Preparedness for Cybersecurity

The Bhutan Experience

Kinley Zam, SAI Bhutan

AGENDA

The Bhutan Experience

ABOUT THE AUDIT

- Audit Objectives
- Audit Approach
- Audit Methodology

INTRODUCTION

- Rationale
- Cybersecurity in Bhutan

CHALLENGES AND ISSUES

- Audit Findings

RECOMMENDATIONS

- Address challenges

CONCLUSION

- Positive Changes

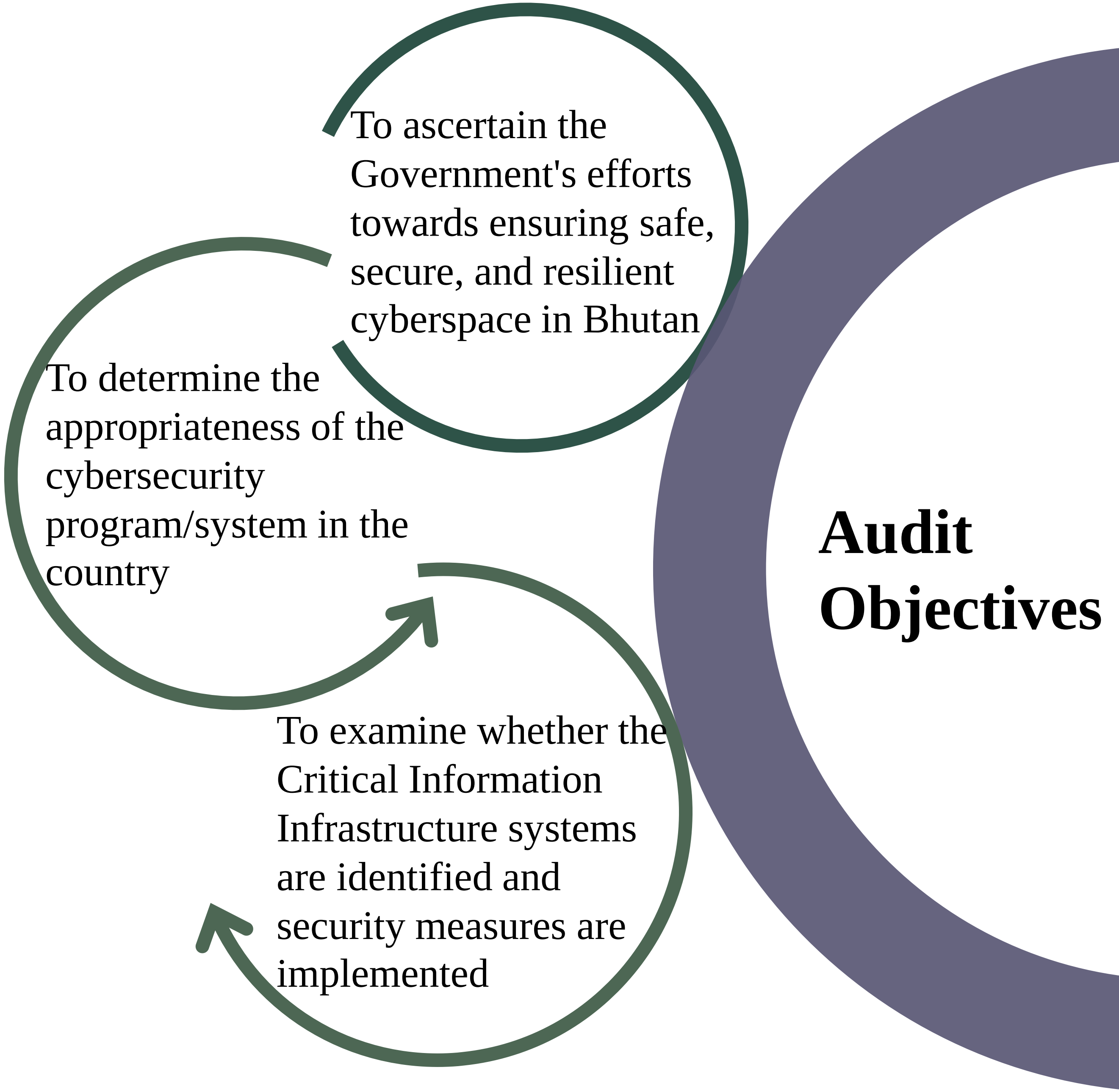
ABOUT THE AUDIT

Mandate

Article 25 of the Constitution of the Kingdom of Bhutan to audit and report on the economy, efficiency, and effectiveness in the use of public resources.

