundaries and can affect multiple entities same time.

Co-operation and collaboration is key for a secure Zimbabwe. The Zimbabweanm is committed to working with internal and external stakeholders to improve Zimbabwe's cybersecurity posture. Cooperation with other states and institutions is key.

4.3.1 Goal:

Foster national and international cooperation and collaboration.

4.3.2 Objective:

Improve national and international cooperation and collaboration.

4.3.3 Interventions:

a. Develop a national framework for national, regional and international co-operation and collaboration.

b. Establish a trusted information-sharing mechanism for information exchange and incident reporting for national and international stakeholders.

c. Participate and promote the development and implementation of international laws, agreements, treaties, policies, norms, standards, conferences and fora on cybersecurity.

d. Carry out a comprehensive stakeholder mapping.

4.3.4 Outcome:

Well-coordinated cooperation and collaboration that strengthens Zimbabwe's cybersecurity.

4.4 TECHNICAL AND CRITICAL INFORMATION INFRASTRUCTURE PROTECTION (CIIP)

Technical controls and measures are key for cyber security. Zimbabwe endeavours to have the needed technical mitigations and controls in place. Issues of supply and demand need to be studied and mechanism to ensure that value is gained by the country must be in place. Supply and value chain need to be secured.

4.4.1 Goal:

Enhance the protection and resilience of CIIs.

4.4.2 Objective:

Protect and safeguard CIIs.

4.4.3 Interventions:

a. Develop a Critical Information Infrastructure Protection framework.

b. Identify and classify CIIs.

c. Implementation of Public Key Infrastructure

d. Implement baseline cybersecurity measures (physical and technical security controls including emergency/disaster contingency and recovery measures).

e. Promote the use of local internet exchange points.

f. Establish Information sharing/reporting and Incident response framework.

g. Conduct periodic penetration tests and vulnerability assessments in MDAs

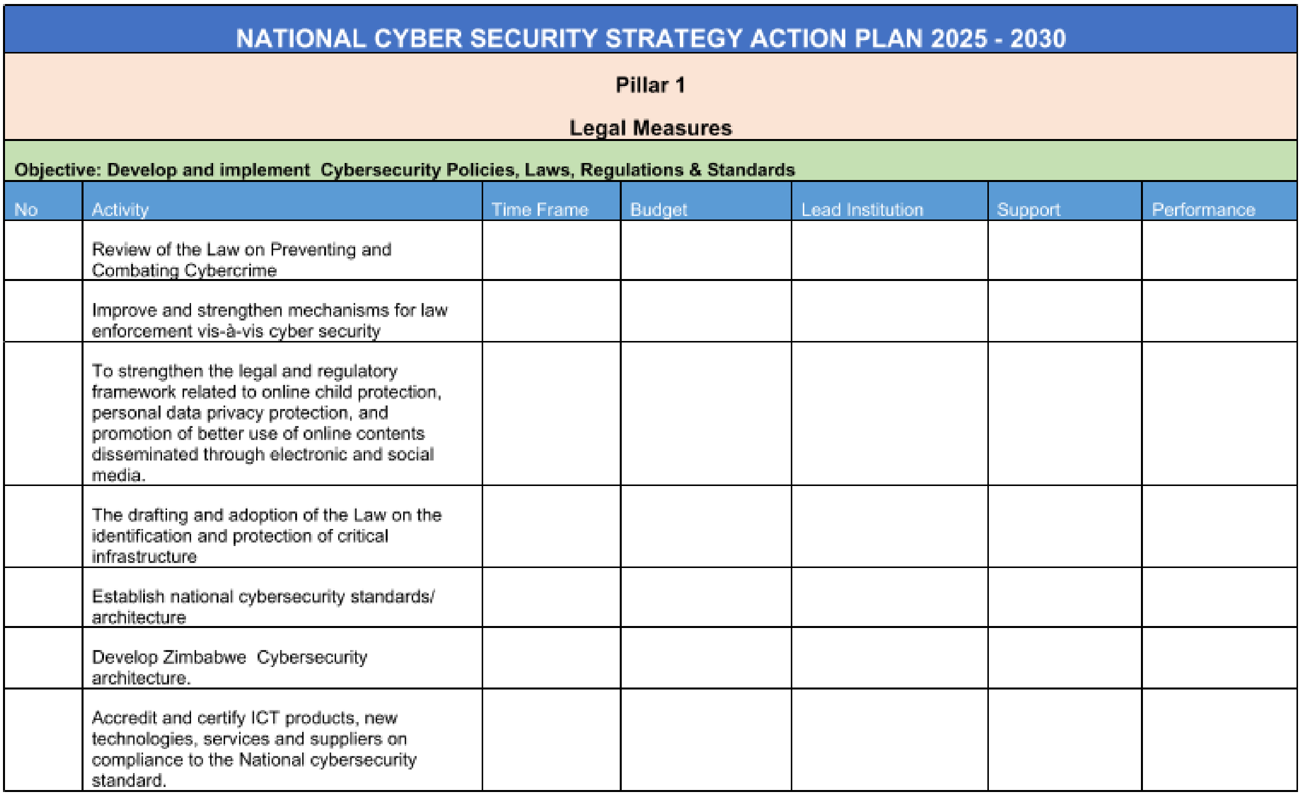
4.4.4 Outcome:

