ATU-S FRAMEWORK

relating to

MODEL FRAMEWORK FOR BUILDING INTERNET RESILIENCE IN AFRICA

numbered

ATU-S Framework 001

June 2025

List of figures

List of tables

EXECUTIVE SUMMARY

The Internet as Network of networks and its ecosystem is complex. It involves many actors, systems, infrastructures in a loose manner. While its underlying protocols are designed for resilience, an end-to-end resilience is more difficult to achieve.

In developing world, due to the economic challenges, priority goes to ultimate affordability, followed by best reliability since ultimate affordability can't always coexist with highest reliability. Also, a cheap and always cheaper Internet services limit revenue and therefore reduce providers' ability to finance capital investment to create robust and reliable infrastructure and services. Costs to resilient services can't be passed on in countries that are economically challenged.

Nevertheless, the Internet plays a critical role in all sectors nowadays and therefore requires more consideration. One of the thirteen (13) principles of the African Declaration of Internet rights and freedom is the "Security, Stability and Resilience of the Internet". This principle implies that everyone has the right to enjoy secure and reliable connectivity to the Internet, regardless of the size and location of their network. However, many African networks are frequently subject to many forms of disruption, such as power failures, cable breaks, (un)intentional shutdowns, and other security incidents.

The process of drafting a model framework document for Building Internet Resilience in Africa started with the assessment of the status of the resilience of Internet in Africa with highlights on the core issues (both internal and external) that impact Internet resilience in African states [1].

Considering the identified issues currently affecting Internet resilience in African states, based on the foundational concepts built in the first deliverable, desk reviews, public data, data and information from providers and regulators, and best practices, a model framework has been proposed.

The document is structured in three (03) parts.

In Part 1: Introduction and resilience principles. Definitions and resilience principles, the focus areas that are subject to the resilience framework are discussed. It also covers case studies of the situation in the European Union region, United Kingdom and in United States of America.

In Part 2: Resilience Framework Model. A model Resilience Framework in six (06) steps is thoroughly elaborated. It expands on resilience assessment, gap analysis, selection of solutions, integration of resilience readiness solutions with focus on how to finance resilience driven projects.

The model framework is inspired from the Department of Homeland Security resilience framework.

Part 3 is dedicated to how a component could demonstrate resilience through stress testing and measurements.

Each Component identified in this internet resilience framework should be required to prepare its plan for Resilience, due one year after issuance of compulsory Resilience Framework document from this model by the respective authorities.

Thereafter, Components should annually review their plans for Resilience and update them accordingly. The Plan for Resilience should be consistent with the Component's Continuity Plan and Reconstitution Plan.

CONTEXT

The Building and Sustaining Internet Resilience in Africa project is a joint initiative of the Africa Telecommunications Union (ATU), African Network Information Centre (AFRINIC) and the Internet Society (ISOC). The development of a model framework document for Building Internet Resilience in Africa is the first phase of the project.

This project will establish an Internet Resilience framework in Africa with the aim of building and sustaining stable and reliable means of connectivity to the Internet on the continent.

The framework will, among other things, propose a model national policy framework, a set of best practices for developing and maintaining Internet resilience at national and sub-regional levels, as well as a series of technical guidelines on the subject matter. Technical guidelines will contain, for example, recommended ways of collecting and analysing empirical data from networks and countries in the African region.

Further and based on the result of the analysis, the project will identify and outline the best practices required for creating a more resilient national and regional interconnection system that, if implemented by Internet Service Providers (ISPs) and network operators, could strengthen, and safeguard the Internet infrastructure from disruption.

The model should elaborate how a country can achieve Internet resilience and ought to include following elements at the minimum:

(1) Country-level Internet Resilience: the ability of a country to provide Internet services to its citizens at an acceptable level of service in the face of faults and challenges to normal operations.

(2) Critical Infrastructure Resilience: the resilience of the power infrastructure, the Internet cable infrastructure (both terrestrial and undersea), the availability and efficiency of Internet Exchange Points (IXPs), as well as the country-code Top-Level Domain (ccTLD) infrastructure.

(3) Network/ISP Resilience: the ability of a network to continue providing an acceptable level of service in the event of an outage or during a crisis. This resilience component is made up of various components such as the resilience of physical links, logical/peering links, performance/QoS, and DNS.

(4) Market Resilience: the ability of the market to self-regulate and provide affordable prices to end-users by maintaining a diverse and competitive market.

(5) Model national roadmap: the steps which a country ought to take in order to pursue and achieve the target objectives in relation to Internet resilience.

Related statutory objective(s)
Objective (a): To promote the development and adoption of appropriate African telecommunications policy and regulatory frameworks.

Strategic Pillar
Pillar 1: Promotion of Enabling Environment for Development and Sustainability of Digital Economies

Deliverables
The final deliverable under this consultancy shall be two documents:
Document 1: A brief report on the core issues (both internal and external) that impact Internet resilience in African states
Document 2: Model Framework document for Building Internet Resilience in Africa.

ABBREVIATIONS AND ACRONYMS

This model framework uses the following abbreviations and acronyms:

ADMS : Advanced Distribution Management Systems

AFRINIC : African Network Information Centre

ARCEP : Autorité de Régulation des Communications Electroniques et des Postes

ARPU : Average Revenue Generated per User

ARPU : Average Revenue Per User

AS : Autonomous System

ASREN : Arab States Research and Education Network

ATU : Africa Telecommunications Union

AU : African Union

BIS : Business Impact Analysis

BPA : Business Process Analysis

CAO : Chief Administrative Officer

CBA : Cost-Benefit Analysis

CCoAs : Number of Cyber Courses of Action

ccTLD : country-code Top-Level Domain

CFO : Chief Financial Officer

CIO : Chief Information Officer

CISA : Cybersecurity and Infrastructure Agency

CNI : Critical National Infrastructure

CRR : Cyber Resilience Review

CRSO : Chief Readiness Support Officer

CSO : Chief Security Officer

DERMS : Distributed Energy Resource Management Systems

DHS : Department of Homeland Security

DNS : Domain Name System

DNSSEC : Domain Name System Security Extensions

DoH : DNS over HTTPS

EC-RRG : Electronic Communications Resilience & Response Group

EPCIP : European Programme for Critical Infrastructure Protection

ETL : ENISA Threat Landscape

EU : European Union

FCC : Federal Communications Commission

GC3B : Global Conference on Cyber Capacity Building

GCSC : Global Commission on the Stability of Cyberspace

gTLDs : generic Top-Level Domain

HTTPS : Hypertext Transfer Protocol Secure

HVAC : Heating, Ventilation, and Air Conditioning

ICT : Information and Communication Technology

IDNs : Internationalized Domain Names

IEEE : Institute of Electrical and Electronics Engineers

IP : Internet Protocol

ISO : International Organization for Standardization

ISOC : Internet Society

ISPs : Internet Service Providers

IT : Information Technology

ITU : International Telecommunication Union

IX-F : Internet eXchange Federation

IXPs : Internet Exchange Points

MAN : Metropolitan Area Network

MDT : Mean down time

MTBF : Mean Time Between Failures

MTBMA : Mean Time Between Maintenance Actions

MTIR : Mean Time to Incident Recovery

MTTR : Mean Time to Repair

NCI : National Critical Infrastructure

NCS : National Cybersecurity Strategy

NIPP : National Infrastructure Protection Plan

NIST : National Institute of Standards and Technology

NOC : Operation and Maintenance Center, Network Operation Center

NPPD : National Protection and Programs Directorate

ODA : Official Development Assistance

POC : Point of contact

PPD : Presidential Policy Directive

QoE : Quality of experience

QoS : Quality of Service

SCADA : Supervisory Control and Data Acquisition

SLA : Service Level Agreement

SLAs : Service-Level Agreement

SLS : Service Level Specification

TCP : Transmission Control Protocol

THIRA : Threat, Hazard Identification and Risk Assessment

TLD : Top Level domain

TLS : Transport Layer Security

TS : Technical Specification

UDP : User Datagram Protocol

US : United States

VPP: Virtual Power Plant

WACREN : West and Central African Research and Education Network

WAN : Wide Area Network

WWW : World Wide Web

PART 1: INTRODUCTION AND RESILIENCE PRINCIPLES

1 ISSUES AFFECTING INTERNET RESILIENCE IN AFRICAN COUNTRIES

The first deliverable (document 1) builds foundational concepts and identifies the core issues that impact Internet resilience in African states.

Internet resilience is complex. In its attempt to identify the core issues that impact Internet resilience in African states, it explored and analysed enabling factors which contribute to the resilience of the Internet under the dimensions of "Trustworthiness" and "Challenge tolerance".

Data from ISOC's Internet Resilience Index 2023, from the ITU on countries with National Emergency Telecommunication plans and the Global Cybersecurity Index of 2020, but also from findings of a study on Internet QoS measurements and reporting mechanism conducted in Sierra Leone in 2020, were used to assess the ability of African countries to provide and maintain an acceptable level of Internet services in the event of outages or during crisis [1].

Very few countries in Africa demonstrated the existence of a mature enabling environment and good foundation for resilient Internet services.

The main issues identified are around the following three categories:

- weak infrastructure
  - poor performance
  - impaired services
- challenged economical context
  - lack of capital investment
  - weak services uptake
  - costs to resilience
- challenged technological context
  - lack of resilience culture
  - immaturity of resilience framework
  - immaturity of emergency framework
  - immature of cybersecurity framework

2 GOALS AND OBJECTIVES TO RESILIENCE

Resilience is complex. Achieving and maintaining resilience requires definition, adherence and acceptance of clear goals and objectives.

We view and present goals and objectives to resilience via two different perspectives: National Institute of Standards and Technology (NIST), Publication on "developing cyber-resilient systems" and ResiliNets' initiative on Network resilience. Both shows how to achieve resilience's goals (Anticipate, Withstand, Recover and Adapt) through objectives, actions, and strategies.

An analysis of the existing and the identified core issues currently affecting Internet resilience in Africa, requires that realistic objectives to resilience must be set with adequate timelines. Expectations may not be the same for everyone in a country or for all African countries.

2.1 Developing cyber-resilient systems

SP800-160, volume 2, rev1[2], on Developing Cyber-Resilient Systems set the following goals and objectives for cyber-resiliency.

Anticipate: Maintain a state of informed preparedness for adversity

Deterrence, avoidance, and prevention are strategies for anticipating potential threats. Other strategies include planning (i.e., identifying available resources and creating plans for using those resources if a threat materializes), preparation (i.e., changing the set of available resources and exercising plans), and morphing (i.e., changing the system on an ongoing basis to change the attack surface).

Withstand: Continue essential mission or business functions despite adversity
Strategies for withstanding the realization of potential threats, even when those threats are not detected, include absorption (i.e., accepting some level of damage to a given set of system elements, taking actions to reduce the impacts to other system elements or to the system as a whole, and repairing damage automatically), deflection (i.e., transferring threat events or their effects to different system elements or to systems other than those that were targeted or initially affected), and discarding (i.e., removing system elements or even a system as a whole based on indications of damage and either replacing those elements or enabling the system or mission or business process to operate without them).

Recover: Restore mission or business functions during and after adversity
Strategies for recovery include reversion (i.e., replicating a prior state that is known to be acceptable), reconstitution (i.e., replicating critical and supporting functions to an acceptable level or using existing system resources), and replacement (i.e., replacing damaged, suspect, or selected system elements with new ones or repurposing existing system elements to serve different functions in order to perform critical and supporting functions, possibly in different ways). Detection can support the selection of a recovery strategy. However, a system can apply these strategies independent of detection to change the attack surface.

Adapt: Modify mission or business functions and/or supporting capabilities in response to predicted changes in the technical, operational, or threat environments
Strategies for adaptation include correction (i.e., removing or applying new controls to compensate for identified vulnerabilities or weaknesses), hardening (i.e., reducing or manipulating attack surfaces), and reorientation (i.e., proactively orienting controls, practices, and capabilities to prospective, emerging, or potential threats). These strategies may result in redefinition (i.e., changing the system's requirements, architecture, design, configuration, acquisition processes, or operational processes).

To meet these goals, a system will have to adhere to some objectives which describe specific statements of what it intended to achieve in its operational environment and throughout its life cycle to meet stakeholder needs for mission assurance and resilient security.

Objectives
Prevent or avoid: Preclude the successful execution of an attack or the realization of adverse conditions
Prepare: Maintain a set of realistic courses of action that address predicted or anticipated adversity
Continue: Maximize the duration and viability of essential mission or business functions during adversity
Constrain: Limit damage from adversity
Reconstitute: Restore as much mission or business functionality as possible after adversity
Understand: Maintain useful representations of mission and business dependencies and the status of resources with respect to possible adversity
Transform: Modify mission or business functions and supporting processes to handle adversity and address environmental changes more effectively
Re-architect: Modify architectures to handle adversity and address environmental changes more effectively.

Cyber resiliency objectives, as described above, support interpretation, facilitate prioritization and assessment, and enable development of questions such as:

- What does each cyber resiliency objective mean in the context of the organization and the mission or business process that the system is intended to support?
- Which cyber resiliency objectives are most important to a given stakeholder?
- To what degree can each cyber resiliency objective be achieved?
- How quickly and cost-effectively can each cyber resiliency objective be achieved?
- With what degree of confidence or trust can each cyber resiliency objective be achieved?

NIST SP800-160 prescribes the sub-objectives and examples of metrics presented in the tables below:

OBJECTIVE	REPRESENTATIVE SUB-OBJECTIVES	REPRESENTATIVE EXAMPLES OF METRICS
PREVENT OR AVOID Definition: Preclude the successful execution of an attack or the realization of adverse conditions.	• Apply basic protection measures and controls tailored to the risks of the system of interest. • Limit exposure to threat events. • Decrease the adversary's perceived benefits. • Modify configurations based on threat intelligence.	• Time to patch or to apply configuration changes. • Percentage of resources for which configuration changes are randomly made. Percentage of resources for which lifespan limits are applied. • Percentage of sensitive data assets that are encrypted. Adversary dwell time in a deception environment. • Percentage of resources to which more restrictive privileges are automatically applied in response to threat indicators.
PREPARE Definition: Maintain a set of realistic courses of action that address predicted or anticipated adversity.	• Create and maintain cyber courses of action. • Maintain the resources needed to execute cyber courses of action. • Validate the realism of cyber courses of action using testing or exercises.	• Number of Cyber Courses of Action (CCoAs) in the cyber playbook. Percentage of identified threat types, categories of threat actions, or Tactics, Techniques and Procedures (with reference to an identified threat model) addressed by at least one CCoA in the cyber playbook. • Percentage of cyber resources that are backed up. Time since the last exercise of alternative communications paths. Percentage of administrative staff who have been trained in their CCoA responsibilities. • Time since last (random, scheduled) exercise or simulation of one or more CCoAs.
CONTINUE Definition: Maximize the duration and viability of essential mission or business functions during adversity.	• Minimize the degradation of service delivery. • Minimize interruptions in service delivery. • Ensure that ongoing functioning is correct.	• Time to perform mission or business function damage assessment. Length of time performance of specified mission or business function remained below acceptable levels. • Time from initial disruption to availability (at minimum level of acceptability) of essential functions. • Percentage of essential data assets for which data quality has been validated. Percentage of essential processing services for which correctness of functioning has been validated.
CONSTRAIN Definition: Limit damage from adversity.	• Identify potential damage. • Isolate resources to limit future or further damage. • Move resources to limit future or further damage. • Change or remove resources and how they are used in order to limit future or further damage.	• Percentage of critical components that employ anti-tamper, shielding, and power line filtering. • Time from initial indication or warning to completion of scans for potentially damaged resources. • Time from initial indication or warning to the completion of component isolation. • Time from initial indication or warning to the completion of resource relocation.