- International Standards of Supreme Audit Institutions on Performance Auditing (ISSAI 300)
- Performance Audit Guidelines 2019

Audit Standards



Audit Objectives

To ascertain the Government's efforts towards ensuring safe, secure, and resilient cyberspace in Bhutan

To determine the appropriateness of the cybersecurity program/system in the country

To examine whether the Critical Information Infrastructure systems are identified and security measures are implemented

ABOUT THE AUDIT

AUDIT SCOPE

Period covered by the audit

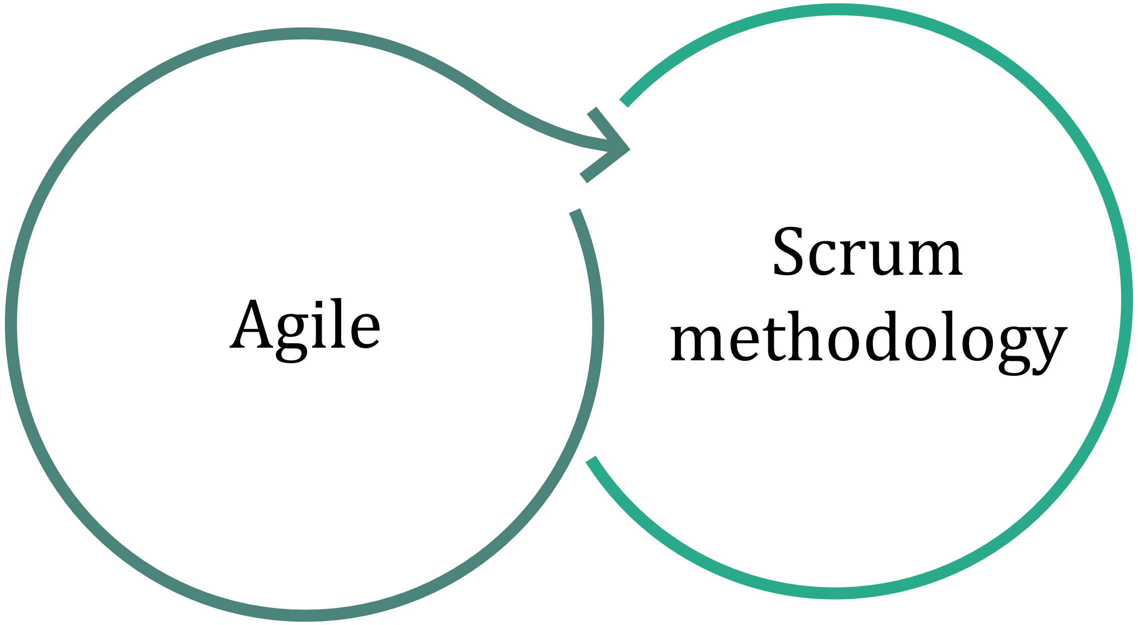
April, 2016

December, 2022

Thrust Areas

1. Legal and Regulatory Framework
2. Institutional Framework
3. Cybersecurity Governance
4. Capacity Building and Awareness
5. Incident Handling Mechanism