Increased protection and resilience of CIIs.

PART 5

NATIONAL CYBER SECURITY STRATEGY ACTION PLAN 2025 – 2030

(Template to be used for Planning and Implementation)



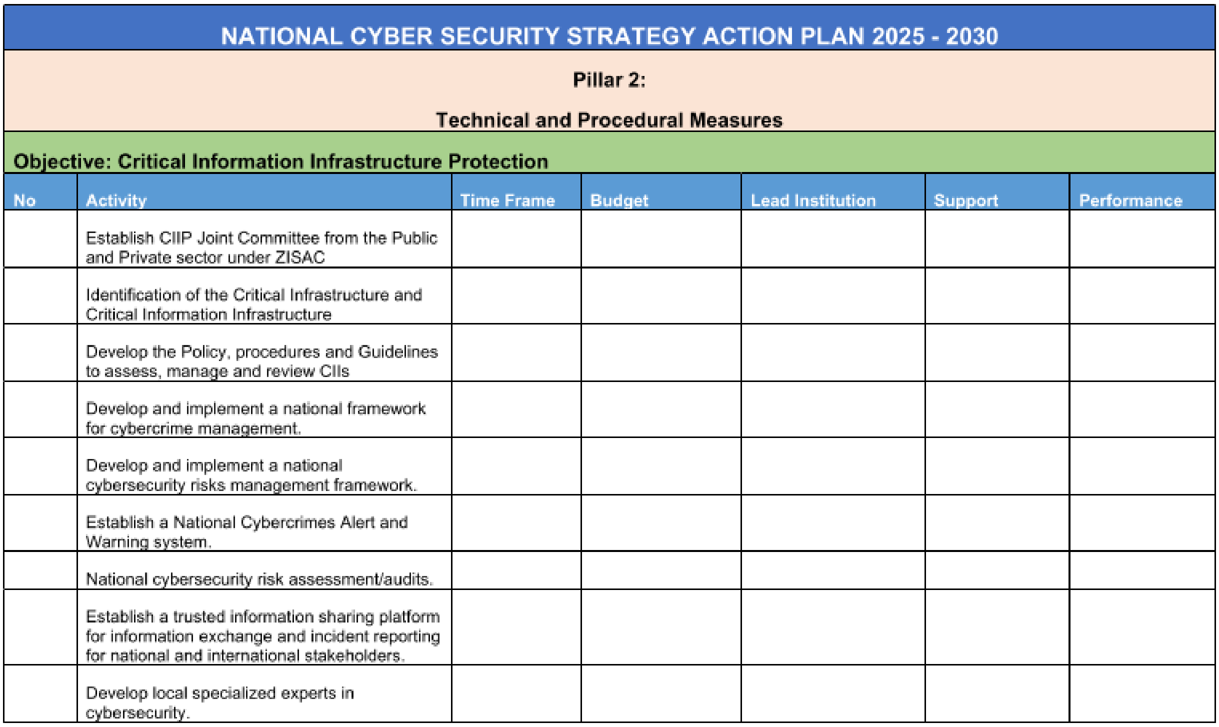
NATIONAL CYBER SECURITY STRATEGY ACTION PLAN 2025 - 2030

Pillar 1

Legal Measures

Objective: Develop and implement Cybersecurity Policies, Laws, Regulations & Standards