		• Time from initial indication or warning to the completion of switch to an alternative.
RECONSTITUTE Definition: Restore as much mission or business functionality as possible after adversity	• Identify untrustworthy resources and damage. • Restore functionality. • Heighten protections during reconstitution. • Determine the trustworthiness of restored or reconstructed resources.	• Time to identify unavailable resources and represent damage in status visualization. • Time between the initiation of recovery procedures and the completion of documented milestones in the recovery, contingency, or continuity of operations plan. Percentage of cyber resources for which access control is maintained throughout the recovery process. • Percentage of cyber resources for which additional auditing or monitoring is applied during and after the recovery process. Time to bring a backup network intrusion detection system online. Percentage of reconstituted cyber resources that are placed in a restricted enclave for a period after reconstitution. • Percentage of restored or reconstructed (mission-critical, security-critical, supporting) data assets for which data integrity/quality is checked
UNDERSTAND Definition: Maintain useful representations of mission and business dependencies and the status of resources with respect to possible adversity.	• Understand adversaries. • Understand dependencies on and among systems containing cyber resources. • Understand the status of resources with respect to threat events. • Understand the effectiveness of security controls and controls supporting cyber resiliency.	• Time between the receipt of threat intelligence and the determination of its relevance. Adversary dwell time in deception environment. • Time since the most recent refresh of mission dependency or functional dependency map. Time since the last cyber table-top exercise, Red Team exercise, or execution of controlled automated disruption. • Percentage of system elements for which failure or the indication of potential faults can be detected. Percentage of cyber resources monitored. • Number of attempted intrusions stopped at a network perimeter. Average length of time to recover from incidents.
TRANSFORM Definition: Modify mission or Business functions and supporting processes to handle adversity and address environmental changes more effectively.	• Redefine mission or business process threads for agility. • Redefine mission or business functions to mitigate risks.	• Percentage of mission or business process threads that have been analysed with respect to common dependencies and potential single points of failure. Percentage of mission or business process threads for which alternative courses of action are documented. • Percentage of essential functions for which no dependencies on resources shared with nonessential functions can be identified. Percentage of problematic data feeds to which risk mitigations have been applied since last analysis.

RE-ARCHITECT Definition: Modify architectures to handle adversity and address environmental changes more effectively.	• Restructure systems or sub-systems to reduce risks. • Modify systems or sub-systems to reduce risks.	• Size of the (hardware, software, supply chain, user, privileged user) attack surface. Percentage of system components for which provenance can be determined. Percentage of system components that can be selectively isolated. • Percentage of cyber resources for which custom analytics have been developed. Percentage of mission-critical components for which one or more custom-built alternatives are implemented.

Table 1: Cyber resiliency sub-objectives and examples of metrics

2.2 Resilient and Survivable Networks

ResiliNets initiative [3] provides a network resilience strategy in two aspects:
- real time control loop
- background loop

D^2R^2 + DR

Real-time control loop: D^2R^2

- Defend against challenges and threats to normal operation.
  - passive defence
  - active defence
- Detect when an adverse event or condition has occurred.
- Remediate the effects of the adverse event or condition to minimise the impact.
- Recover to original and normal operations.

Background loop: DR

- Diagnose the fault that was the root cause.
- Refine future behaviour.

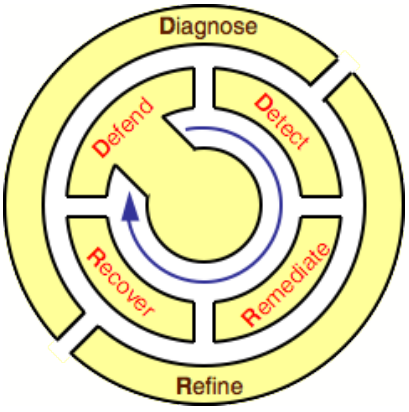


Figure 1: Resilience Strategy: D^2R^2 + DR

ResiliNets outlines four (04) principles to resilience as presented below:

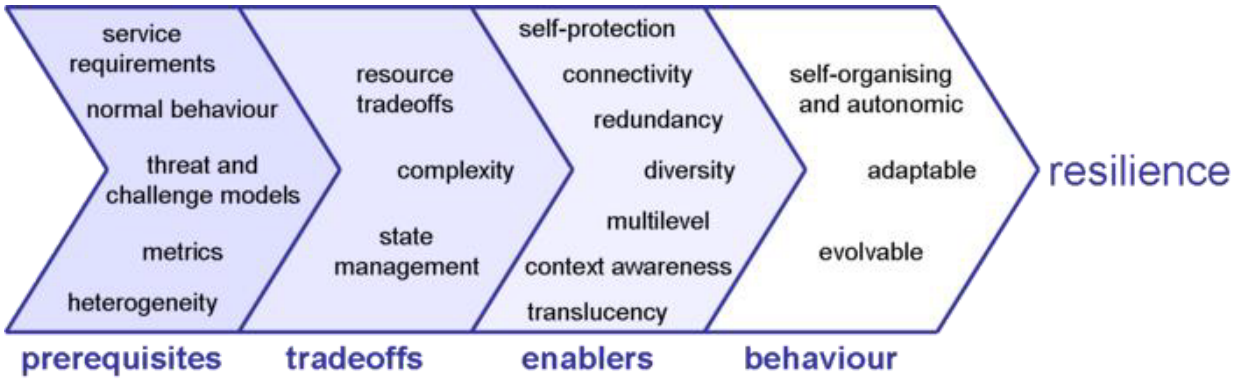


Figure 2: Resilience principles

Prerequisites: Service requirements; normal behaviour; threat and challenge models; metrics; heterogeneity in mechanism, trust, and policy.

From operation perspective, what is "normal"," partially degraded", "severely degraded"?
From service perspective, what is "acceptable", "impaired", "unacceptable"?

Tradeoffs: resource tradeoffs; complexity; state management.

How are resources, systems and processes prioritized and managed?

Enablers: security and self-protection; connectivity; redundancy; diversity; multilevel; context awareness; translucency.

Which resilience enablers are in place and to which extent?

Behaviour: self-organising and autonomic; adaptability; evolvability.

How flexible, evolutive and adaptable is the system?

3 SCOPE AND DEFINITIONS

Internet as a network of networks with no boundary is a complex system. Its resilience depends on many parameters which are not necessary under the control of a network or a country.

The scope of the resilience sought by this project is how a country can achieve Internet resilience through the following elements at the minimum:

(1) Country-level Internet Resilience: the ability of a country to provide Internet services to its citizens at an acceptable level of service in the face of faults and challenges to normal operations.

(2) Critical Infrastructure Resilience: the resilience of the power infrastructure, the Internet cable infrastructure (both terrestrial and undersea), the availability and efficiency of Internet Exchange Points (IXP), as well as the country-code Top-Level Domain (ccTLD) infrastructure.

(3) Network/ISP Resilience: the ability of a network to continue providing an acceptable level of service in the event of an outage or during a crisis. This resilience component is made up of various components such as the resilience of physical links, logical/peering links, performance/QoS, and DNS.

(4) Market Resilience: the ability of the market to self-regulate and provide affordable prices to end-users by maintaining a diverse and competitive market.

(5) Model national roadmap: the steps which a country ought to take to pursue and achieve the target objectives in relation to internet resilience.

The picture below presents a taxonomy of the Internet resilience components.

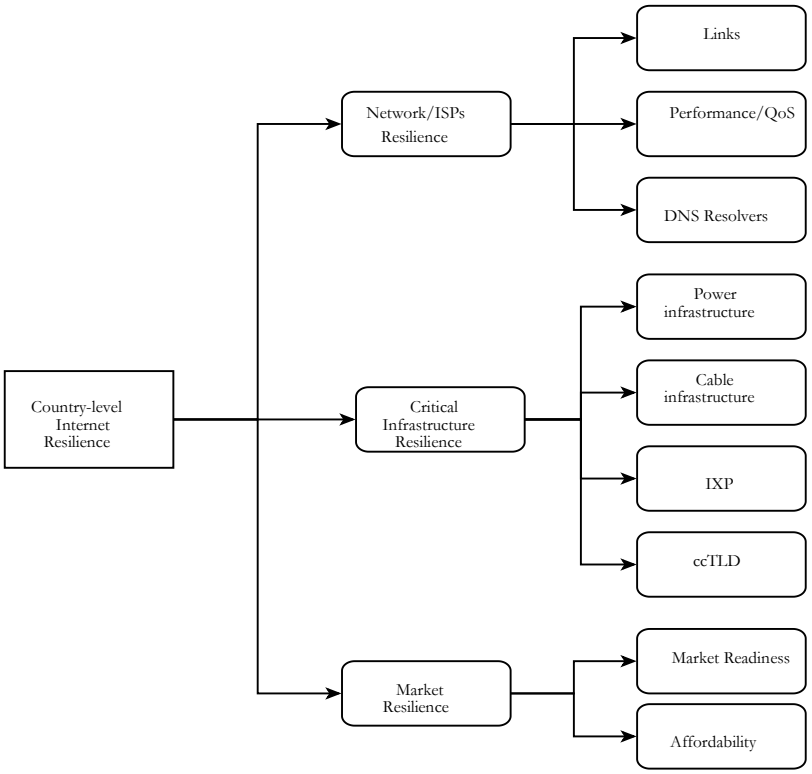


Figure 3: Taxonomy of resilience components.

3.1 The Internet

The Internet (or internet)[4] is the global system of interconnected computer networks that uses the Internet protocol suite (TCP/IP) to communicate between networks and devices. It is a network of networks that consists of private, public, academic, business, and government networks of local to global scope, linked by a broad array of electronic, wireless, and optical networking technologies. The Internet carries a vast range of information resources and services, such as the interlinked hypertext documents and applications of the World Wide Web (WWW), electronic mail, telephony, and file sharing.

3.1.1 The Network of Networks

The communication infrastructure of the Internet consists of its hardware components and a system of software layers that control various aspects of the architecture. As with any computer network, the Internet physically consists of routers, media (such as cabling and radio links), repeaters, modems etc. However, as an example of internetworking, many of the network nodes are not necessarily Internet equipment per se, the Internet packets are carried by other full-fledged networking protocols with the Internet acting as a homogeneous networking standard, running across heterogeneous hardware, with packets guided to their destinations by IP routers.

Internet service providers (ISPs) establish the worldwide connectivity between individual networks at various levels of scope. End-users who only access the Internet when needed to perform a function or obtain information, represent the bottom of the routing hierarchy.
At the top of the routing hierarchy are the tier 1 networks, large telecommunication companies that exchange traffic directly with each other via very high-speed fiber-optic cables and governed by peering agreements.

Tier 2 and lower-level networks buy Internet transit from other providers to reach at least some parties on the global Internet, though they may also engage in peering.

An ISP may use a single upstream provider for connectivity or implement multihoming to achieve redundancy and load balancing.

Internet exchange points are major traffic exchanges with physical connections to multiple ISPs. Large organizations, such as academic institutions, large enterprises, and governments, may perform the same function as ISPs, engaging in peering and purchasing transit on behalf of their internal networks.

Research networks tend to interconnect with large regional research networks such as GEANT, Internet2, Ubuntunet Alliance, WACREN, ASREN.

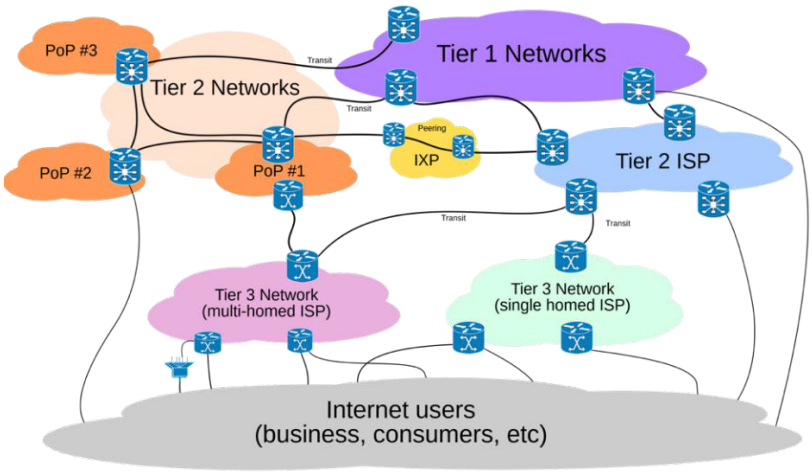


Figure 4: Illustration of the Internet service tiers[1]

At country level, Internet can be represented as per the picture below. Internet Services Providers, Content Providers, Government and Enterprise Networks, and other networks (represented by their autonomous system numbers and IP addresses) Interconnect through various means and connect to the Internet via other tiers. They provide services to customers and end-users, generally in the best effort mode, even though some customers do request SLAs.

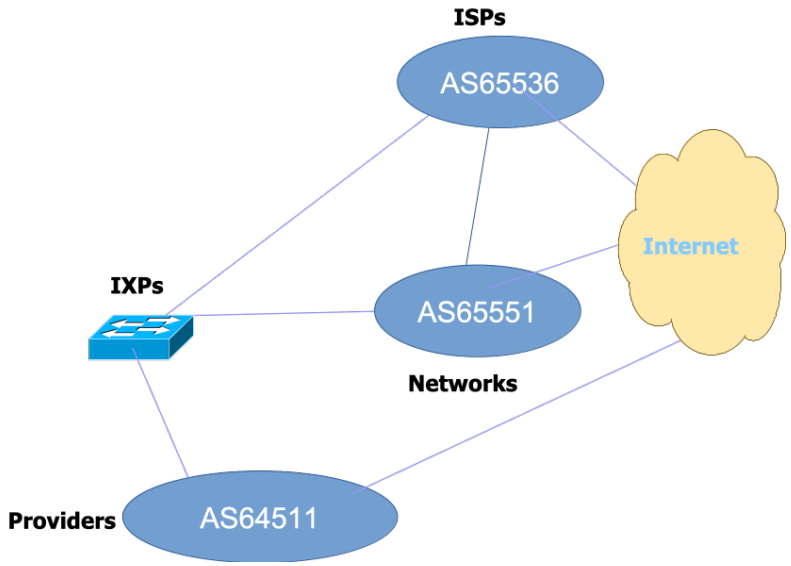


Figure 5: Country level Internet.

An ISP's network includes many segments and components: WAN, MAN, Internet access services, data centers, servers, etc.