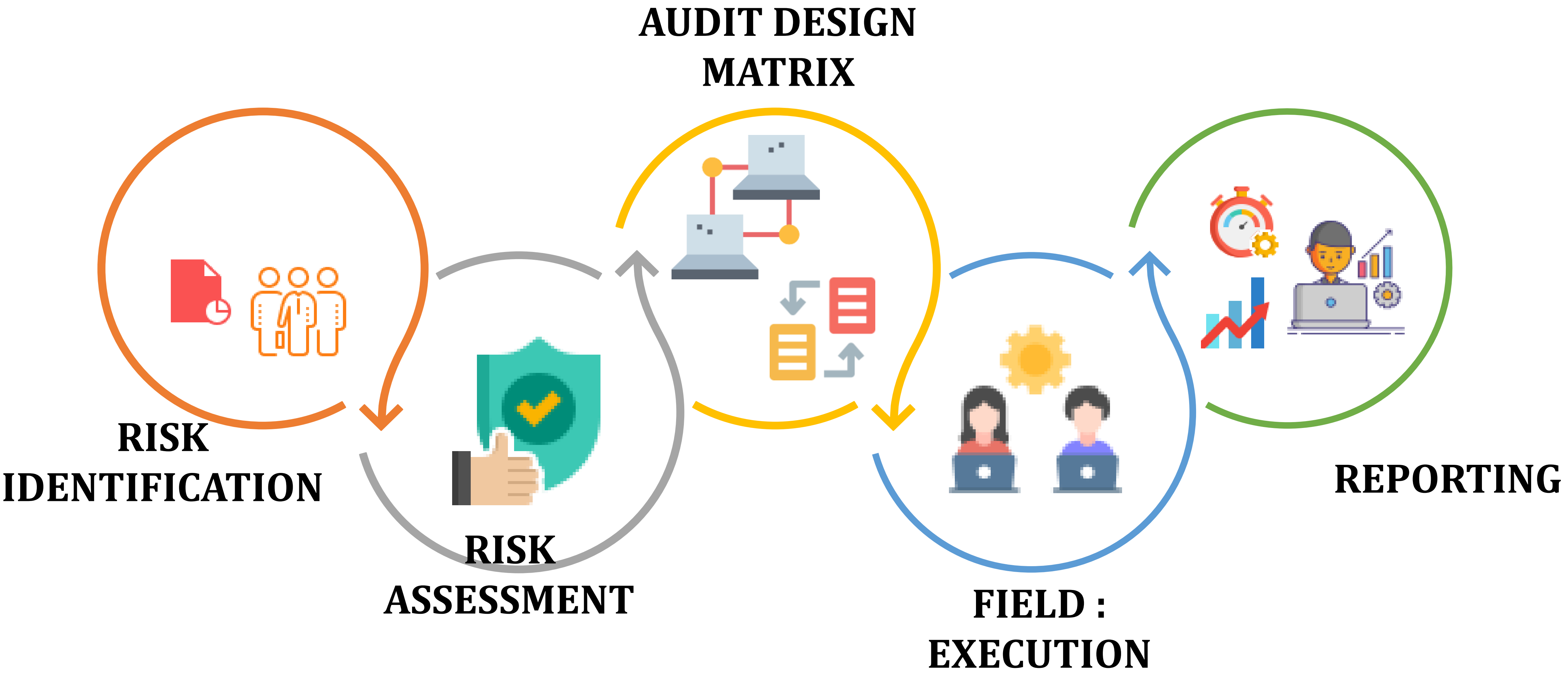
Audit Methodology



Agile

Scrum methodology

Audit Methodology



AUDIT DESIGN MATRIX

RISK IDENTIFICATION

RISK ASSESSMENT

FIELD : EXECUTION

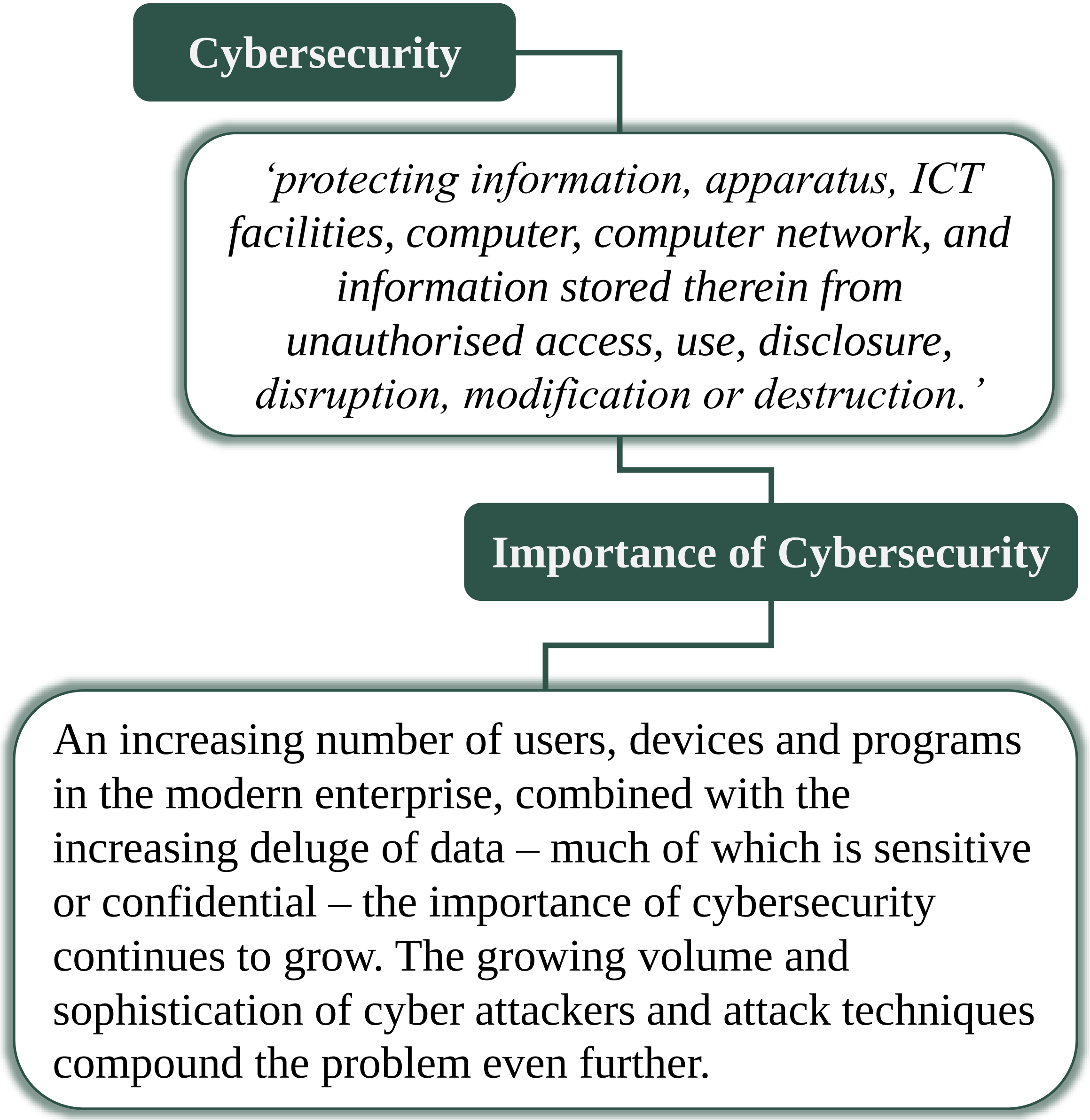
REPORTING

Sprint – 3 weeks

INTRODUCTION

RATIONALE

1. Nation’s Critical Information Infrastructure (CII)
2. Major ICT initiatives and investments
3. Increased digital usage due to the pandemic
4. Low capabilities
5. Top management attitude towards cybersecurity
6. Low awareness of cybersecurity amongst Bhutanese
7. Recent cyberattacks
8. Disinformation
9. Limited cybersecurity professionals



Cybersecurity