No	Activity	Time Frame	Budget	Lead Institution	Support	Performance
	Review of the Law on Preventing and Combating Cybercrime					
	Improve and strengthen mechanisms for law enforcement vis-à-vis cyber security					
	To strengthen the legal and regulatory framework related to online child protection, personal data privacy protection, and promotion of better use of online contents disseminated through electronic and social media.					
	The drafting and adoption of the Law on the identification and protection of critical infrastructure					
	Establish national cybersecurity standards/ architecture					
	Develop Zimbabwe Cybersecurity architecture.					
	Accredit and certify ICT products, new technologies, services and suppliers on compliance to the National cybersecurity standard.					



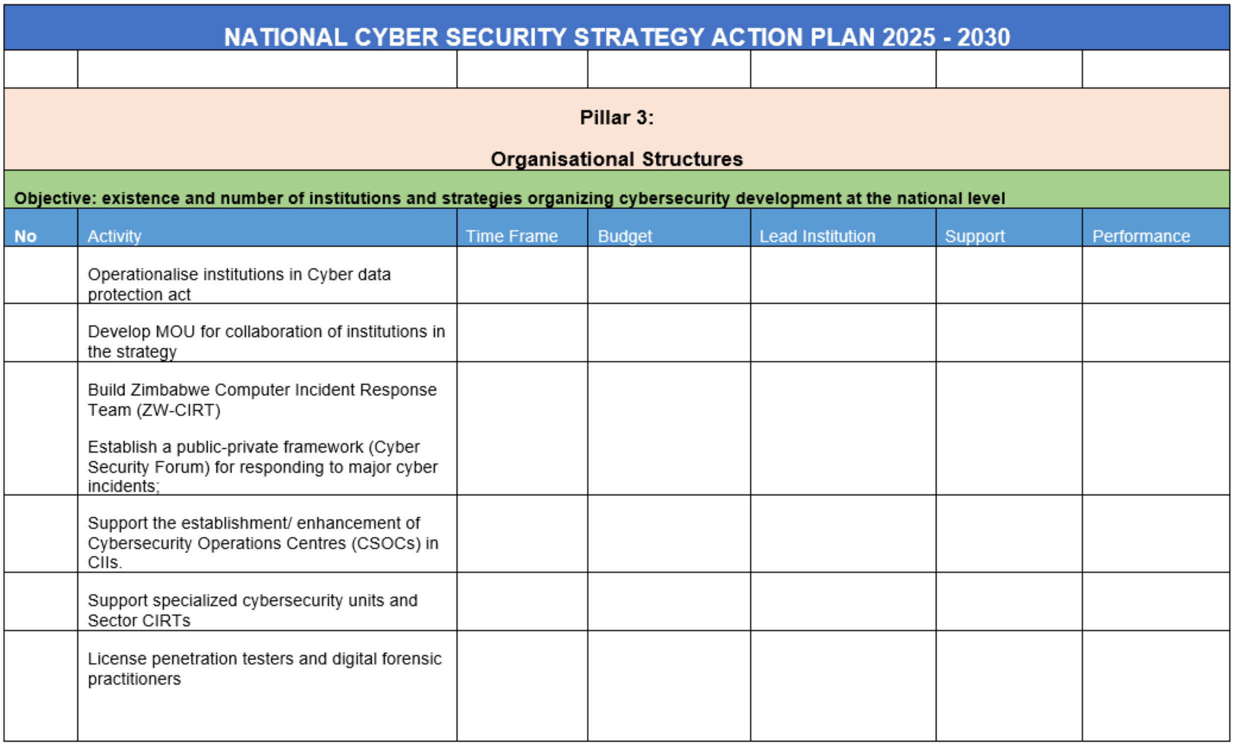
NATIONAL CYBER SECURITY STRATEGY ACTION PLAN 2025 - 2030

Pillar 2:

Technical and Procedural Measures

Objective: Critical Information Infrastructure Protection

No	Activity	Time Frame	Budget	Lead Institution	Support	Performance
	Establish CIIP Joint Committee from the Public and Private sector under ZISAC					
	Identification of the Critical Infrastructure and Critical Information Infrastructure					
	Develop the Policy, procedures and Guidelines to assess, manage and review CIIs					
	Develop and implement a national framework for cybercrime management.					
	Develop and implement a national cybersecurity risks management framework.					
	Establish a National Cybercrimes Alert and Warning system.					
	National cybersecurity risk assessment/audits.					
	Establish a trusted information sharing platform for information exchange and incident reporting for national and international stakeholders.					
	Develop local specialized experts in cybersecurity.					



NATIONAL CYBER SECURITY STRATEGY ACTION PLAN 2025 - 2030

Pillar 3:

Organisational Structures

Objective: existence and number of institutions and strategies organizing cybersecurity development at the national level

No	Activity	Time Frame	Budget	Lead Institution	Support	Performance
	Operationalise institutions in Cyber data protection act					
	Develop MOU for collaboration of institutions in the strategy					
	Build Zimbabwe Computer Incident Response Team (ZW-CIRT) Establish a public-private framework (Cyber Security Forum) for responding to major cyber incidents;					
	Support the establishment/ enhancement of Cybersecurity Operations Centres (CSOCs) in CIIs.					
	Support specialized cybersecurity units and Sector CIRTs					
	License penetration testers and digital forensic practitioners					

NATIONAL CYBER SECURITY STRATEGY ACTION PLAN 2025 - 2030

Pillar 4:

Capacity Building

Objective: Education, Awareness and Prevention

No	Activity	Time Frame	Budget	Lead Institution	Support	Performance
	Develop a cyber-security capacity building strategy and Retention Policy					
	Collaborate with the Ministry responsible for Higher and Tertiary Education to include cyber security curriculum for undergraduate/graduate programs					
	Improve and extend instruction and training in primary, secondary and higher education as a means of improving skills and knowledge on the safe use of ICT					
	Develop Security Certification Programs for Security Professionals					
	Promote specialist training of decision-makers and public body and critical infrastructure administrators from an awareness and prevention perspective for the need to safeguard critical national interests and information;					
	Promote information campaigns and alerts for all citizens and businesses					
	All Schools to run Awareness Program					

NATIONAL CYBER SECURITY STRATEGY ACTION PLAN 2025 - 2030

Objective: Building Cyber Security Industry

No	Activity	Time Frame	Budget	Lead Institution	Support	Performance
	Cooperate with academia and industry to launch short and the long-term cyber security R&D program					
	Develop a cyber-security R&D centre					
	Support national participation in international projects					
	Develop local specialized experts in cybersecurity					
	Establish a Cybersecurity Centre of Excellence (CCoE) in Zimbabwe					
	Promote cybersecurity R&D of in-country secure, competitive, cost-effective and tailor-made cybersecurity solutions.					
	Develop Cyber-Security Awareness Materials and dissemination channels					
	Establish a national Cybersecurity awareness curriculum compulsory for all organisation					
	Register all Participants that work in the ICT and Cybersecurity Industry					
	All Cybersecurity service providers to be registered and comply with basic requirements of the NCS Strategy					

NATIONAL CYBER SECURITY STRATEGY ACTION PLAN 2025 - 2030

Pillar 5:

Cooperation

Objective Develop a national framework for national, regional and international cooperation and collaboration.