[1] https://en.wikipedia.org/wiki/Internet#/media/File:Internet_Connectivity_Distribution_&_Core.svg

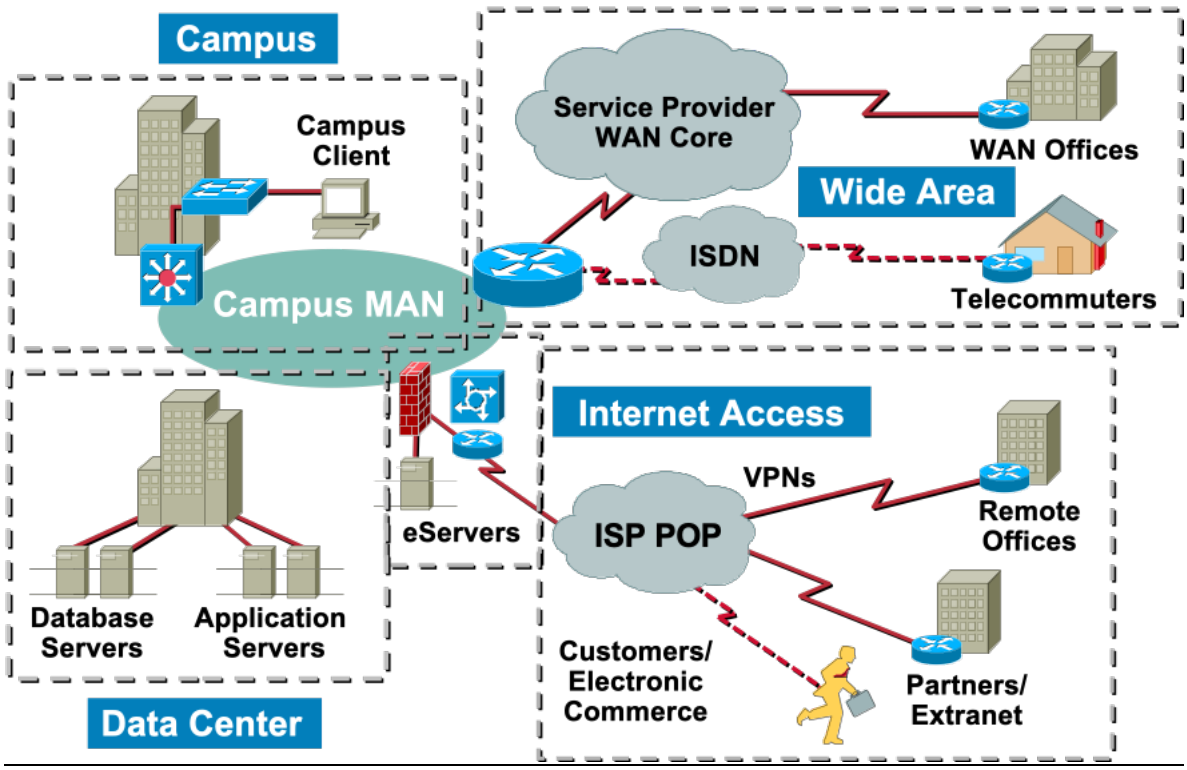


Figure 6: ISP's network.

The network generally spans multiple cities, regions, countries, and continents. Customers and users are connected via different media such as fiber-optic, radio links, mobile networks (2G,3G,4G…). Services and speed varied from providers, type and technology of access, localities, and end-users' terminals.
The African Union (AU) digital transformation strategy for Africa (2020-2030) [5] indicates as specific objective that all Africans should be digitally empowered and able to access safely and securely to at least (6 Mbp/s – Megabits per Second) all the time wherever they live in the continent. In Togolese republic for example, ARCEP (Autorité de Régulation des Communications Electroniques et des Postes) have set the thresholds for 4G to 25Mbps/12Mbps, for 3G to 3Mbps/2Mbps. [6]

Kenya's National Broadband Strategy 2023[7] defines broadband as: "Connectivity that delivers interactive, secure, quality and affordable services at a minimum speed of 2 Mbps (Megabits Per Second) to every user in Kenya".

In the US, the Federal Communications Commission (FCC) defines broadband as 25 Megabit per second download and 3 Megabit per second upload or a ratio of 8/1[8]. The asymmetry between download and upload merits are being debated considering the pandemic experience where upstream speeds have become important from the widespread use of videoconferencing. It has been argued that a user is now better off with a symmetrical 20 Megabit per second in both directions, yet that would not meet the FCC definition.

Like African Union, the European Union (EU) did not specify whether its Digital Agenda goal of broadband speeds [9] of at least 30 Megabit per second with at least half of households with 100 Megabit per second by 2020 were symmetrical. Its new goal calls for 100 Megabit per second in all households by 2030 without specifying symmetry as well as full 5G coverage in all urban areas.

3.1.2 Internet Exchange Point (IXP)

According to the Internet eXchange Federation (IX-F)[2], 'Internet Exchange Point' means a network facility which enables the interconnection of more than two independent autonomous systems, primarily for the purpose of facilitating the exchange of internet traffic, which provides interconnection only for autonomous systems and which neither requires the internet traffic passing between any pair of participating autonomous systems to pass through any third autonomous system nor alters or otherwise interferes with such traffic.
"Autonomous Systems" has the meaning given in BCP6/RFC1930, "Guidelines for creation, selection, and registration of an Autonomous System (AS)".
"Independent" means Autonomous Systems that are operated by organisational entities with separate legal personality.

Various definitions of Internet Exchange Point (IXP) exist. Some are more flexible on the requirements and the services which could be provided.

By having a presence inside of an IXP location, companies are able to shorten their path to the transit coming from other participating networks, thereby reducing latency, improving round-trip time, and potentially reducing costs.

Without IXPs, traffic going from one network to another would potentially rely on transit providers to carry the traffic from source to destination. In some situations, there's no problem with doing this: it is how a large portion of international Internet traffic flows, as it's cost prohibitive to maintain direct connections to each-and-every ISP in the world.

However, relying on a backbone ISP to carry local traffic can be averse to performance, sometimes due to the backbone carrier sending data to another network in a completely different city. This situation can lead to what is known as Tromboning, where in the worst case, traffic from one city destined to another ISP in the same city can travel vast distances to be exchanged and then return.

During the preparation of this document, there are currently fifty-three (53) active IXPs located in forty-seven (47) cities in thirty-six (36) countries in Africa [10].

As previously discussed, IXPs represent a critical component of the Internet's infrastructure.

3.2 Domain Name system

One of the critical services needed over IP networks is the Domain Name System (DNS), which facilitates the resolution of names to IP addresses, essential for establishing communication between nodes. DNS operates as a namespace, comprising a collection of wordstrings organized hierarchically into labels. It serves as a distributed name registration framework, assigning unique licenses for the use of human-readable strings for a fee. Additionally, DNS functions as a distributed database, mapping wordstrings to IP addresses. It operates using a protocol that resolves wordstrings to corresponding IP addresses.

3.2.1 DNS components

The Domain Name System comprises many elements, each operated by different entities:

- Distributed Database: The domain name system is organized as a distributed database, where a network of servers' store and convert domain names into IP addresses.
- Name Servers: A name server provides directory services within the domain name system, matching domain names with their corresponding numerical IP addresses and allowing end users to reach their desired destination on the Internet.
- Domain Name Resolvers: Domain Name Resolvers, also called DNS resolvers, are the computers which are used by ISPs to respond to a user request to resolve a domain name. "Resolving a domain name" refers to the translation of a domain name into an IP Address.
- The DNS Root Zone is the network of database servers that maintain the names and the numeric IP addresses of over gTLDs, ccTLDs, and IDNs.
- Domains: A Domain Name is part of an URL and can be typed into a browser to find a particular web site. When a computer connects to the Internet, it uses a unique IP Address; because IP Addresses can be difficult to remember, the DNS or Domain Name System was put in place to correlate IP Addresses to domain names.
- TLD Registry operators maintain the database of registrations for a particular TLD.
- Registrars allow registrants to register a domain name.

[2] https://www.euro-ix.net/en/forixps/

3.2.1.1 Resolvers

ISPs and enterprises run DNS resolver services to respond to end-users request to resolve domain names. As this service is critical, it is suggested to use a trusted resolver that is close to the network. DNS resolvers use DNS caching to speed up name resolution and reduce DNS traffic. DNS data are public data, the integrity and authenticity are guaranteed via DNSSEC protocol. Zone owners sign their zone and resolvers run the cryptographical validation.
Public free DNS [11] servers have been made available to users all over the world. Google [12] and Cloudfare [13] public DNS are most used.
In addition to traditional DNS over UDP or TCP, DNS resolvers also provide DNS over TLS (DoT) and DNS over HTTPS (DoH) for greater security and privacy. DoH make DNS packets move over HTTPS like secure web traffic, making it difficult to differentiate DNS traffic.
DNS resolvers are key components of Internet services, hence their implication in the resilience strategy of ISPs and networks.

3.2.1.2 Top Level Domains

Top Level domain (TLD)'s Registry operators are responsible for the registration database for TLDs (ccTLD, gTLD, IDN….). Each country manages at least one ccTLD based on the ISO 3166-1 alpha-2 country codes. Some do manage the equivalent of their ccTLD in local language as International Domain Names at TLD level.

Like IXP, ccTLD is a main component of the national Internet Ecosystem and, as such, is subject to resilience's requirements.

4 CASE STUDIES

In developing this Model framework for building Internet resilience in Africa, it is worth learning from what other regions or countries have done. We reviewed the cases of European Union (EU), United Kingdom (UK) and the United States of America (USA).
In these three cases, Internet resilience is covered in resilience framework, plan, or strategy of critical infrastructure as element of "information and communication technology" or as part of "digital infrastructure".
In the case of EU, Members states are requested to even apply higher resilience level to entities under digital infrastructure.
A comparative summary is covered in Appendix, table 19.

4.1 European Union

Resilience of critical infrastructure is addressed through three (03) components:

- Directive on the Resilience of Critical Entities [14]

The Directive on the Resilience of Critical Entities entered into force on 16 January 2023. Member States have until 17 October 2024 to adopt national legislation to transpose the Directive.

- Council Recommendation to strengthen the resilience of critical infrastructure [15]

The Council Recommendation on a Union-wide coordinated approach to strengthen the resilience of critical infrastructure, adopted on 8 December 2022, was the reaction to calls for additional measures in the aftermath of acts of sabotage against critical infrastructure in the EU. It builds on the 5-point plan for resilient critical infrastructure presented by President von der Leyen in October 2022. The Council Recommendation urges Member States **to enhance preparedness and response against current threats**, both by anticipating certain elements of the Critical Entities Resilience Directive and by making use of additional instruments in a coordinated manner.

- European Programme for Critical Infrastructure Protection (EPCIP) [16]

The EU's general framework for securing resilience of critical infrastructure is the European Programme for Critical Infrastructure Protection (EPCIP). The programme was established in 2006 based on the Commission Communication on Critical Infrastructure Protection in the Fight against Terrorism.

The Directive aims to strengthen the resilience of critical entities against a range of threats, including natural hazards, terrorist attacks, insider threats, or sabotage, as well as public health emergencies. Under the new rules:

- Member States will need to adopt a **national strategy** and carry out **regular risk assessments** to identify entities that are considered critical or vital for the society and the economy.

- In turn, the critical entities will need to carry out risk assessments of their own and take **technical, security and organisational measures** to enhance their resilience and **notify incidents**.
- **Critical entities** in the EU **providing essential services in six or more Member States**, will benefit from extra advice on how best to meet their obligations to **assess risks** and **take resilience-enhancing measures**.
- Member States will need to provide **support to critical entities** in enhancing their resilience. **The Commission will provide complementary support to Member States and critical entities**, by developing a Union-level overview of cross-border and cross-sectoral risks, best practices, guidance material, methodologies, cross-border training activities and exercises to test the resilience of critical entities, among others.

The Directive covers **eleven sectors**:

- Energy
- Transport
- Banking
- Financial market infrastructure
- Health,
- Drinking water
- Wastewater
- **Digital infrastructure**
- Public administration
- Space and
- Production, processing, and distribution of food

The following entities are included in digital infrastructure:

- Providers of Internet exchange points (IXPs)
- DNS service providers
- Top-level-domain name registries
- Providers of cloud computing services
- Providers of data centre services
- Providers of content delivery networks
- Trust service providers
- Providers of public electronic communications networks
- Providers of electronic communications services

These entities manage the elements which make modern digital infrastructure including the Internet. Their criticality is so high that article 8 of the directive indicates that "Member States shall ensure that Article 11 and Chapters III, IV and VI do not apply to critical entities that they have identified in the sectors set out in points 3, 4 and 8(digital infrastructure) of the table in the Annex. Member States may adopt or maintain provisions of national law to achieve a higher level of resilience for those critical entities, provided that those provisions are consistent with applicable Union law.

4.2 United Kingdom

In his October 2018 Budget Statement, the Chancellor of the Exchequer confirmed that the National Infrastructure Commission would be examining the resilience of the UK's infrastructure.
In the final report of the study – Anticipate, react, recover – Resilient infrastructure systems [17]– the Commission concludes that there is a need for a new framework for resilience which **anticipates** future shocks and stresses; improves actions to **resist**, **absorb** and **recover** from them by testing for vulnerabilities; values resilience properly; and drives adaptation before it is too late**.**
It proposes a resilience framework around six elements:

- **anticipate** – actions to prepare in advance to respond to shocks and stresses, such as collecting data on the condition of assets.
- **resist** – actions taken in advance to help withstand or endure shocks and stresses to prevent an impact on infrastructure services, such as building flood defences.

- **absorb** – actions that, accepting there will be or has been an impact on infrastructure services, aim to lessen that impact, such as building redundancy through a water transfer network to prepare for future droughts.
- **recover** – actions that help quickly restore expected levels of service following an event, such as procedures to restart services following an event such as a nationwide loss of power.
- **adapt** – actions that modify the system to enable it to continue to deliver services in the face of changes, for example using storage in the electricity system to support renewable generation.
- **transform** – actions that regenerate and improve infrastructure systems, for example transforming infrastructure to meet the net zero target.

The report also stresses the following actions to be taken:

2021

- Government to ensure that Ofwat, Ofgem and Ofcom have resilience duties (as recommended in the Commission's regulation study) and consider whether to extend this to road and rail.
- Government to introduce a statutory requirement for Secretaries of State to publish resilience standards every five years, starting in 2022, alongside an assessment of where changes are needed to existing structures, powers, and incentives to support the delivery of these standards.
- Regulators to set out initial plans for stress tests.

2022

- Regulators to advise government on costs and benefits of different resilience standards.
- Secretaries of State to publish the first set of resilience standards and assessment of changes to structures, powers, and incentives.
- National Infrastructure Commission | Anticipate, React, Recover: Resilient infrastructure systems

2023

Regulators to introduce new obligations on infrastructure operators, to ensure they:

- meet government's resilience standards
- undertake regular stress tests
- develop and implement plans to address vulnerabilities identified by stress tests
- develop and maintain long term resilience strategies from 2023 onwards.

2024 (at the latest)

- Regulators to ensure the first round of the new stress tests are complete.
- Future price reviews
- Regulators to ensure their determinations in future price reviews are consistent with meeting resilience standards in the short and long term.

The Electronic Communications Resilience & Response Group (EC-RRG) provides some Resilience Guidelines for Providers of Critical National Telecommunications **[**18**]**. The purpose of these guidelines is to bring together a wide range of advice and guidance on agreed best practice in the establishment and maintenance of resilience within telecommunications networks and services, for those Communications Providers which are considered to be part of the UK's Critical National Infrastructure (CNI), either because of the scale of their operations or because they provide key services to other parts of the CNI.

4.3 United States of America

The Presidential Policy Directive (PPD) [19] on Critical Infrastructure Security and Resilience advances a national unity of effort to strengthen and maintain secure, functioning, and resilient critical infrastructure.

National Infrastructure Protection Plan (NIPP 2013) [20] meets the requirements of Presidential Policy Directive (PPD) on Critical Infrastructure Security and Resilience, signed in February 2013. The Plan was developed through a collaborative process involving stakeholders from all 16 critical infrastructure sectors, all 50 states, and from all levels of government and industry. It provides a clear call to action to leverage partnerships, innovate for risk management, and focus on outcomes.

The National Plan is streamlined and adaptable to the current risk, policy, and strategic environments. It provides the foundation for an integrated and collaborative approach to achieve the vision of: "[a] Nation in which physical and cyber critical infrastructure remain secure and resilient, with vulnerabilities reduced, consequences minimized, threats identified and disrupted, and response and recovery hastened.
The Department of Homeland Security (DHS)'s Resilience Framework [21] focuses on four key critical infrastructure areas where the Framework process is applied. These four focus areas are:

- Energy and Water,
- Facilities,
- Information and Communication Technology, and
- Transportation.

The information and Communication Technology sector identified as part of critical infrastructure, operates in conjunction with the communications sector, particularly through **the Internet**. ICT encompasses the hardware, software, internal telecommunications infrastructure, programming, and information systems that comprise the assets, networks, and systems under communications and related information technology. The communications sector may include broadcast, cable, satellite, wireless, and wireline.