‘protecting information, apparatus, ICT facilities, computer, computer network, and information stored therein from unauthorised access, use, disclosure, disruption, modification or destruction.’

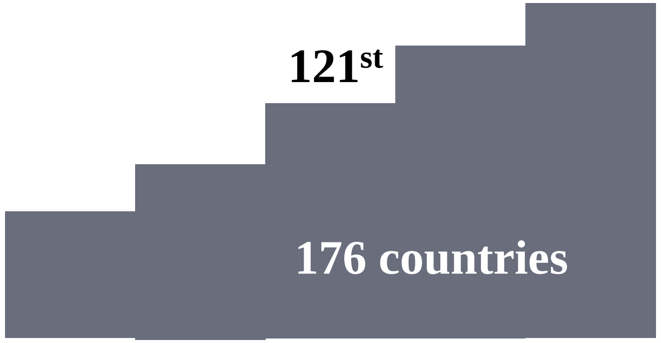
Importance of Cybersecurity

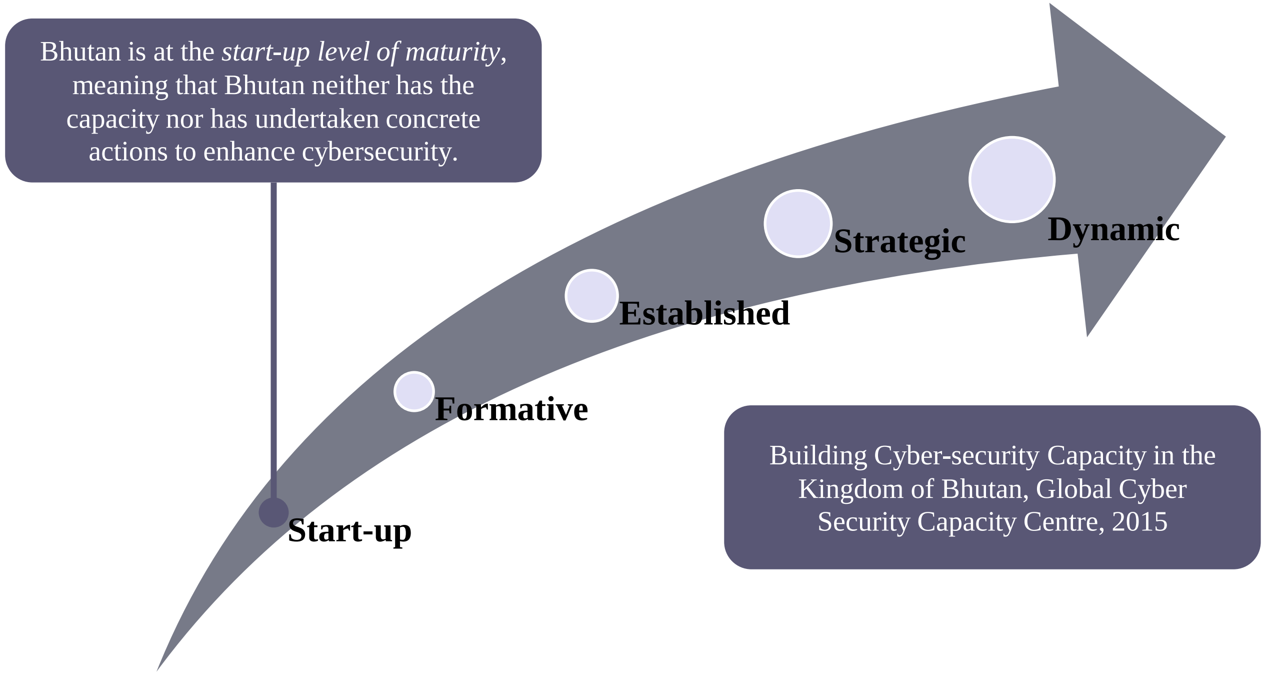
An increasing number of users, devices and programs in the modern enterprise, combined with the increasing deluge of data – much of which is sensitive or confidential – the importance of cybersecurity continues to grow. The growing volume and sophistication of cyber attackers and attack techniques compound the problem even further.