No	Activity	Time Frame	Budget	Lead Institution	Support	Performance
	Participation in international activities in the field of cyber security					
	Identify and create membership with Regional and International CERTs (e.g. FIRST, ITU-IMPACT and AfricaCERT)					
	Develop cooperation initiatives in areas linked to the security of information systems, cybercrime, cyber defence and cyber terrorism, cyber espionage and cyber diplomacy, in such a way as to enhance the necessary knowledge to protect national information systems					
	Establish a trusted information sharing platform for information exchange and incident reporting for national and international stakeholders.					
	Participate and promote the development and implementation of international laws, agreements, treaties, policies, norms, standards, conferences and fora on cybersecurity.					

Strategy Review:

A rapid evolution is intrinsic to cyberspace and, consequently, there is an increase of threats, vulnerabilities, processes and infrastructures, as well as an evolution of the economic, social and cultural models upon which their use is based. This demands that this Strategy be periodically reviewed. It is believed that, without prejudice to any extraordinary review procedures that can be carried out whenever circumstances demand, this document should be reviewed:

a) Within no more than two years.
b) Annual verification of the strategic objectives and lines of action and their adaptation to changing circumstances.

Conclusion

Zimbabwe's remarkable Information and Communication technology growth continues, on a guided and informed road that insists on ensuring the confidentiality, integrity, and availability of public and private sector information throughout the nation and to all stakeholders. The ICT infrastructure is of significant importance. Zimbabwe 's National Cybersecurity Strategy is a true reflection and demonstration of the government's commitment to improving Zimbabwe's cybersecurity posture and share overarching vision, goals, and objectives. Implementation of the strategy is supported by an evolving national Cybersecurity Master Plan which operates not in isolation with other existing and established frameworks , developed to define (and ultimately govern) a prioritized roadmap of discreet cybersecurity projects. The cybersecurity strategy and master plan are critical to securing the online environment for citizens, industry, and foreign partners; increasing the Zimbabwean people's confidence in online transactions, data security, fraud protection, and privacy; encouraging greater foreign investment and enhancing trade opportunities; and enabling the country's broader economic and societal goals, with safe and respected resiliency structures.

PART 6

Definitions

6.1 DEFINITION OF TERMS

Cyber

- Cyber isdefined as: “anything relating to, or involving, computers or computer networks (such as Internet)”.
- According to International Standardisation Organisation (ISO), “Cyber is a complex environment resulting from the interaction of people, software, and services on the Internet by means of technology devices and networks connected to it, which does not exist in any physical form”.

Cyberspace

- Cyberspace is the virtual space of all IT systems linked at data level on a global scale. The basis for cyberspace is the Internet as a universal and publicly accessible connection and transport network which can be complemented and further expanded by any number of additional data networks. IT systemsin an isolated virtual space are not part of cyberspace.
- It is also known as the global environment that is created through the interconnection of communication and information systems. The cyberspace includes the physical and virtual computer networks, computer systems, digital media and data.

Cyber security

- International Standardisation Organisation (ISO) defines cyber security as “preservation of confidentiality, integrity and availability of information in cyberspace”.

Cyber Crime

- Cybercrime commonly refers to a broad range of different criminal activities where computers and information systems are involved either as a primary tool or as a primary target.

Cyber-attack, cyber espionage and cyber sabotage

- A cyber-attack is an IT attack in cyberspace directed against one or several other IT systems and aimed at damaging IT security. The aims of IT security, confidentiality, integrity and availability may all or individually be compromised.
- Cyber-attacks directed against the confidentiality of an IT system, which are launched or managed by foreign intelligence services, are called **cyber espionage**. Cyber-attacks against the integrity and availability of ITsystems are termed **cyber sabotage**.