The Resilience Framework is formulated to support a process in six (06) steps. DHS Components apply the Resilience Framework and Resilience Readiness Planning Assessment, along with additional information from other assessments such as facility energy, water, and sustainability audits and physical and vulnerability assessments, to develop Component Plans for Resilience. These plans will identify the current overall level of resilience of Component critical infrastructure mission essential assets and the solutions and projects required to make these assets fully resilient.

PART 2: INTERNET RESILENCE FRAMEWORK MODEL

1 RESILIENCE DRIVERS

Security and resilience are everyday concerns for everyone. Countries, companies, institutions, government's agencies, etc, have always been forced and tasked to plan and incorporate security and resilience into their strategies. The following requirements, recommendations, and initiatives direct towards more resilience over times.

1- Goal 9 of the 17 Sustainable Development Goals [22], adopted by all United Nations Member States in 2015, mandates to "Build resilient infrastructure, promote inclusive and sustainable industrialization and foster innovation". Target 9.4 indicates to "Develop quality, reliable, sustainable, and resilient infrastructure, including regional and transborder infrastructure, to support economic development and human well-being, with a focus on affordable and equitable access for all.

2- The recent Accra call [23] for cyber-resilient development, conclusions of the Global Conference on Cyber Capacity Building (GC3B) held in Accra in November 2023 recommends that:

Cyber resilience can play a crucial role in achieving sustainable development objectives, managing risk in national and international development investments, promoting the rule of law, contributing to international security and stability, and protecting and realizing human rights. Key actions to consolidate this multi- faceted role include:

- Encourage decision-makers across different strategic areas, including development, security, technology, and diplomacy, to integrate cyber resilience into national, regional, and international sustainable development strategies as a cross-cutting priority.

- Promote the mainstreaming of cyber resilience across international development programming, including the roll-out of digital risk impact assessments in the design of initiatives, accompanied by digital risk mitigation and management plans during implementation.

- Accelerate the integration of the cyber capacity building community of practice with the development field to consolidate its links and approaches with broader development goals. This can be pursued, inter alia, by creating opportunities for more structured dialogues involving the respective communities, leveraging the convening power of existing multistakeholder platforms.

- Strengthen and promote cyber resilience knowledge and skills among international development workforce – including donors, implementors, and partner organizations – through the development and implementation of regular training and education courses.

3- One of the thirteen (13) principles of the African Declaration of Internet rights and freedom [24] is the Security, Stability and Resilience of the Internet. This principle implies that everyone has the right to enjoy secure and reliable connectivity to the Internet regardless of the size and location of their network. However, many African networks are frequently subject to many forms of disruption, such as power failures, cable breaks, (un)intentional shutdowns, and other security incidents.
In some instances, the outages are caused by accident, either due to poor engineering or lack of redundant infrastructure. Whether intended or not, Internet disruptions can have a considerable impact on society and the economy.

2 RESILIENCE FOCUS AREAS

The framework model is expected to elaborate how a country can achieve Internet resilience and ought to cover at least the three (03) focus areas which constitute key elements of the Internet's infrastructure. Each time any of these elements are challenged or impacted, continuity of Internet services is threatened and sometimes, requires substantial efforts to reconstitute operations after events. The focus areas are:

- Networks/ISPs,
- Critical infrastructure,

- Market

For each focus area, being resilient entails the ability to adapt to changing conditions and withstand and rapidly recover from disruption.
Focus area covers certain key Components which are interdependent and together form the resilience of the Internet in country.

2.1 Networks/ISPs

As presented in section 3.1, Internet Services Providers, Network and Content Providers, Government and Enterprise Networks, and other networks (represented by their autonomous system numbers and IP addresses) Interconnect through various means and connect to the Internet.

They form the core national Internet Infrastructure. They rely on cable infrastructure (terrestrial, undersea), wireless infrastructure, and other infrastructures like power, Internet Exchange Points, data centers, ccTLDs etc.

2.2 Critical Infrastructure

Critical infrastructure is an asset or system which is essential for the maintenance of vital societal functions.

Critical Internet infrastructure is a collective term for all hardware and software systems that constitute essential components in the operation of the Internet.

In an attempt to define critical Internet Infrastructure", Global Commission on the Stability of Cyberspace (GCSC) Critical Infrastructure Assessment Working Group defines "the public core of the Internet [25]" to include:

- packet routing and forwarding,
- naming and numbering systems,
- the cryptographic mechanisms of security and identity
- physical transmission media.

The model framework among others, addresses under "critical infrastructure", the power infrastructure, cable infrastructure (both terrestrial and undersea), availability and efficiency of Internet Exchange Points (IXP), as well as the country-code Top-Level Domain (ccTLD) infrastructure. Network operations and services depend on packet routing and forwarding, but also on cryptographic mechanisms of security and identity.

The power infrastructure is the most challenging vital sector in many countries. Internet infrastructure depends on the power system, thus its inclusion in the components of critical Internet infrastructure. All related facilities as well as end-users depend on power to provide or use services.

In the context, power infrastructure refers to Electricity infrastructure, defined as "consists of the equipment and services necessary to take electrical energy generated from things like hydroelectric dams, fossil fuel (coal, natural gas, or oil), nuclear, solar, wind, geothermal, and biomass power plants (or electrical energy stored by energy storage systems) and transmit it to end-use residential, commercial, and industrial customers. Electricity infrastructure includes transmission- and distribution-level equipment like power transformers, voltage regulators, circuit breakers, switchgear, capacitors, fuses, controls, arresters, conductor, as well as electric vehicle charging infrastructure and associated grid control technologies like supervisory control and data acquisition (SCADA) systems, advanced distribution management systems (ADMS), distributed energy resource management systems (DERMS), virtual power plant (VPP), cybersecurity systems and more."[26]

2.3 Market

The Internet market includes services providers and users. Services encompass connectivity and access, contents, applications, Over-The-Top services, etc. The uptake of these services depends on availability and affordability, as well as on the consumer readiness factors such as literacy and School Life Expectancy. Additionally, the local relance of the content and applications play a significant role. Affordability is influenced by various factors including standard of living, system cost per user; cost per service area; cost per megabit. Moreover, the situation may differ between urban and rural areas.
The Average Revenue Per User (ARPU) is generally different, and in many rural areas, where it is difficult to generate sufficient revenue to support digital services, priority then goes to ultimate affordability, followed by the best reliability since ultimate affordability may not coexist with the highest reliability.

2.4 Resilience Focus Areas Interdependencies

Infrastructure sectors and systems do not exist nor operate in isolation. Due to the various dependencies and interdependencies between infrastructure sectors, a disruption or breakdown in any one area could create cascading effects that impact other areas.

Table 2 shows how interdependent the focus areas are. Understanding the interdependencies of critical infrastructure assets required to meet mission essential functions and the effects of disruption of these assets are key to the continuity program and process, and in turn, to developing resilient solutions that ensure sustained mission essential functions.

Networks/ISPs and other providers depend on services provide by the critical infrastructure (power, IXPs, cables and DNS) to provision and deliver services to users. They also depend on the market ability to afford and use sustainable and resilient services.

Critical infrastructure depends on networks and communication services for data networking, computing, and building automation systems that control their systems. They also depend on the market ability to afford and use sustainable and resilient services.

Market depends on Power, DNS, and other identity and trust systems to use services offered by providers.

		Networks/ISPs	Critical Infrastructure	Market
Networks/ISPs	Depends on…		Power, IXPs, cables and DNS to provision and deliver services to users.	Market readiness to take and use sustainable and resilient services provided by providers
Critical Infrastructure		Networks and communication services for data networking, computing, and building automation systems that control critical infrastructure		Market readiness to take and use sustainable and resilient services provided by critical infrastructure
Market			Power, DNS and other identity systems to use services offered by providers	

Table 2: Focus Area Interdependencies

Table 3 shows the interdependencies between the Components of the resilience framework presented at figure 3. It shows dependency relationship between them. Some components depend on others to be able to operate, provide services and meet performance level.

		ISP Links	DNS Resolver	Cable system	Power ecosystem	IXP	ccTLD
ISP Links	Depends on…		-to resolve endpoints naming	-to connect to upstreams, downstreams and to IXPs	-to power links endpoints. -to provide HVAC in hosting facilities.	-to interconnect with upstreams for normal or emergency services	-to name endpoints
DNS Resolver		-to query authoritative name servers			-to operate and provide services	-to query local authoritative name servers	
Cable system		-to control and monitor power system through data networks and communication services			-to power endpoints. -to power transmission equipment. -to provide HVAC in hosting facilities -to operate and provide services	-to control and monitor cable system through data networks and communication services	
Power ecosystem		-to control and monitor power system through data networks and communication services				-to control and monitor power system through data networks and communication services	
IXP		-to access external services -to provide services to the public - for monitoring		- to connect to other IXPs and other networks	-to power endpoints. -to power switching/routing equipment -to provide HVAC in hosting facilities -to operate and provide services		-to name endpoints
ccTLD		-to provide registration and DNS services		-to connect to Internet, IXP and other networks	-to operate and provide services	-to provide local names registration and DNS services	

Table 3: Components Interdependencies

3 RESILIENCE FRAMEWORK PROCESS

Network resilience is the ability of the network to provide and maintain an acceptable level of service in the face of various faults and challenges to normal operation.

Resilience can be conceptualized through the following four disciplines or dimensions.

- Dependability, which is the property of a system such that reliance can justifiably be placed on the service it delivers. It generally includes the measures of availability (ability to use a system or service) and reliability (continuous operation of a system or service), as well as integrity, maintainability, and safety.

- Security, which is the property of a system and measures taken such that it protects itself from unauthorised access or change, subject to policy. Security properties include AAA (auditability, authorizability, authenticity), confidentiality, and nonrepudiation. Security shares with dependability the properties of availability and integrity.

- Performability, which is the property of a system such that it delivers performance required by the service specification, as described by QoS (quality of service) or QoE (Quality of experience) measures.

- Robustness, as a property that relates the operation of a control system to perturbations of its inputs. In the context of resilience, robustness describes the trustworthiness (quantifiable behaviour) of a system in the face of challenges.

The resilience of networks shall be considered from the operational and service perspectives, with defined "**acceptable service level**" and "**normal operations"**, while assessing the level of "Trustworthiness" and "Tolerance to faults" through these disciplines or dimensions.

Achieving resilience's objectives may require the following qualities:

- Redundancy refers to system properties that allow for alternate options, choices, and substitutions under stress. For equipment and functions that are likely be damaged, extra capacity or capabilities are prepared in advance and activated as needed or used in normal operation.

- Resourcefulness is the capacity to mobilize needed resources and services in emergencies:
  - to detect and manage congestion.
  - to substitute: damaged equipment and facilities are replaced by newly deployed multi-purpose facilities or surviving resources originally installed for a different purpose or repair.
  - to repair: systems and facilities, multiple routes, spare equipment, and materials necessary to restore temporarily (emergency restoration construction, installation of temporary telecommunications lines, electric power supply) are prepared to repair the damaged equipment and facilities.

- Rapid Recovery is the speed with which disruption can be overcome and services stability is restored. Matching accepted downtime, recovering within restoration time or incident recovery time.

The model framework is inspired from the department of Homeland Security resilience framework [21]

Table 4 describes these four resilient qualities with examples related to the technical, organizational, and economic dimensions of infrastructure. When determining resilience solutions, these qualities of resilient infrastructure and systems should be considered.

Quality	Technical	Organizational	Economic
Redundancy	Capacity for technical substitutions and workarounds	Alternate sites for managing disaster operations	Ability to substitute and conserve needed inputs
Resourcefulness	Availability of equipment and materials for restoration and repair	Capacity to improvise, innovate, and expand operations	Business and industry capacity to improvise
Rapidity	System downtime, restoration time	Time between impact and early recovery	Time to regain capacity, lost revenue

Table 4: Resilience Qualities with examples related to infrastructure dimensions.

3.1 Resilience Framework Integration of Continuity and Reconstitution

Continuity requirements must be incorporated into the operational activities of all Entities to ensure the sustainment of services. Continuity implementations follow the four phases [27]: readiness and preparedness, activation, continuity operations, and reconstitution. As presented in Figure 7 these implementation phases represent the full spectrum of activities during all phases of operation from normal operations, throughout a disaster event, and to recovery.

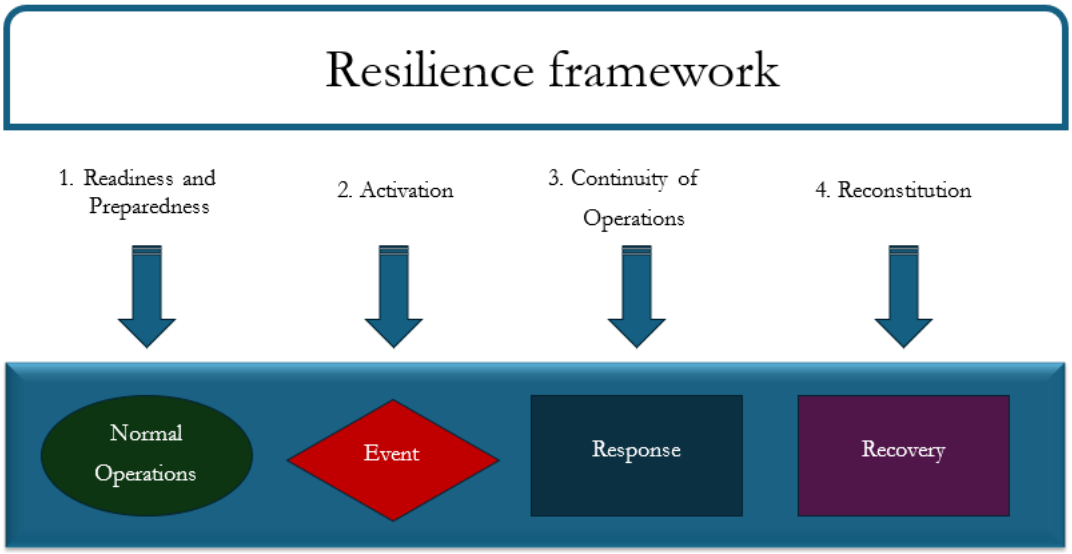


Figure 7: Resilience Phases of Operations/Continuity and Reconstitution Implementation

Readiness and preparedness refer to priority measures taken during normal operations to prepare for and reduce the effects of disruption to essential functions and services. This pre-event/threat function primarily consists of the required planning and training necessary to enhance the resilience of continuity mission and to ensure that a viable framework exists to support and facilitate the execution process.
Normal operation is the time to perform continuity processes and analyses and prepare the required continuity plan and reconstitution plan. This is also the time to implement the resilience framework process and prepare the plan for resilience to ensure that networks and systems are sufficiently resilient to provide and maintain an acceptable level of service in the face of various faults and challenges to normal operations.

Activation focuses on executing the entity's initial response to an event or threat and those actions taken to execute that response according to the continuity plan.

Continuity operations focus on implementing recovery strategies to restore system capabilities, repair damage, and resume operational capabilities at the original or new alternate location.
The Reconstitution Phase defines the actions taken to test and validate system capability and functionality. During Reconstitution, recovery activities are completed, and normal system operations are resumed. If the original facility is unrecoverable, the activities in this phase can also be applied to preparing a new permanent location to support system processing requirements.

The resilience framework provides a process that incorporates into steps 2, 3, and 4 of the existing processes and analyses for continuity planning, along with additional processes and analyses to:

1. Identify potential gaps in the resilience of the Internet component to be able to fully support mission essential functions during and after a disruption event, as well as during normal operations.