INTRODUCTION

CYBERSECURITY IN BHUTAN

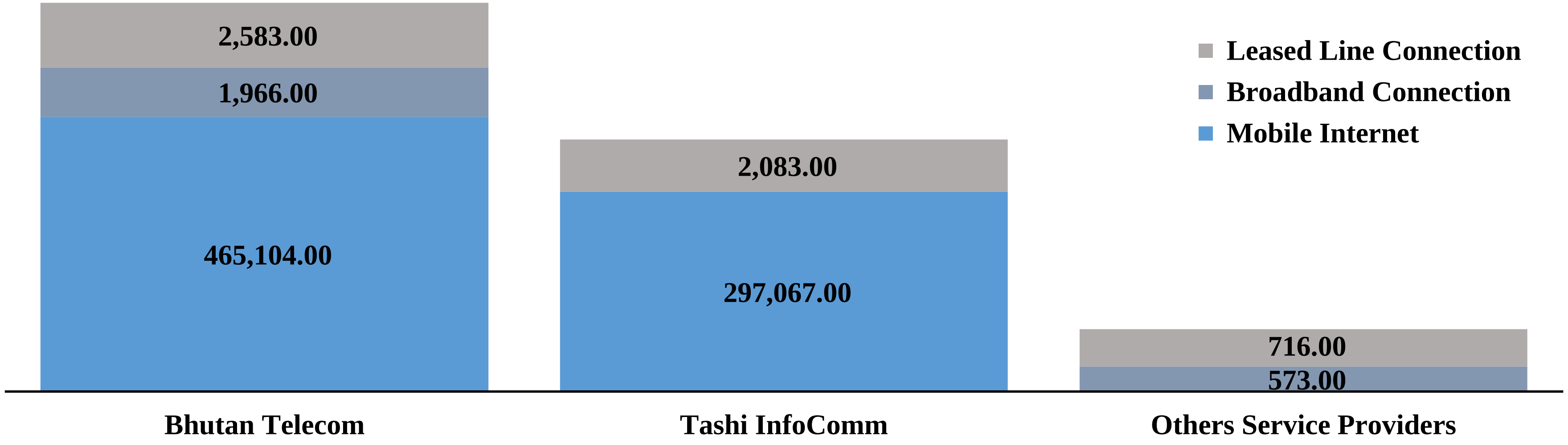
Bhutan’s ranking in the ICT Development Index of the ITU





Bhutan is at the *start-up level of maturity*, meaning that Bhutan neither has the capacity nor has undertaken concrete actions to enhance cybersecurity.

Building Cyber-security Capacity in the Kingdom of Bhutan, Global Cyber Security Capacity Centre, 2015



INTRODUCTION

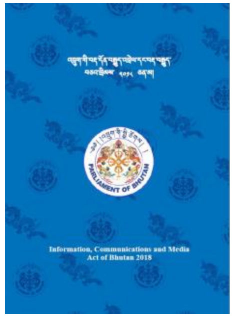
National Cybersecurity Strategy

Under development since late 2018

Challenges of Cybersecurity in Bhutan

- Lack of awareness
- Perception of management
- Stakeholder participation
- Visibility and funding

Legal Framework

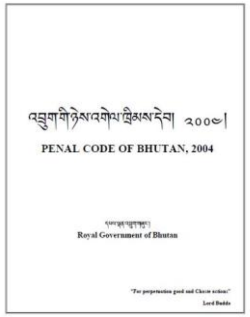


འབྲུག་གི་བརྡ་དོན་བརྒྱུད་འཕྲིན་དང་བརྡ་བརྒྱུད་
བཅའ་ཁྲིམས་ ༢༠༡༨ ཅན་མ།

PARLIAMENT OF BHUTAN

Information, Communications and Media
Act of Bhutan 2018

ICM Act of Bhutan, 2018



འབྲུག་གི་ཉེས་འགེལ་ཁྲིམས་དེབ། ༢༠༠༤།

PENAL CODE OF BHUTAN, 2004

Royal Government of Bhutan

"For perpetuation good and Chaste actions"

Lord Budda

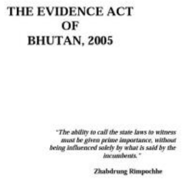
Penal Code of Bhutan, 2004

འབྲུག་གི་ཞི་ཧྲོད་དང་ཉེས་ཧྲོད་བྱ་བའི་གནད་སྤྱོད་ཀྱི་ཁྲིམས་དེབ་
(འཕྲི་སྣོན་) བཅའ་ཁྲིམས་ ༢༠༢༡ ཅན་མ།