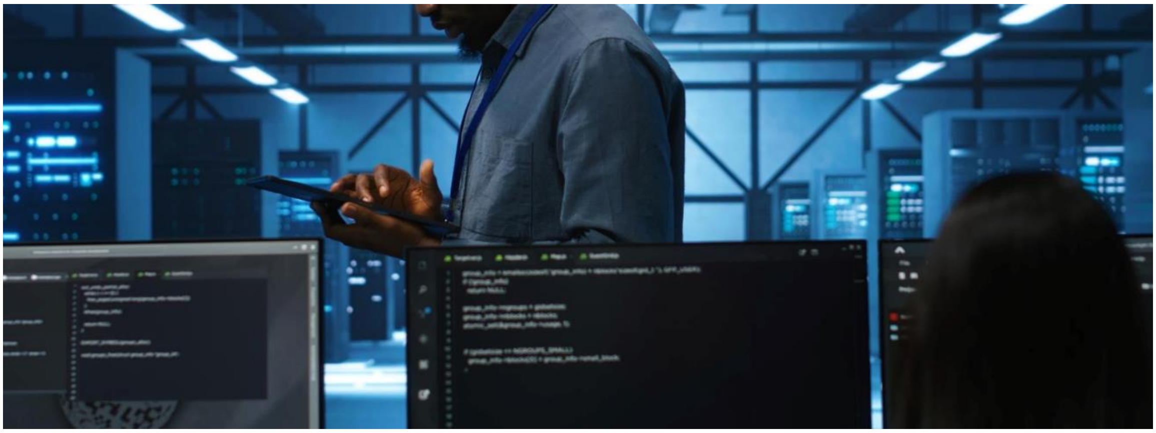
Cyber defence

- cyber defence is "the ability to safeguard the delivery and management of services in an operational Communications and Information Systems (CIS) in response to potential and imminent as well as actual malicious actions that originate in cyberspace".

Cyber Defence consists of following duties: Protect, Detect, Respond, and Recover.

Cyber Intelligence

- Activities using all "intelligence" sources in support of Cyber Security to map out the general cyber threat, to collect cyber intentions and possibilities of potential adversaries, to analyse and communicate, and to identify, locate, and allocate the source of cyber-attacks.

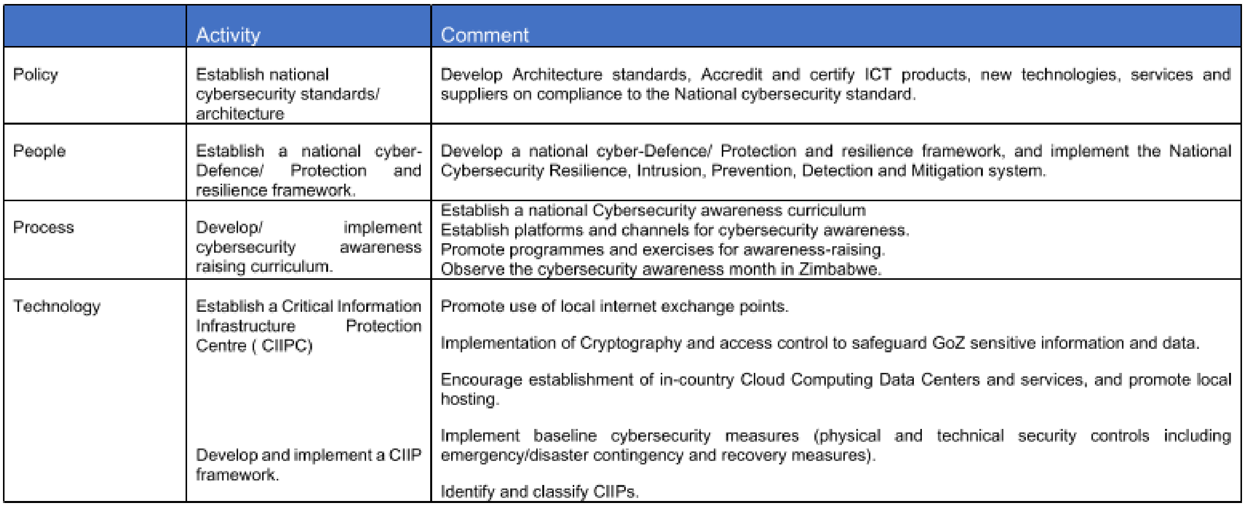


PART 7

Annexure – Consultation Process

The Ministry of Information Technology, Communication, postal and Courier Services appointed a National Cyber Security Strategy implementation working committee. This committee was composed of different members from multi stakeholders. The committee as a working group then established a working plan to roll out consultative forums and workshop throughout the country. The working group consultative forums was composed of members and representatives from different sectors that include public, private, critical, academia, regulatory bodies, law enforcement and judiciary. The approach followed, first of all was to establish a structure to adopt when gathering input from the consultative forums most which included a cybersecurity awareness training in the mornings before the consultations continued in the afternoon. The Committee also carried our a gap assessment based on the existing cybersecurity threat landscape Key questions asked were packaged to address issues in the following areas