2. Determine and integrate the resilience solutions and projects necessary to close these gaps (Figure 7)

As the Internet Component stakeholders implement the Resilience Framework process steps, starting with identifying critical mission essential functions and assets, the resilience readiness of these assets will begin to be determined, and gaps will be identified. This will lead to solutions and projects that must be implemented to close those gaps and reach a state of full resilience readiness. These activities should answer the following three essential questions:

- What is critical?
- Is it vulnerable?
- What can be done to make it resilient?

The outcome of these steps will result in development of the Component plan for resilience, as well as the Continuity and Reconstitution Plans.

The proposed Resilience Framework's holistic approach will ensure resilience is considered, planned, and incorporated into the performance of all services during all phases of operations normal, event, response, recovery, and mitigation.

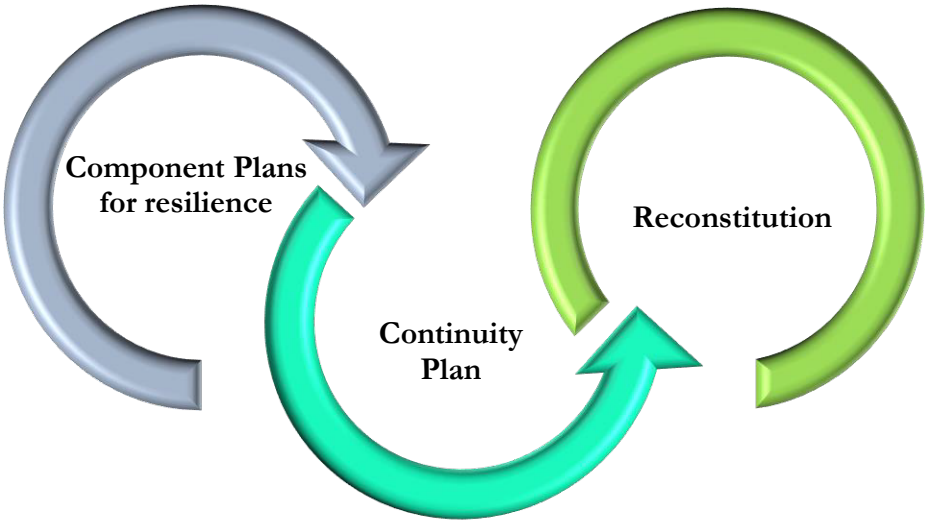


Figure 8: Approach to Resilience Planning

3.2 Resilience Readiness Assessment Score

To help assess existing resilience, entities must be evaluated across the different systems that support their mission. The cyber resilience review [28] developed by Cybersecurity and Infrastructure Agency (CISA) could be used. The Cyber Resilience Review (CRR) is an interview-based assessment to evaluate an organization's operational resilience and cybersecurity practices. Through the CRR, an entity can develop an understanding of its ability to manage cyber risk during normal operations and times of operational stress and crisis. The outcome of scoring continuity, reconstitution, and resilience assists entities in determining their resilience readiness.

The Cyber Resilience Review provides tools to help guide entities in executing each step of the Resilience Framework process. The CRR Self-Assessment [29] evaluates maturity across ten(10) domains of cybersecurity and identifies specific gaps that can be used to initiate a process improvement project. A plan for improvement is guided in part by:

• an evaluation of the self-assessment results
• the identification of practice performance gaps in each domain
• an alignment of each domain's practices with the organization's mission, strategic objectives, and the risk to critical infrastructure, resulting in a target maturity level for each domain
• review of provided options for consideration

Table 5 gives a more detailed description of the process improvement activities.

This baseline assessment should be taken initially to determine entities status about executing the steps of the process. For instance, currently many or all Components may have already completed their Continuity planning steps as Components should have been implementing Continuity planning.

However, with the aid of the CRR, Components may identify gaps in their existing Continuity planning that should be completed or specific areas of these steps that need to be revisited to ensure the entities have derived all the information necessary to continue with the subsequent Resilience Framework process steps. This will enable them to accurately determine the right resilience solutions required to make the Component sites fully resilient where needed.

	Inputs	Activities	Outputs
Perform Evaluation	1. CRR Self-Assessment 2. Organizational policies and procedures 3. Understanding of current cybersecurity management and operations	1. Conduct the CRR Self-Assessment	1. CRR Self-Assessment Report
Analyse Identified Gaps	1. CRR Self-Assessment Report 2. Understanding the organization's objectives with respect to the critical service and its impact on critical infrastructure	1. Analyze gaps within the context of the organization (e.g., risk tolerance or threat profile) 2. Determine the potential impact of gaps to organizational objectives and impact on the critical service and on critical infrastructure. 3. Determine which gaps should receive further attention	1. List of gaps and potential impact
Prioritize and Plan	1. List of gaps and potential impact 2. Understanding of organizational constraints (e.g., resources, legislation)	1. Identify potential actions to address gaps. 2. Perform cost-benefit analysis (CBA) for actions. 3. Prioritize gaps and actions based on CBA and impact. 4. Develop plan to implement prioritized actions	1. Prioritized implementation plan
Implement Plans	1. Prioritized implementation plan	1. Monitor and measure implementation progress against plan. 2. Reevaluate periodically and in response to major changes in the risk environment	1. Improvement plan tracking data

Table 5: Recommended Process for Using Results of Resilience self-assessment

Each of the six steps of the proposed Resilience Framework process is shown in Figure 8 and discussed in the following sections.

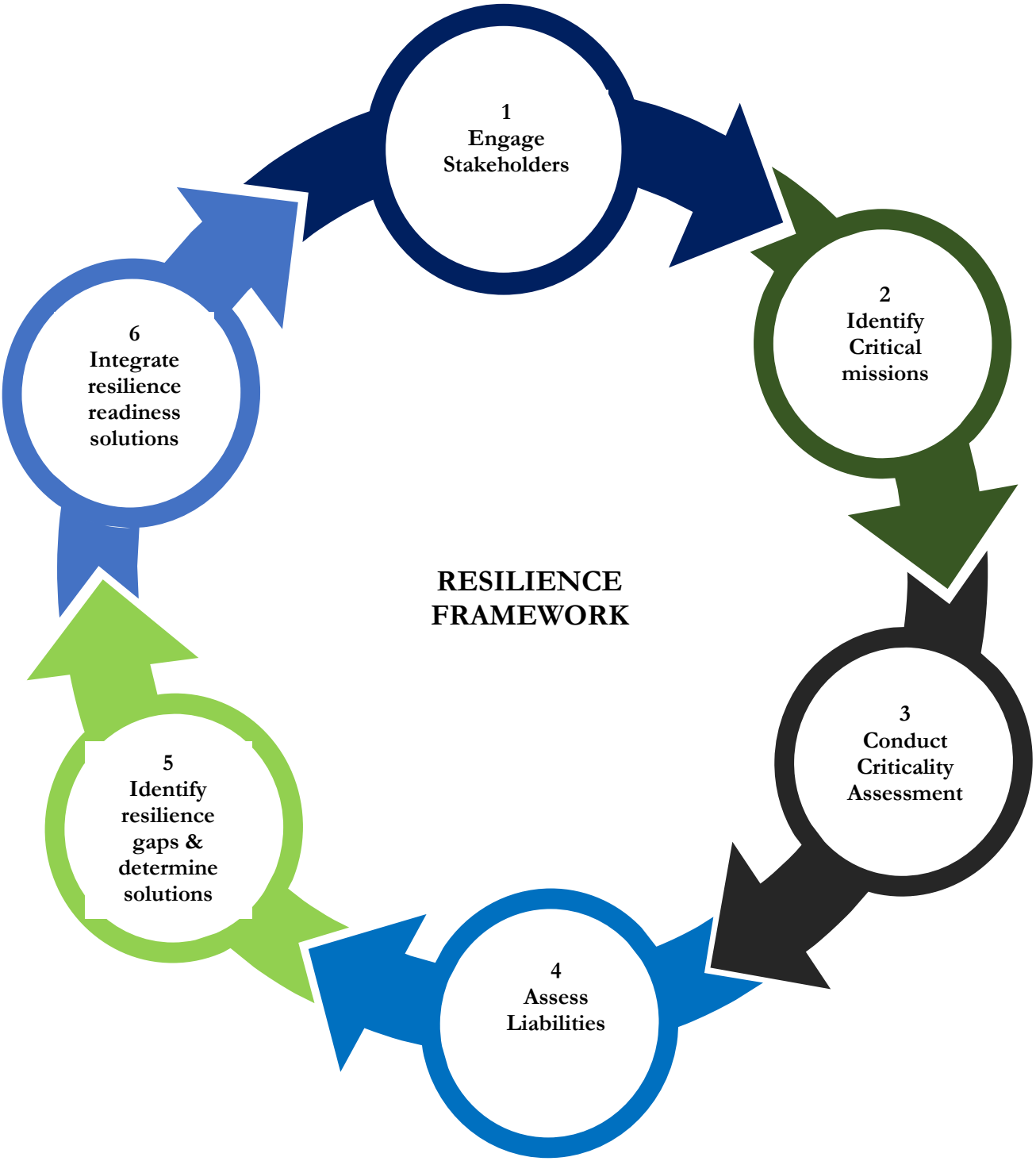


Figure 9: Six-Step Resilience Framework Process

3.3 Step 1: Engage Stakeholders

Planning for resilience requires convening appropriate stakeholders who represent a diverse range of perspectives and expertise on various issues. The number and types of stakeholders may vary depending on the focus area or component mission, geographic location, size, and assets portfolios.

It is essential to assemble the right team of stakeholders to implement each step of the Resilience Framework process, so that the appropriate expertise and decision-making authority actively participate when needed.

Understanding gaps in stakeholders and filling those gaps accordingly will be essential to the success of the resilience plan. The mix of stakeholders may vary to some extent throughout the Resilience Framework process depending on which step of the process is being implemented and which of the three resilience focus areas or component is being examined.
Stakeholders like end-users and Intermediaries like in the case of ccTLD (registrars, hosting companies, resellers) may be considered.

It should be noted that because of the high degree of interdependencies among the three focus areas, it is advisable that expertise from each focus area participate together throughout the process to help ensure that important interdependencies are not overlooked.

Stakeholders should be engaged to actively participate throughout the process. Assigning tasks to stakeholders and regularly reporting to the team are effective ways to secure stakeholder buy-in and ownership of the planning process outcome, as well as to maintain communication among team members.

To facilitate stakeholder engagement, entities should carefully select the most appropriate person or persons to lead the stakeholder team in navigating through the entire Resilience Framework process, taking into consideration the leader(s)'s expertise, group facilitation skills, decision-making authority, etc.

Table 6 lists potential stakeholder roles that should be considered when assembling a stakeholder team to implement the resilience process. Note that this list does not necessarily comprise all possible stakeholders that should be considered.
Stakeholders could be drawn from component, depending on which steps of the Resilience Framework are being implemented and at what level (e.g., individual site, Component portfolio). Additionally, external stakeholders may also be needed, such as service vendors or technical support contractors.

Role	Responsibility
Sector's leadership	Supports development of the plan and development of resilience projects
Continuity manager/Point of contact (POC)	Oversees and manages the day-to-day operations of the Component Continuity program
Chief Information Officer (CIO)	Exercises responsibility for approval, management, and oversight of information technology systems and assets
Chief Security Officer (CSO) / Security manager	Supervises, oversees, and directs the security program to safeguard Department/Component people, information technology and communication systems, facilities, property, equipment, information, and other material resources
Chief Readiness Support Officer (CRSO) / Chief Administrative Officer (CAO)	Responsible for coordination, policy, and planning of Readiness Support programs and operations across (the Component), including facilities, property, equipment, and other material resources; logistics programs; and environmental programs
Safety and Health manager	Ensures compliance with safety and health requirements for personnel, functions, and assets
Real Property manager / Facility manager	Maintains facility conditions and ensures performance of real property assets (buildings, structures, land); supports maintenance and operations of a specific site and serves as a guide to potential projects
Energy manager	Ensures energy measures are incorporated into resilience plans and actions
Chief Financial Officer (CFO)	Oversees and directs the (Component) budget, appropriations, expenditures of funds, accounting, internal controls, and finances
National Protection and Programs Directorate (NPPD) representative	Leads the national effort to protect and enhance the resilience of the nation's physical and cyber infrastructure

Utility manager / service provider	Provides utility services at the site and may provide alternative financing and assistance for projects
Contractors for supplies / delivery	Ensures supplies are delivered during daily operations and could identify potential contingency plans during emergencies
Government representative	Ensures good partnerships and may enter into agreements to provide mutual aid or benefits during long-term disruptive events
Regulators	Ensure understanding and compliance to regulatory frameworks and may provide assistance and support when implementing resilience solutions
End-users' representatives	Ensure end-users constraints and needs are considered

Table 6: Potential Stakeholders for Resilience Planning

Note

This is an important phase which will determine the success of the whole process. It is expected that countries or regional organization engaged in this shall recommend that existing stakeholder's identification and engagement methods be used to convene the appropriate team for each focus area. Guidelines and principles to governance used in developing the National Cybersecurity Strategy (NCS) can applied. In the absence of prior experience, the guide to developing a national cybersecurity strategy from ITU provides detailed insights. [30]. In addition to this, international standardisation organization's standard on governance of Information Technology (IT) for the organization can seed the step.[31]

3.4 Step 2: Identify Critical Mission

Because it is crucial to target the right assets for infrastructure protection, determining these assets is the first phase in the continuity planning and Resilience Framework life cycle. After orienting the stakeholders so they understand the meaning of critical infrastructure, and particularly the Resilience Framework critical infrastructure focus areas (i.e., Networks/ISPs, Critical infrastructure, and market), the team should be ready to begin Step 2: Identify Critical Mission.

Identifying Critical Mission is the first step in continuity planning and incorporated into the Resilience Framework as Step 2 (following Step 1: Stakeholder Engagement).

Identifying Critical Mission entails using the Business Process Analysis (BPA), to identify mission essential functions and their associated infrastructure mission essential assets. This activity will likely be spearheaded by the continuity team lead or manager leading the stakeholder team.

The first activity in identifying the critical mission is to identify mission essential functions. A mission essential function enables an organization to provide to provide and maintain an acceptable level of service in the face of various faults and challenges to normal operation.

The distinction between mission essential and non-essential categories is whether a component must perform a function or continue to perform the function during a disruption to normal operations or during emergencies.

The component will apply the Business Process Analysis to help define its mission essential functions.

Business Process Analysis is a systematic method that dissects missions and examines how essential functions are accomplished by identifying and mapping the functional processes, workflows, activities, personnel expertise, systems, data, essential/vital records, facilities, alternate locations for devolution, dependencies, and interdependencies inherent to the execution of the mission essential functions.

The outcome of this analysis is a clear understanding of mission essential functions and the associated assets critical to performing those functions. Determining these critical assets is the key and foundation of the six-step Resilience Framework life cycle process, as these assets are the targets for infrastructure protection and resilience. Without this solid foundation, the remaining life cycle steps of the Framework may be flawed, resulting in a Plan for Resilience that fails to protect the appropriate critical infrastructure and therefore, mission assurance.

A key piece of information needed at this step is an accurate list of applicable assets to review. The stakeholders are additionally responsible to provide to the team other assessments, processes, and documentation relevant to the critical

mission and resilience to include in the Business Process Analysis and help develop a baseline of the current state of the component's functions, assets, and policies.

All essential functions must be supported by a completed Business Process Analysis and Business Impact Analysis (performed in Resilience Framework Step 3) conducted regularly.
Identify and prioritize those critical services that must continue during an emergency can be done in accordance with local regulations/requirements or other best practices.

3.5 Step 3: Conduct Criticality Assessment

Step 3 of the Resilience Framework process is to conduct Criticality Assessment. Criticality refers to the level of "importance to a mission or function, or continuity of operations". A criticality assessment establishes a baseline from which to prioritize projects to improve resilience. It prioritizes mission essential functions and associated mission essential assets based on consequence factors, thus enabling risk-based decision-making on mitigation strategies and resilience requirements.