PARLIAMENT OF BHUTAN

Civil and Criminal Procedure Code
(Amendment) Act of Bhutan 2021

Civil and Criminal Procedure Code Act of Bhutan, 2021



THE EVIDENCE ACT
OF
BHUTAN, 2005

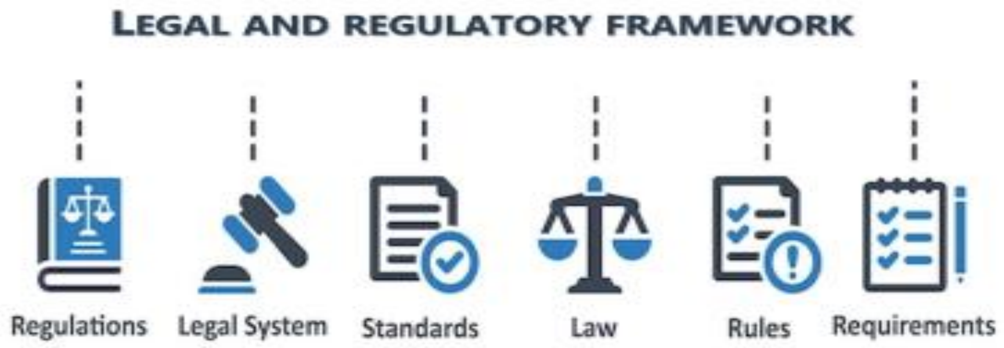
"The ability to call the state laws to witness must be given prime importance, without being influenced solely by what is said by the incumbents."