- The general public level of awareness of cybersecurity challenges
- The advent of cybercrime and internet fraud in the country
- What is the current status of cybersecurity?
- The need for a cybersecurity strategy
- Positioning ourselves in the future



	Activity	Comment
Policy	Establish national cybersecurity standards/ architecture	Develop Architecture standards, Accredit and certify ICT products, new technologies, services and suppliers on compliance to the National cybersecurity standard.
People	Establish a national cyber-Defence/ Protection and resilience framework.	Develop a national cyber-Defence/ Protection and resilience framework, and implement the National Cybersecurity Resilience, Intrusion, Prevention, Detection and Mitigation system.
Process	Develop/ implement cybersecurity awareness raising curriculum.	Establish a national Cybersecurity awareness curriculum Establish platforms and channels for cybersecurity awareness. Promote programmes and exercises for awareness-raising. Observe the cybersecurity awareness month in Zimbabwe.
Technology	Establish a Critical Information Infrastructure Protection Centre (CIIPC) Develop and implement a CIIP framework.	Promote use of local internet exchange points. Implementation of Cryptography and access control to safeguard GoZ sensitive information and data. Encourage establishment of in-country Cloud Computing Data Centers and services, and promote local hosting. Implement baseline cybersecurity measures (physical and technical security controls including emergency/disaster contingency and recovery measures). Identify and classify CIIPs.

Format used for information gathering 1

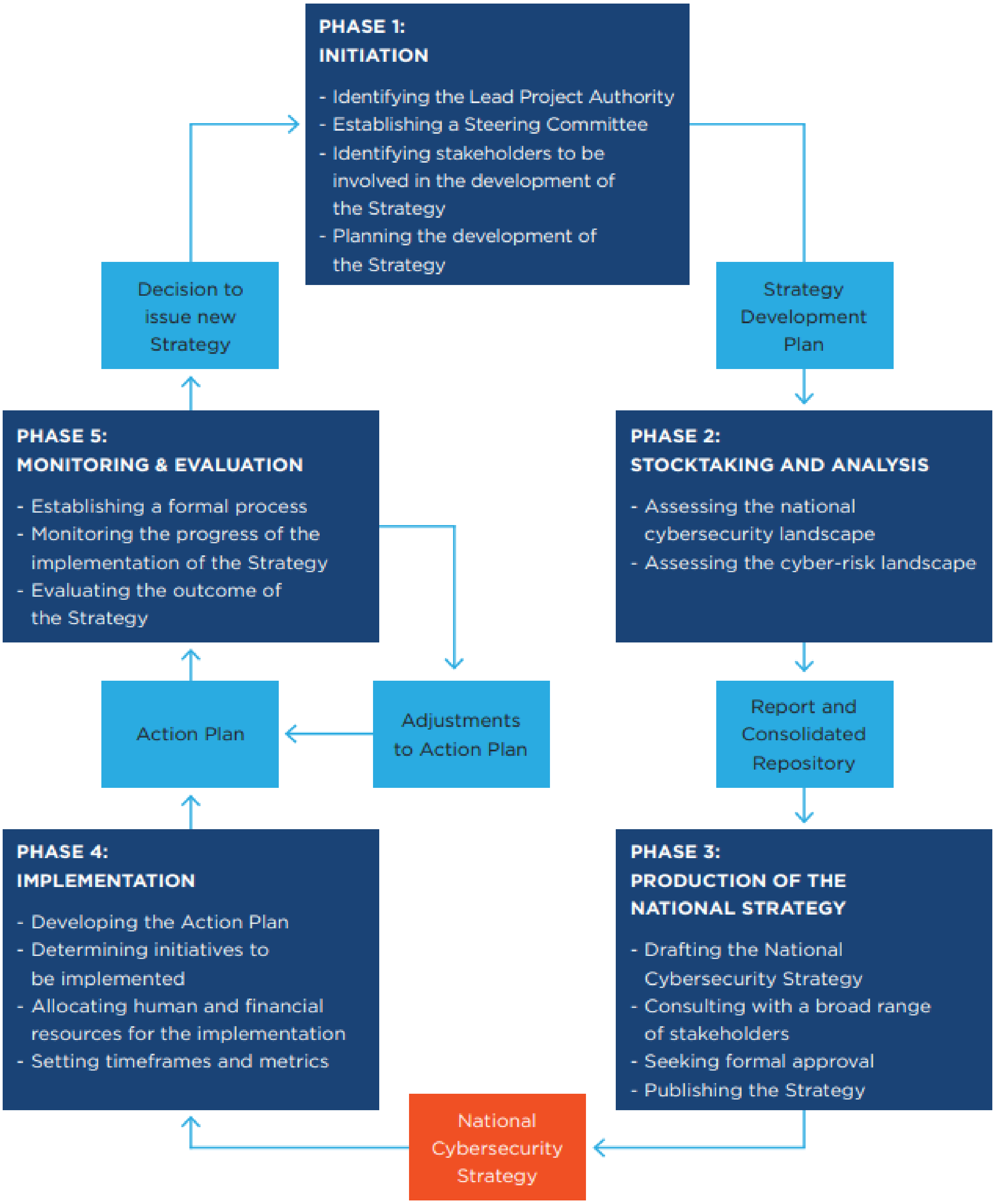
Following the assessment, the groups have focused their discussion around the following thematic areas:

- Working Legislations and regulations
- Evolution of the cyber threat landscape
- Alignment of legislation with the current and local issues
- Making the Cybersecurity and Data Protection Act implementable
- Policies that support training, certifications and career development in ICT
- Establishment of local research and development areas
- Cyber threats targeting Zimbabwe and the growth of cybercrime
- Emerging technologies and associated threats
- Establish local innovation and certification centres for cyber
- Public and private partnership
- Information sharing and National Incident Response
- Cybersecurity Education and forming cybersecurity professionals
- Law enforcement capability to tackle cybercrime
- Procedures for combatting cybercrime
- SMEs and cybersecurity
- Local technologies development for economic opportunities for Zimbabwe
- Research and Development
- Involving the Informal Sector
- Protecting the consumer of ICT services data all time
- Positioning Zimbabwe in the future The groups came up with different views and recommendations to formulate the new strategy.

Emerging cyber threats also took centre stage to be considered and addressed in the NCS Implementation Plan It was also urged that organisations need to understand Cyber Threat Intelligence and be able to appropriately manage it. Understanding the cyber threat landscape helps organizations develop effective security strategies to mitigate risks and protect against evolving threats

The Ministry of Information Communication Technology Postal and Courier Services is now conducting a validation workshop along with all relevant stakeholders to finalize the strategy document.

Lifecycle of a National Cybersecurity Strategy



PHASE 1: INITIATION

- Identifying the Lead Project Authority
- Establishing a Steering Committee
- Identifying stakeholders to be involved in the development of the Strategy
- Planning the development of the Strategy

Strategy Development Plan

PHASE 2: STOCKTAKING AND ANALYSIS

- Assessing the national cybersecurity landscape
- Assessing the cyber-risk landscape

Report and Consolidated Repository

PHASE 3: PRODUCTION OF THE NATIONAL STRATEGY

- Drafting the National Cybersecurity Strategy
- Consulting with a broad range of stakeholders
- Seeking formal approval
- Publishing the Strategy

National Cybersecurity Strategy

PHASE 4: IMPLEMENTATION

- Developing the Action Plan
- Determining initiatives to be implemented
- Allocating human and financial resources for the implementation
- Setting timeframes and metrics

Action Plan

PHASE 5: MONITORING & EVALUATION

- Establishing a formal process
- Monitoring the progress of the implementation of the Strategy
- Evaluating the outcome of the Strategy

Adjustments to Action Plan

Decision to issue new Strategy