When conducting criticality assessments, it is important to ask the stakeholders the following questions about the asset or function.

- Why is it important?
- What quantitative and qualitative factors will assist in assessing its level of criticality?
- Where does it rank in priority relative to other critical assets and functions?
- How can this asset or function be prioritized for implementing projects at each level of criticality?

An asset's criticality is a function of both time and situation, based on the asset's operational or business value. Value depends on several factors. First, "what mission essential functions rely on an asset and how those dependencies change across time"; Second, "how sensitive the functional operation is to the loss or compromise of the asset"; in other words, what is the maximum allowable downtime if the asset is compromised.

Finally, whether the asset can be restored after an interruption or if a switch to a backup can be made within the allowable downtime.

A Business Impact Analysis (BIA) is essential in identifying and prioritizing what is critical to the component by prioritizing services that must continue during disruption or emergency, as well as during normal operations.

Business Impact Analysis is a method of identifying the potential negative impacts of failing to perform an essential function through quantitative and qualitative assessments of continuity criticality.

It determines the consequence of loss of essential functions, assets, and systems that are critical in supporting the execution of mission essential functions. Further, it requires the application of organization-wide risk analysis to inform decision making and strengthen operations through effective risk management. The results of Business Impact Analysis, integrated with intelligence and threat reporting, inform risk management activities to ensure the continued performance of essential functions.

A Business Impact Analysis supports the risk analysis and risk management of the essential functions, essential supporting activities, and supporting internal critical infrastructure previously identified in the Business Process Analysis.

Business Impact Analysis provides the scoring of the component "mission criticality levels." Part of the purpose in conducting a Business Impact Analysis is to plan, prepare, and respond to any kind of threat, by identifying the criticality levels and resiliency of various systems and assets. To do this, component should identify the potential impacts on the performance of essential functions and asset from a disruptive event.

National regulations or component policy may impose Business Impact Analysis scoring metrics to assess the criticality of services and functions. An example is provided at table 7. Scores are based on the consequence of loss or disruption over an extended period. Higher values indicate greater impact on the successful execution of mission essential functions, or greater consequence of loss.
International Organization for Standardization (ISO) Technical Specification (TS) 22317:2021[32], Security and resilience – Business continuity management systems – Guidelines for business impact analysis, offers good guidance on using Business Impact Analysis to inform risk prioritization and response.

A criticality Level 4 has greater impact on the component's ability to execute its mission essential functions, and has a greater consequence of loss, than a Criticality Level 1.

Criticality Level 4	**Very high consequence**—Loss or disruption of the asset or function has exceptionally grave consequences, such as total loss of primary services, core functions, and processes.
Criticality Level 3	**High consequence**—Loss or disruption of the asset or function has grave consequences, such as, loss of primary services, and major loss of core processes and functions for an extended period.
Criticality Level 2	**Medium consequence**—Loss or disruption of the asset or function has moderate to serious consequences, such as impairment of core functions and processes.
Criticality Level 1	**Low consequence**—Loss or disruption of the asset or function has minor consequences or impact, such as a slight impact on core functions and processes for a short period of time.

Table 7: Example of continuity Criticality Quantitative Scoring Definitions

When prioritizing the need for and implementation of resilience solutions and projects, first consideration should be given to addressing those associated with mission essential functions and assets falling into Criticality Level 4.

Furthermore, as discussed in Section 2.4, interdependencies among Components can produce significant cascading impacts across the assets. That is why it is important to perform dependency analysis to map functions and relationships among the critical assets. As a result of the dependency analysis, the criticality attributes for previously identified assets may be updated and additional critical assets may be identified.

3.6 Step 4: Assess Liabilities

Risk's management requires leveraging resources to address the most critical assets that are also the most vulnerable and that have the greatest threat exposure. In Step 4: "Assess Liabilities", the Component identifies the threats, risks, and vulnerabilities of these assets.

The end goal of assessing liabilities is to determine the level of risk that exists under each focus area and components. The level of risk is a function of the threat that exists, combined with the vulnerability to the threat, considering the consequence of the action and impact on mission.

Based on a comprehensive risk assessment and risk management, the Component should understand what can happen (hazards and outcomes), the likelihood of it happening (the combined probability of hazards and vulnerabilities), and the consequences if it does happen (severity of outcomes).

Liabilities should be evaluated based on the degree of mission impact and the extent to which a liability will cause interruption.

Evaluators should refer to the focus areas and determine how a liability will affect each focus area independently, as well as how a liability in one focus area will affect other focus areas due to their interdependencies. For each Component and site, a comprehensive evaluation must be performed to determine the unique threats that exist, and how these may have an impact on the mission of the system or sub-system.

The Business Process Analysis and Business Impact Analysis, conducted as part of the Component's Continuity of Operations program, are used to support risk assessment, and are integrated into the component Risk Management processes. These analyses aid in identifying obvious and non-obvious, emerging, and future risks or threats to an organization's operations. As a result, structured and in-depth analysis enables organizations to consider and allocate resources to those areas of greatest risk and where the most benefit from investment may be achieved.

3.6.1 Ascertain Hazards and Threats

Hazards are generally classified into three main categories: natural, technological, and human-caused.
Natural hazards result from acts of nature, severe weather, or changes in climate (e.g., increased precipitation, increased intensity, increases in temperature).
Technological hazards, also referred to as infrastructure hazards, result from accidents or the failures of systems and structures. Examples of common technological hazards include power disruptions or outages, and roadway or bridge failures.
Human-caused hazards are threats or intentional actions of an adversary, such as acts of terror and cyberattacks.

The process for identifying and addressing many of the hazards is similar. Taking an all-hazards approach to resilience planning will help Components become much more robust and assist with reacting to and withstanding events of many different types. For example, extreme weather (natural hazard) can cause power outages (technological hazard) and cyberattacks (human caused) to communication infrastructure may hamper recovery efforts after major weather events or power outages.

Identifying solutions to address one type of hazard may apply to all three types. It is most effective to address all hazards when conducting resilience planning as focusing on one set of hazards may not enhance resilience as a whole.

Table 8 shows potential threats and hazards from ENISA 's "Threat Landscape of Internet Infrastructure" [33]

Threat types	Threat	Asset types
Physical attacks		
	Sabotage	Hardware, Infrastructure
	Unauthorised physical access/unauthorised entries to premises	Hardware, Infrastructure
Disasters.	Natural disasters	Hardware, Software, Information, Services, Interconnection, Infrastructure, Human resources
	Environmental disasters	Ditto
Failures/Malfunction		
	Failures of parts of devices	Protocols, Hardware, Software, Information, Services
	Configuration errors	Protocols, Hardware, Software, Information, Services
Outages		
	Lack of resources	Hardware, Software, Information, Services, Interconnection, Infrastructure, Human resources
	Network outages	Hardware, Software, Information, Services
Unintentional damages (accidental)		
	Information leakage/sharing	Hardware, Software, Information, Services, Interconnection
	Unintentional change of data in an information system	Protocols, Hardware, Software, Information, Services
Damage/Loss (IT assets)		
	Damage caused by a third parties	Hardware, Software, Information, Services, Interconnection, Infrastructure, Human resources
	Loss of reputation	Interconnection, Human resources

Nefarious activity/Abuse		
	Manipulation of hardware and software	Protocols, Hardware, Software, Information, Services
	Denial of service attacks (DoS/DDoS)	Hardware, Software, Information, Services
Eavesdropping /Interception/Hijacking		
	Interception compromising emissions	Protocols, Software, Information, Services
	Man in the middle/session hijacking	Software, Information, Services
Legal		
	Violations of law or regulation/breaches of legislation	Software, Information, Interconnection, Human resources
	Failure to meet contractual requirements	Ditto

Table 8: Internet threats landscape

The table 9 shows the association between agents and threats from the same source.

	Corporations	Hacktivists	Cyber criminals	Cyber terrorists	Script kiddies	Online social hackers	Employees	Nations states
Physical attacks	✓		✓	✓	_	_	✓	✓
Disasters	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
Failures/ Malfunctions	✓	_	_	_	_	_	✓	_
Outages	✓	✓	✓	✓	✓	✓	✓	✓
Unintentional damages	✓	_	_	_	_	_	✓	_
Damage/Loss	✓	✓	✓	✓	✓	✓	✓	✓
Nefarious activity/Abuse	✓	✓	✓	✓	✓	✓	✓	✓
Eavesdropping/ Interception/ Hijacking	✓	✓	✓	✓	✓	✓	✓	✓
Legal	✓	✓	✓	✓	✓	✓	✓	✓

Table 9: Involvement of threat agents in threats

Identifying top risks to Component infrastructure supports the determination and prioritization of resilience solutions and projects. As components conduct and coordinate assessments of risk to essential functions, they can leverage other potential sources of risk assessment information that may provide useful information. Other sources may include the ENISA Threat Landscape (ETL) annual report on the state of the cybersecurity threat landscape. [34]

By identifying and prioritizing those threats, the ecosystem can make smarter decisions and manage the risks through appropriate planning, mitigation strategies, and developing needed capabilities. The steps of the Threat, Hazard Identification and Risk Assessment (THIRA) process entail:

1. **Identify Threats and Hazards of Concern:** Based on a combination of experience, forecasting, subject matter expertise, and other available resources, identify a list of the threats and hazards of primary concern to the ecosystem or asset.
2. **Give the Threats and Hazards Context:** Describe the threats and hazards of concern, showing how they may affect the ecosystem or asset.
3. **Establish Capability Targets:** Assess each threat and hazard in context to develop a specific capability target for each core capability. The capability target defines success for the capability. The five core capability areas include: planning, organization, equipment, training, and exercises.

4. **Apply the Results**: For each core capability, estimate the resources required to achieve the capability targets through the use of ecosystem assets and mutual aid, while also considering preparedness activities, including mitigation opportunities.

There is also an alternative effects-based approach that is hazard diagnostic, wherein you begin with a disruptive event that will have an impact on facility operations (e.g., loss of power, loss of communications). Once you have identified all the ways in which facility functions could be disrupted, you then work backwards to consider what events could cause those disruptions—the hazard scenarios. In this case, you mainly plan for dealing with the impact of the disruption, with some unique tailoring as needed to account for the one or many hazards that might cause it. This process often identifies disruptive scenarios, such as labour strikes at ports that disrupt operations, fuel shortages, and supply chain disruptions. These types of hazards do not often come to mind when people think about typical hazards, such as storms, fires, and cyberattacks.

3.6.2 Identify Vulnerabilities and Risks

Vulnerabilities are defined as component and site exposure to the possibility of harm. A general rule of thumb for remembering the differences between hazards and vulnerabilities is that hazards are typically not within a component's control, but vulnerabilities could be within a component's control.

The vulnerabilities that arise in the risk assessment are the starting point for identifying resilience solutions. Examples of vulnerabilities that may occur at a site include: a single electricity supply to a facility; a single point of access to a facility such as one road or bridge, Single point of access to a network, IXP, etc.

3.6.3 Service level

In the definition of resilience, the term "**provide"** represents the delivery of the network service at an acceptable level given normal operational parameters. The term **"maintain"** represents ensuring that the network will provide service at the normal condition for a maximum fraction of operating time, particularly in the light of faults and challenges.
It refers to the goal of delivering an acceptable or highest possible network service level, by taking measures to prevent challenges, minimizing their possible service impact, and rapidly restoring the network service level in case it is degraded.

3.6.4 Acceptable level of service and operation

The aim of resilient networks and services is to provide an acceptable level of service (and be able to maintain that level of service) when faults are occurring in the network, or the level of service is being put at risk by challenges (for example: the incoming network traffic exceeds the traffic rate the service can handle). Therefore, it is fundamental to specify the acceptable or desired level of service and align any measurement practices with such definition.

In the domain of telecommunications and networking, acceptable service levels are typically defined in a Service Level Specification (SLS), often as part of a Service Level Agreement (SLA) between the network service provider and customer.

The SLA describes the service levels that are acceptable to the customer. What is acceptable can also be determined by regulatory requirements and standards set out for the operators (some of these regulatory requirements and standards implicitly target societal acceptance of the network service level).

Network Service level Agreements and Specifications are commonly defined in terms of quantitative service parameters such as service availability, throughput (bandwidth), latency (average round trip time), packet loss, jitter (packet delay variation), etc. These availability and service quality elements express whether the network service is actually delivered and can be measured.

It should be noted that acceptable service level definitions can also be refined based on further classification of the service disruption impact. More specifically, the significance of the service impact can be quantified using a number of impact metrics such as the extent of the network impacted in terms of users, services or network portions or in terms of recovery times.

The Service Level Agreement (SLA) with customers or other parties really determines the level of network service resilience which will be built into the network (the SLA defines, among others, network service parameters, such as a maximum guaranteed delay or a minimum guaranteed bandwidth). The SLA also requires proper business continuity management to ensure that the network service is delivered to the service consumer according to the SLA parameters, even when facing network faults.

Impact measures can also be incorporated in service level specifications in order to provide more fine-grained control over the specification. For example, an acceptable level of service for Internet connections consumers could contain the following thresholds:

- 90% of all the service users have an availability of 99,99% measured on a yearly basis. Assuming a population of 1 million service users, this implies that the service provider must provide 900.000 users with Internet access that can go below the acceptable service level for 0.87 hours yearly for each user.

- 95% of all the service users have an availability of 99% measured on a yearly basis. Assuming a population of 1 million service users, this implies that the service provider must provide 950.000 users with Internet access that can go below the acceptable service level for 3.62 days yearly for each user.

Whether or not these fine-grained specifications are an attainable and measurable quantity depends largely on the type of service. For example, while a cellular provider can approximate the number of service users by the region that is out of service, it is very difficult for a housing provider of an externally facing web application to foresee how many users may or may not experience.
The acceptable levels of service can be looked at through "dependability"," security" and "performability" dimensions in the various phases of operation: preparedness, Service delivery and Recovery.

Below we propose the following measures of the "service delivery" and "recovery" mode to be used by implementing this framework, either during building or measuring resilience.

Dependability

- **Operational Mean Time Between Failure (MTBF)**

Operational MTBF is an indicator of reliability for fault tolerant ICT systems. Operational MTBF expresses the expected time between consecutive failures in an ICT system. It is important to note how a failure is defined: **Failure is defined as the transition from the normal service level to impaired or even unacceptable service level.** Operational MTBF is reported as an absolute value in hours.
Target values depend highly on the criticality of the service and the topology of the system. If a service is very critical, the operational MTBF targets will be higher compared to a normal service. As an example, the operational MTBF target for an Internet service for large corporations will be higher than the target for Internet service for residential customers.

- **Operational Availability**

Operational availability is defined as the percentage of time an ICT system is available to end users. The goal of the metric is to indicate the observed availability, which is the probability that an ICT system is not failed or undergoing a repair action when it is requested for use. The operational availability is expressed as a percentage. Operational availability is measured in a predefined time window. For example: 99,9% operational availability measured on a yearly basis allows for a consecutive unavailability of 8,72 hours whereas the same operational availability in a measurement window of one (01) month would only allow for 0,724 hours of consecutive service unavailability.

- **Mean Down Time**

Mean down time (MDT) is the average time that an ICT system is non-operational. This measure indicates the average time between the occurrence of a failure to the restoration of the normal service level. A higher value would indicate that a failure is likely to impact the service for a longer time, hence indicating a lower resilience (lower resistance to faults and challenges). MDT is expressed as an absolute value in seconds or hours.

Security

- **Incident Rate**

The incident rate measure indicates the number of security incidents that occur in each time period from selected incident categories. The incident rate indicates the number of detected security incidents the organisation has experienced during the measure time period. In combination with other measures, this can indicate the level of threats, the effectiveness of security controls and/or incident detection capabilities.
A target should be set the variation of incidents that occur. Incident rate values should trend lower over time – assuming perfect detection capabilities. The value of "0" indicates hypothetical perfect security since there were no security incidents.