Zhabdrung Rimpochhe

Evidence Act, 2005

Audit Findings

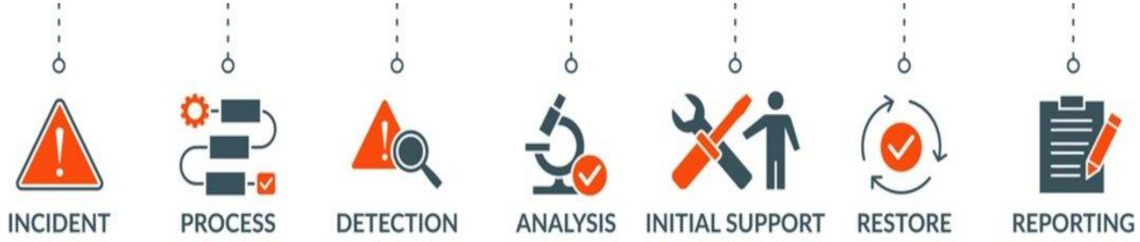
Cyber Governance



Cybersecurity Awareness and Capability

Institutional Framework

Incident Handling Mechanism



Legal and regulatory framework

Regulations

Legal System

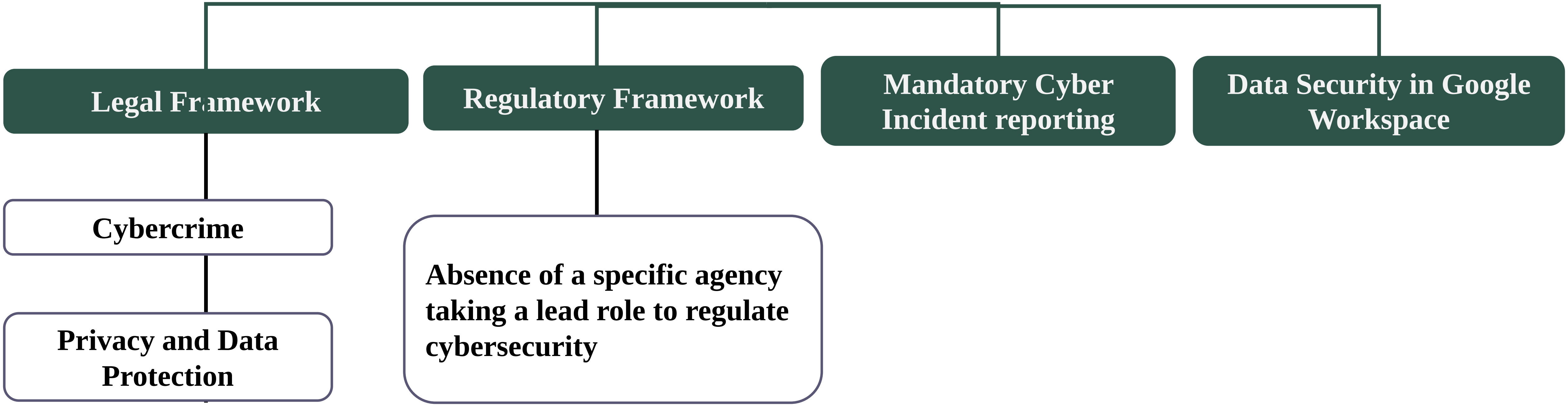
Standards

Law

Rules

Requirements

Legal and regulatory Framework



Legal Framework

Regulatory Framework

Mandatory Cyber Incident reporting

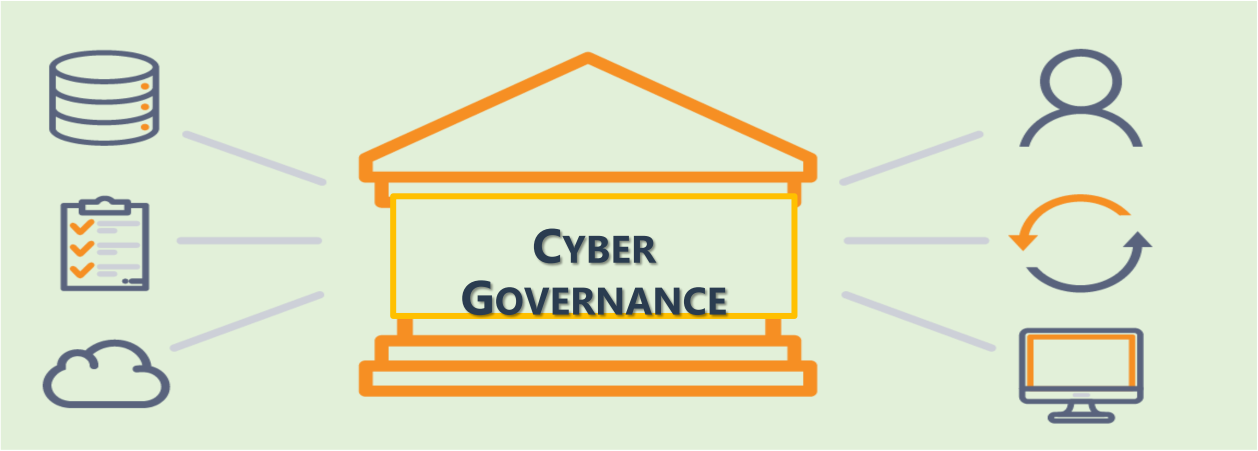
Data Security in Google Workspace

Cybercrime

Privacy and Data Protection

Absence of a specific agency taking a lead role to regulate cybersecurity

Audit Findings



Cyber Governance

Legal and regulatory framework

Regulations Legal System Standards Law Rules Requirements

Cybersecurity Awareness and Capability

Institutional Framework

Incident Handling Mechanism

INCIDENT PROCESS DETECTION ANALYSIS INITIAL SUPPORT RESTORE REPORTING

Institutional Framework

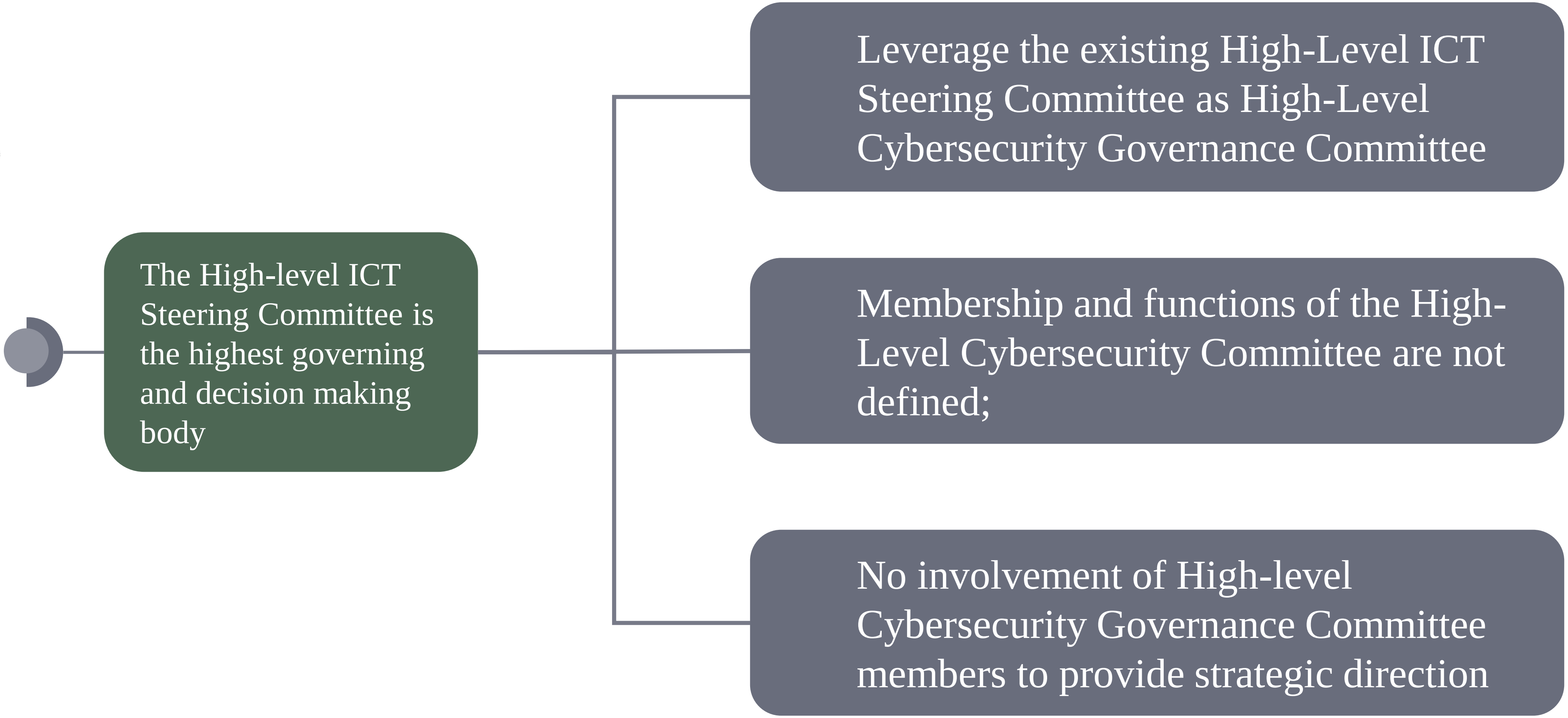
COORDINATING LEADERSHIP TO PROVIDE STRATEGIC DIRECTION AND STEER STRATEGIES FOR CYBERSECURITY