- **Mean time for Incident Recovery**

Mean Time to Incident Recovery (MTIR) characterizes the ability of the organisation to return to a normal state of operations. This is measured by the average elapse time between when the incident occurred to when the organisation recovered from the incident. Mean time to incident recovery measures the effectiveness of the organisation to recovery

from security incidents. The sooner the organisation can recover from a security incident, the less impact the incident will have on the overall organisation. Unit of the metric is a time over the number of incidents, for example hours/incident.
Depending on the sector, components or site, some extra measures may be required in quantifying systems dependability and tolerance to fault and challenge.

Table 10 shows the measures per component. It is expected that this table will be used as template when setting acceptable level of services and operations.

Focus area	Component	Dependability	Target	Security	Target
ISP Resilience	Links	Operational MTBF		Incident Rate	
		Operational Availability		Mean Time to Incident Recovery	
		Mean Down Time			
	QoS/QoE	N/A		N/A	
	DNS Resolver	Operational MTBF		Incident Rate	
		Operational Availability		Mean Time to Incident Recovery	
		Mean Down Time			
Critical infrastructure resilience	Cable system	Operational MTBF		Incident Rate	
		Operational Availability		Mean Time to Incident Recovery	
		Mean Down Time			
	Power infrastructure	Operational MTBF		Incident Rate	
		Operational Availability		Mean Time to Incident Recovery	
		Mean Down Time			
	IXP	Operational MTBF		Incident Rate	
		Operational Availability		Mean Time to Incident Recovery	
		Mean Down Time			
	ccTLD	Operational MTBF		Incident Rate	
		Operational Availability		Mean Time to Incident Recovery	
		Mean Down Time			
Market resilience	Affordability	N/A			
	Market readiness	N/A			

Table 10: Fault tolerance measures template

Table 11 presents performability measures also in a template format.

Focus area	Component	Performability (QoS/QoE)[35]	Target
ISP Resilience	Links	- Delay variation (Jitter)	
		- Packet loss	
		- Bandwidth (average)	
	QoS/QoE	- Median upload throughput	
		- Median download throughput	
		- Median jitter	
		- Median latency	
	DNS Resolver	- UDP name resolution time for 95%	
		- TCP Name resolution time for 95%	
Critical infrastructure resilience	Cable system	- Transmission network length (Route kilometres)	
		- Equipped capacity vs design capacity	
		- Percentage of the population within 10km of a fibre connection point	
		- Mobile Network coverage includes 2G/3G/4G/5G	
		- Spectrum allocation	
	Power Infrastructure	- Electricity supply (connected vs demand)	
		- Electrification –Total population (%)	
		- Electricity Consumption	
		- Transmission-distribution losses	
	IXP	- Ratio of ASes peering at IXPs vs allocated ASes in a country.	
		- Percentage of traffic exchanged via IXP	
	ccTLD	- UDP query time for 95% of requests	
		- TCP query time for 95% of requests	
		- Whois query time	
		- Domain name registration time	
		- Domain name count	
Market resilience	Affordability	-Market concentration	
		- System cost per user; cost per service area; cost per megabit	
		- Data affordability	
		- Terminal affordability	
		- Taxation	
	Market readiness	- Basic skills	
		- Local relevance (contents & apps)	
		- Online security	

Table 11: Performability measures template

When assessing overall liabilities from hazards, threats, risks, and vulnerabilities, consideration should be given to the sustainability of potential solutions (e.g., renewable backup power vs. fossil fuel generation); duration of outage, which can be unique to each site or mission; and the interdependencies among the focus areas. For instance, hazards and threats can impact the delivery of resources to conduct the mission, such as interruption of power supplies.

The component needs to determine what are the acceptable level for interruption of the specific mission essential functions performed at its sites. These targets can be used as a basis for determining how vulnerable is the site to exceed the threshold during a hazard event and what resilience solutions and projects might be necessary to ensure the actual downtime will not exceed the thresholds.

While it may be desirable to set high expectations for resilience or set the same requirements for every country or provider, care should be taken considering the identified core issues currently affecting the resilience of the Internet in Africa presented referred to in part 1, "ISSUES AFFECTING INTERNET RESILIENCE IN AFRICAN COUNTRIES". No single standard can apply to all. Enterprise customers 'resilience requirements may be different from for end-users.

In a particular country, the situation may not be the same for rural regions compared to the urban regions. While an operational availability of 99,99% may be desirable un urban regions, this may not be achievable in rural areas where useful target may be of operational availability of 99% or lower. Same applies to other measures.

Recommendation ITU-T L.1700[36]discussed and set some requirements and framework for low-cost sustainable telecommunications infrastructure for rural communications in developing countries.

3.7 Step 5: Identify Resilience Gaps and Determine Resilience Readiness Solutions

Step 5 aims to help with the identification of the difference, or gap, between the current baseline conditions of a component and the conditions that would make it sufficiently resilient to maintain service level during and after a hazard or threat event, as well as during normal operations.

Based on the identified gaps, the component should determine the solutions and projects necessary to close the gaps. When determining resilience solutions, Components should consider the resilience qualities of infrastructure discussed in Section 3.0, **namely robustness, redundancy, resourcefulness, and rapid recovery**.

Risk management requires leveraging resources to address the most critical infrastructure assets that are also the most vulnerable and that have the greatest threat exposure. As Steps 1 through 4 of the Resilience Framework process are completed and mission essential functions and assets are defined and prioritized based on their levels of criticality and their associated liabilities, the gaps in resilience readiness of these assets should start to become apparent.

Note

The risk management should follow or aligns with the risk management in national cybersecurity, the defined risk-management approach and abide to the sectorial cybersecurity risk profiles. Determining the resilience readiness solutions should seek guidance from existing national critical information infrastructures and services protection's plans.

3.8 Step 6: Integrate Resilience Readiness Solutions

Step 6 will close the gaps between the current state and a resilient state of critical assets to ensure continuous performance of critical mission essential functions as needed during times of hazard or threat disruption, as well as during normal operations. While prioritizing individual resilience solutions and projects for greatest impact and effectiveness, one may consider what is achievable and the following attributes:

- Responsiveness to the scale and impact of likely hazards and vulnerabilities;
- Ability to meet identified performance goals for resilient infrastructure systems and critical operations;
- Ability to address and strengthen interdependent infrastructure systems;
- Co-location opportunities to further the mission set;
- How to obtain and execute funding to implement capital projects or institutionalize resilience into existing activities;
- Administrative capacity necessary for implementation;
- Data and analysis required for implementation; and
- Implementation plan requirements.

A successful approach to resilience must integrate resilience considerations into normal site operations and identify opportunities to implement resilience projects as part of capital improvements. Often, resilience considerations may be incorporated into capital projects at little or no additional cost.

Note

The integration of Resilience Readiness Solutions should follow when applicable, the national cybersecurity crisis management plans or national emergency telecommunication plans.

3.8.1 Financing Resilience-Driven Projects

Once potential resilience readiness solutions have been identified and prioritized, these solutions should be integrated to the maximum extent feasible into the component's project life cycle planning and budgeting. Financing a resilience project involves identifying feasible funding and procurement strategies. To address this, especially in low-income countries financial solutions including grant assistance, Official Development Assistance (ODA) loans and universal service obligations may be needed to enable services to be extended to all people and help fund resilience projects. Where feasible, components should consider costs sharing options such as co-locations, infrastructure sharing, roaming, etc. Resilience may conflict with affordability and necessary actions should be taken to guarantee that good resilience is achieved without impact of service uptake and usage.

4 COMPONENT PLANS FOR RESILIENCE

Each Component identified in this internet resilience framework should be required to prepare its plan for Resilience, due one year after issuance of compulsory Resilience Framework document from this model by the respective authorities.
Thereafter, Components should annually review their plans for Resilience and update them accordingly. The Plan for Resilience should be consistent with the Component's Continuity Plan and Reconstitution Plan.

It is understood that Components are diverse in mission and organization, and each faces a set of unique challenges. Therefore, each Component's plan for Resilience will reflect its own mission, processes, geography, and capacity.

However, these plans should show the prioritization of Component critical mission assets, solutions and projects required to make these assets resilient, the priorities for funding to implement these resilience solutions and projects, and overall pathways for implementing the resilience solutions and projects for a better Internet.

PART 3: DEMONSTRATING RESILIENCE

1 INTRODUCTION

Components will be required to implement resilience into the lifecycle of their operations, continuously review, evaluate, and improve knowledge base on vulnerabilities, risks, processes, etc. Despite this, some vulnerabilities, gaps, and impacts that may not visible and addressed by that government, regulators and infrastructure operators until a disruption occurs. Covid-19 pandemic revealed many issues and shows limitations of several key infrastructures which had claimed high resilience.
It is therefore important that resilience of critical infrastructure be monitored closely by running stress tests and measuring performances.

2 STRESS TESTS

Stress testing, by simulating how systems would react to shocks and stresses, can help operators identify and address vulnerabilities in advance of an event. It can also help infrastructure operators test their decision-making processes, preparing operators for disruptions other than those in the scenarios set out in the stress tests.

To ensure the stress tests address resilience issues, it is important that realistic scopes and scenarios for stress tests are set out. Guidance for developing bespoke tests where necessary should also be provided. Outcomes of the tests should be scrutinised and plans to remedy any vulnerabilities identified required.

Best practices sharing across sectors should be encouraged. The stress tests can support regulators and operators and provide better and real overall understanding of the resilience. Regulators can use the stress tests to develop an overview of resilience in their sector and assess progress.

3 MEASURING RESILIENCE

3.1 Measurements

In section 3.6.4 (acceptable level of service and operation), some measures were identified as key indicators of service level. Target values for these measures will be set and component's performance toward these values can be measured. Local and competent authorities shall set the targets and compliance requirements to the obligated parties. As an example, in Togolese Republic, the Minister of the digital economy and digital transformation has set the QoS indicators and their targets for 2G, 3G, 4G operators [6]. At annexe 1, section 6 of the decree, the indicators and targets for network infrastructure are defined as below:

Code	Indicator	Definition	Target (2G, 3G et 4G)
DR1	Number of unavailability of a base station	Number of times the same base station remained unavailable for a period of at least one hour during the last 30 days.	≤ 2
DR2	Base station downtime	Unavailability time per day for the same base station regardless of where it is located on the national territory.	≤ 3H

Table 12: Example of targets for network infrastructure

These indicators and targets set the parameters for monthly "Operational MTBF" and daily "Operational Availability".

These measures are not exhaustive, and depending on sectors, activity and evolutions, other measures may be needed. They should be developed in collaboration with the stakeholders and follow measure and measurement development process.

Based on best practices on the security and resilience measurement, we propose the template presented at table 13 to be used when defining and implementing measures.

Measure name	Standard or assigned name, used to reference the measure.
ID(Identifier)	Unique Identifier to track and sort measure at regional, sub-regional, country, and organizational level.
Domain	Statement of which dimension of the resilience, the measure belongs to: dependability, security or performability
Phase	Statement of which phase of the resilience process, the measure belongs to: preparedness, service Delivery or recovery
Type	Statement of whether the measure is implementation, efficiency, effectiveness or impact
Responsible parties	Information Owner, Information Collector, Information Customer
Source	Indication of the literature from which the matric was adopted.
Description	Description of the metric, explaining the concept / attribute under measurement and the measures from which the metric is derived.
Objective	Description of the resilience measurement goal. What value does it bring to measure the metric? What conclusions could be derived from the metric? What purpose does the metric serve?
Measurement method	Description of the base measures and units of measurement, and the formula to calculate the numeric metric value of the metric. The formula consists of a mathematical function of two (02) or more measures. The measurement method for these measures needs to be accurately described as well, in order to assure repeatability and comparability of metrics.
Frequency	Number of times per period that the data will be collected in order to measure the metric. The frequency will be dependent on several factors, including the rate of change in the measure attribute, compliance & reporting requirements, business specifics, etc.
Target values	Threshold for an acceptable value of the metric. The target value can be part of, for example, a service level agreement or a performance goal in Capability Maturity Model.
Reporting format	Description of an example reporting format to visually or verbally best characterize the metric.
Data source	Location of data to be used in calculating the measure

Table 13: Resilience baseline measure template

Tables 14 to 18 present some of the recommended measures using that template.

Metric name	Operational Mean Time Between Failures (MTBF)
ID	**001/Internet/Resilience/MTBF**
Responsible parties	**Office of the technical department, of the Chief Technology Officer, Audit, Compliance**
Domain	Dependability
Phase	Service Delivery
Type	Effectiveness
Source	This metric definition is adopted from the IEEE Standard Glossary of Software Engineering Terminology
Description	Operational MTBF is a basic indicator of reliability for fault tolerant ICT systems. For obvious reasons the ability of the ICT system to recover from failures is a prerequisite here. Operational MTBF expresses the expected time between consecutive failures in an ICT system. It is important to note how a failure is defined: We define a failure as the transition from the normal service level to impaired or even unacceptable service level.
Objective	This metric indicates the predicted time between different failures of an ICT system during operation.
Measurement method	Operational MTBF is defined as the mean value of the length of time between consecutive failures, computed as the ratio of the cumulative observed time to the number of failures under stated conditions, for a stated period of time in the life of an item. It is calculated as the sum of the operational periods divided by the number of observed failures (the operational period is defined as the difference in time between the moment the service starts operating at the normal service level until the moment the service fails). Note that the duration of the failure has no impact on the metric value. $$OperationalMTBF = \frac{\sum_i operational\ periods_i}{number\ of\ failures}$$ Operational MTBF is reported as an absolute value in hours.
Frequency	Operational MTBF should be monitored on real-time basis.
Target values	Target values depend highly on the criticality of the service and the topology of the system. For example: If a service is very critical, the operational MTBF targets will be higher compared to a normal service. As an example, the operational MTBF target for an Internet service for large corporations will be higher than the target for Internet service for residential customers.
Reporting format	Operational MTBF is reported as an absolute time value versus the target value for different services.
Data source	**Operation and Maintenance Center, Network Operation Center (NOC)**

Table 14: Operational MTBF

Measure name	Operational Availability
ID	**002/Internet/Resilience/Availability**
Responsible parties	**Office of the technical department, of the Chief Technology Officer, Audit, Compliance**
Domain	Dependability
Phase	Service Delivery
Type	Effectiveness
Source	This metric definition is based on the definitions from: Complete guide to security and privacy metrics: measuring regulatory compliance, operational resilience, and ROI / Debra S. Herrmann.
Description	Operational availability is defined as the percentage of time an ICT system is available to end users.
Objective	The goal of the metric is to indicate the observed availability, which is the probability that an ICT system is not failed or undergoing a repair action when it is requested for use.
Measurement method	Operational availability is calculated as the percentage of the mean time that an ICT system is running at the normal service level over the total time. Two intermediate concepts are introduced, needed for the calculation of the operational availability terms: • Mean Time Between Maintenance Actions (MTBMA): The mean time between maintenance actions (corrective and preventive maintenance). • Mean Down Time (MDT): The mean time that an ICT system is non-operational, including preventive/corrective maintenance actions. A more extended MDT definition can be found in 1.1.1.27. $Operational\ availability = \frac{MTBMA}{MTBMA+MDT}$ The unit of MTBMA and MDT should be the same (hours, seconds …) while the operational availability Is expressed as a percentage.
Frequency	Operational availability should be monitored on real-time basis
Target values	Target values for operational availability are impossible to specify for a generic ICT system. They are specified in the service level specification of the service provider. The difference between the operational availability and the availability as specified in service level specification should be monitored
Reporting format	Operational availability is measured in a predefined time window. For example: 99,9% operational availability measured on a yearly basis allows for a consecutive unavailability of 8,76 hours whereas the same operational availability in a measurement window of 1 month would only allow for 0,744 hours of consecutive service unavailability. Availability reporting is done in function of the measurement window (e.g. reporting of the availability per month for all months of the year).
Data source	**Operation and Maintenance Center, Network Operation Center (NOC)**

Table 15: Operational Availability

Measure name	Mean Down Time
ID	**003/Internet/Resilience/MDT**
Responsible parties	**Office of the technical department, of the Chief Technology Officer, Audit, Compliance**
Domain	Dependability
Phase	Recovery
Type	Effectiveness
Source	This metric definition is based on IEEE Standard Computer Dictionary: A Compilation of IEEE Standard Computer Glossaries
Description	Mean down time (MDT) is the average time that an ICT system is non-operational. This includes all non-operational time associated with repair, corrective and preventive maintenance and includes any logistical or administrative delays. The difference between MDT and MTTR (mean time to repair) is that MDT includes any and all delays involved; MTTR looks solely at repair time.
Objective	This metric indicates the average time between the occurrence of a failure to the restoration of the normal service level. A higher value would indicate that a failure is likely to impact the service for a longer time, hence indicating a lower resilience (lower resistance to faults and challenges).
Measurement method	MDT is the total non-operational time divided by the total number of outages during a given period of time. $$MDT = \frac{\sum_i (Non\ Operational\ Time_i)}{Number\ of\ outages}$$ MDT is expressed as an absolute value in seconds or hours.
Frequency	Weekly, Monthly, Quarterly, Annually
Target values	No specific target values can be given, as this is highly specific per organisation.
Reporting format	Reporting of the Mean down time should be per category and in a time-series plot.
Data source	**Operation and Maintenance Center, Network Operation Center (NOC)**

Table 16: Mean Down Time

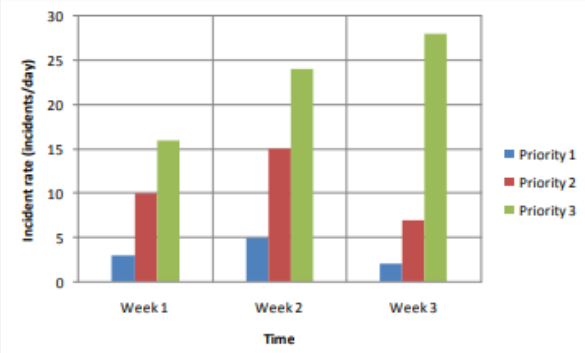
Metric name	Incident Rate
ID	**004/Internet/Resilience/IR**
Responsible parties	**Chief Security Officer (CSO) / Security manager, Audit, Compliance**
Domain	Security
Phase	Service delivery
Type	Effectiveness
Source	This metric is adopted from 'The CIS security metrics - Consensus Metric Definitions v1.0.0'.
Description	The incident rate metric measures the number of security incidents that occur in a given time period from selected incident categories.
Objective	The incident rate indicates the number of detected security incidents the organisation has experienced during the metric time period. In combination with other metrics, this can indicate the level of threats, the effectiveness of security controls and/or incident detection capabilities.
Measurement method	To calculate the incident rate metric, the number of security incidents in a given time period are counted, additional grouping could occur per incident category or organisational departments for example. $Incident\ Rate = \frac{Amount\ of\ incidents\ per\ category}{Length\ of\ time\ window}$ The time window is expressed as an absolute unit of time (e.g. hours or days) while the number of incidents is an absolute number, indicating how many incidents have occurred in the past time window. Note: In a network of ICT security systems, it is possible that each security device reports an attack at the very same time, although only one attack is ongoing (for example: an incident on the outer firewall and an incident on the IDS system can indicate the very same event). This can result in a skewed view of the amount of incidents that occurs on the network.
Frequency	The incident management and follow-up should happen on a continuous basis and at least daily.
Target values	No specific target can be set, as the metric will also depend on the categories of incidents that are taken into account in this measure. A target should be set the variation of incidents that occur (to trigger alarms). Incident rate values should trend lower over time – assuming perfect detection capabilities. The value of "0" indicates hypothetical perfect security since there were no security incidents. Because of the lack of experiential data from the field, no consensus on range of acceptable goal values for Incident Rate exists.
Reporting format	Reporting of the incident rate should be per category and in a time-series plot. Example of a reporting format with an incident categorization per incident priority: 
Data source	**Network Operation Center, Security Operation Center**

Table 17: Incident Rate

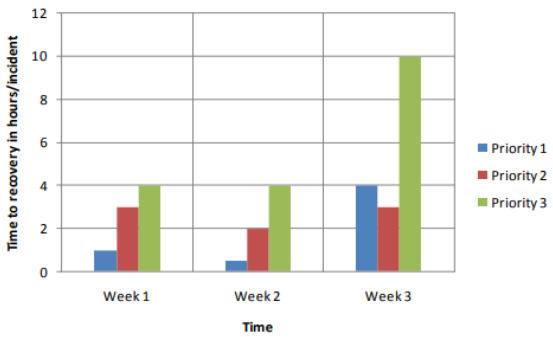
Measure name	Mean Time to Incident Recovery
ID	**005/Internet/Resilience/MTIR**
Responsible parties	**Chief Security Officer (CSO) / Security manager, Audit, Compliance**
Domain	Security
Phase	Recovery
Type	Effectiveness
Source	This metric is adopted from 'The CIS security metrics - Consensus Metric Definitions v1.0.0'
Description	Mean time to incident recovery (MTIR) characterizes the ability of the organisation to return to a normal state of operations. This is measured by the average elapse time between when the incident occurred to when the organisation recovered from the incident.
Objective	Mean time to incident recovery measures the effectiveness of the organisation to recovery from security incidents. The sooner the organisation can recover from a security incident, the less impact the incident will have on the overall organisation.
Measurement method	MTTIR is measured by dividing the average elapsed time between the incident occurrence and the recovery to normal service level over the number of incidents. This calculation can be averaged over a time period $$MTTIR = \frac{\sum_i (Date\ of\ Recovery_i - Date\ of\ Occurrence_i)}{Number\ of\ incidents}$$ Unit of the metric is a time over the number of incidents, for example hours/incident.
Frequency	Weekly, Monthly, Quarterly, Annually.
Target values	MTTIR values should trend lower over time. There is evidence the metric result will be in a range from days to weeks (2008 Verizon Data Breach Report). The value of '0' indicates hypothetical instantaneous recovery. Because of the lack of experiential data from the field, no consensus on the range of acceptable goal values for Mean Time to Incident Recovery exists.
Reporting format	Reporting of the incident recovery time should be per category and based on the hours/incident value. 
Data source	**Network Operation Center, Security Operation Center**

Table 18: Mean Time to Incident Recovery

3.2 Data collection

Plans for quantitative and qualitative data collection are required. Some data can be collected directly by any agent using a network or service. Other data can only be collected from inside by owners of the infrastructures.

Protocols for data collection, submission and treatment must be defined. Protocols may specify data collection methods, which include data from Operation and Maintenance Center, drive-test, probe-based test, or crowdsourcing, etc. Responsible parties, data sources as well as frequency and reporting format should be specified for each measure. Greater transparency in the measurement activities should be observed through consultation, openness, and trust.

Some data may require specific calculation method taking into considering the topology of measured systems, and the interdependencies between components, sites, or systems.

Most of the measures proposed in the framework model could be used within a single corporation or at a level where single and unified measurements are possible. This one is not enough when one wants to have the resilience status at different levels of abstraction. To assess the resilience status beyond the level of a single corporation, for example on sector-wide basis, on national basis or even on a continental level, aggregation and composition of measure will be required.

CONCLUSION

In the face of ongoing threats to the Internet, it is imperative that resilience is fully integrated into all phases of essential operations. Local authorities and components must deliberately plan for and implement resilience solutions to support their operations and services. This Resilience Framework model was formulated as a holistic process to meet this requirement by integrating resilience into the entire life cycle of planning and implementation in the operations of identified components to this Internet resilience framework.

Implementing the Resilience Framework process will greatly facilitate country's ability to prepare for and adapt to changing conditions and rapidly recover from disruption of normal operating conditions when and where they occur. The resulting component Plans will provide a resilience driven basis for informed and sound decision making.

ENDNOTES

1. African Telecommunications Union, Consultancy on the Development of a Model Framework document for Building Internet Resilience in Africa, **Draft report core issues affecting Internet resilience in African states**
2. National Institute of Standards and Technology at the U.S. Department of Commerce, Special Publication 800-160, Volume 2, Revision 1 (2021), **Developing Cyber-Resilient Systems**
3. ResiliNets initiative is a collaboration between the University of Kansas (US) and Lancaster University (UK) and aims to understand and progress the state of resilience and survivability in computer networks, including the Global Internet, PSTN, SCADA networks, mobile ad-hoc networks, and sensor networks, **ResiliNets Wiki**
4. The Wikipedia, **Internet**
5. African Union, (2020), **The digital transformation strategy for Africa (2020-2030)**
6. Ministère de l'économie numérique et de la transformation digitale, République Togolaise, (2022), **Arrêté N°005/MENTD/CAB portant définition des indicateurs de qualité des services mobiles 2G 3G 4G et leurs seuils**
7. Government of Kenya, (2018), **National broadband strategy 2018-2023**
8. Federal communications Commission, **Broadband Speed Guide**
9. European Commission, (2010), **A Digital Agenda for Europe**
10. The African IXP Association, **Map of Internet exchange points in Africa**
11. Ruby on Rails, (2009), **Public DNS Server List**
12. Google, **Google public DNS resolver**
13. Cloudflare docs **Cloudflare's public DNS resolver**
14. European parliament and the council of the European union, (2022), **Directive (EU) 2022/2557 on the resilience of critical entities and repealing Council Directive 2008/114/EC**
15. Council of the European union (2022), **Council Recommendation on a Union-wide coordinated approach to strengthen the resilience of critical infrastructure (Text with EEA relevance) 2023/C 20/01**
16. European Commission, (2006), **European Programme for Critical Infrastructure Protection**
17. National Infrastructure commission (2020), **study report on the resilience of the nation's economic infrastructure**
18. Electronic Communications Resilience & Response Group (2021), **Resilience Guidelines for Providers of Critical National Telecommunications Infrastructure**
19. The White House president BARACK OBAMA (2013), **Presidential Policy Directive -- Critical Infrastructure Security and Resilience**
20. Cybersecurity and Infrastructure Security Agency (CISA) **2013 National Infrastructure Protection Plan**
21. U.S. Department of Homeland Security, (2021), **DHS Resilience Framework: Providing a Roadmap for the Department in Operational Resilience and Readiness**
22. United Nations, Department of Economic and Social Affairs, (2015), **Sustainable Development Goal 9 -Build resilient infrastructure, promote inclusive and sustainable industrialization and foster innovation**
23. Global Conference on Cyber Capacity Building (2023), **Accra call for cyber resilient development**
24. African Declaration Coalition, (2013), **African declaration on internet rights and freedoms**

25. Global commission on the stability of cyberspace, (2019), **Advancing cyberstability final report**

26. International Trade Administration, U.S. Department of Commerce, **Brief Overview of the Electricity Infrastructure Sector**

27. National Institute of Standards and Technology at the U.S. Department of Commerce, Special Publication 800-34 Rev. 1, (2010), **Contingency Planning Guide for Federal Information Systems**

28. Cybersecurity & Infrastructure Security Agency, **Cyber Resilience Review (CRR)**

29. Cybersecurity and Infrastructure Security Agency, (2020), **Cyber Resilience Review (CRR) Self-assessment package**

30. ITU Telecommunication Development Sector, (2018), **Guide to Developing a National Cybersecurity Strategy**

31. International Organization for Standardization, (2024), **ISO/IEC 38500:2024 Information technology — Governance of IT for the organization**

32. International Organization for Standardization, **ISO/TS 22317:2021 Security and resilience Business continuity management systems Guidelines for business impact analysis**

33. European Union Agency for Cybersecurity, (2015), **Threat Landscape of Internet Infrastructure**

34. European Union Agency for Cybersecurity, (2023), **ENISA Threat Landscape 2023** https://www.enisa.europa.eu/topics/cyber-threats/threats-and-trends

35.

- ITU Telecommunication Development Sector, WTIM 25-27 September 2012, Bangkok, Thailand, **Broadband transmission capacity indicators**
- International Energy Agency, **Energy Statistics Data Browser**
- Association Française pour le Nommage Internet en Coopération, **Performance : resilience and service quality**
- Internet Society Pulse, **Internet Resilience**
- The GSM Association (GSMA) , **GSMA Mobile Connectivity Index, Data Set**
- Internet Health Report, **About Internet Health Report**

36. ITU Telecommunication Standardization Sector, **L.1700: Requirements and framework for low-cost sustainable telecommunications infrastructure for rural communications in developing countries**

APPENDIX

Region/Country	European Union	United Kingdom	United States of America
RESILIENCE FRAMEWORK	- Directive on the Resilience of Critical Entities, 16 January 2023. - Council Recommendation to strengthen the resilience of critical infrastructure, 8 December 2022. - European Programme for Critical Infrastructure Protection (EPCIP), 12 December 2006.	- In his October 2018 Budget Statement, the Chancellor of the Exchequer confirmed that the National Infrastructure Commission would be examining the resilience of the UK's infrastructure. - In the final report of the study – Anticipate, react, recover – Resilient infrastructure systems (28 May 2020) – the Commission concludes that there is a need for a new framework for resilience which **anticipates** future shocks and stresses; improves actions to **resist**, **absorb** and **recover** from them by testing for vulnerabilities; values resilience properly; and drives adaptation before it is too late. - The Electronic Communications Resilience & Response Group (EC-RRG) provides some Resilience Guidelines for Providers of Critical National Telecommunications, 2021.	- The Presidential Policy Directive (PPD) on Critical Infrastructure Security and Resilience advances a national unity of effort to strengthen and maintain secure, functioning, and resilient critical infrastructure, February 12, 2013 . - The National Infrastructure Protection Plan (NIPP 2013) meets the requirements of Presidential Policy Directive (PPD) on Critical Infrastructure Security and Resilience, signed in February 2013. - The Department of Homeland Security (DHS)'s Resilience Framework focuses on four key critical infrastructure areas where the Framework process is applied, 13 August 2018.

SECTORS/NCI	Eleven sectors: • Energy • Transport • Banking • Financial market infrastructure • Health, • Drinking water • Wastewater • **Digital infrastructure** • Public administration • Space • Production, processing, and distribution of food Digital infrastructure: - Providers of Internet exchange points (IXPs) - DNS service providers - Top-level-domain name registries - Providers of cloud computing services - Providers of data centre services - Providers of content delivery networks - Trust service providers - Providers of public electronic communications networks - Providers of electronic communications services	Thirteen national infrastructure sectors. • Chemicals • Civil Nuclear • **Communications** • Defence • Emergency Services • Energy • Finance • Food • Government • Health • Space • Transport • Water	Sixteen critical infrastructure sectors. • Chemical • Commercial Facilities • **Communications** • Critical Manufacturing • Dams • Defense Industrial Base • Emergency Services • Energy • Financial Services • Food and Agriculture • Government Facilities • Healthcare and Public Health • **Information Technology** • Nuclear Reactors, Materials, and Waste • Transportation Systems • Water and Wastewater Systems Focus areas for (DHS)'s Resilience Framework : - Energy and Water, - Facilities, - **Information and Communication, Technology,** - Transportation.

Table 19: Case studies comparative summary

African Telecommunications Union

Westlands Office Park, Acacia House, 1st Floor

P. O Box 35282 – 00200 Nairobi, Kenya

Tel: +254 722 203132

Email: sg@atuuat.africa

Website: www.atuuat.africa

*****