NATIONAL CYBERSECURITY STRATEGY (NCS) of Bhutan

(2021 to 2025)

Draft_Version 1.0

Date: 1st November 2020
Ministry of Information and Communications
Royal Government of Bhutan



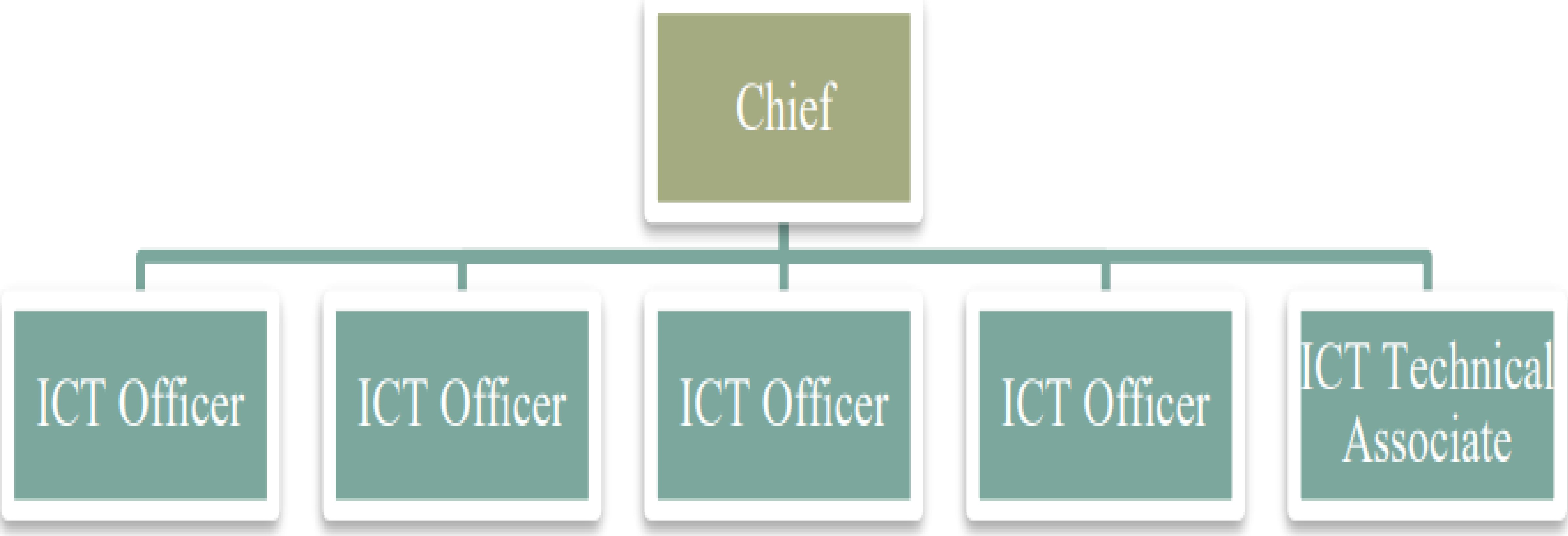
The High-level ICT Steering Committee is the highest governing and decision making body

Leverage the existing High-Level ICT Steering Committee as High-Level Cybersecurity Governance Committee

Membership and functions of the High-Level Cybersecurity Committee are not defined;

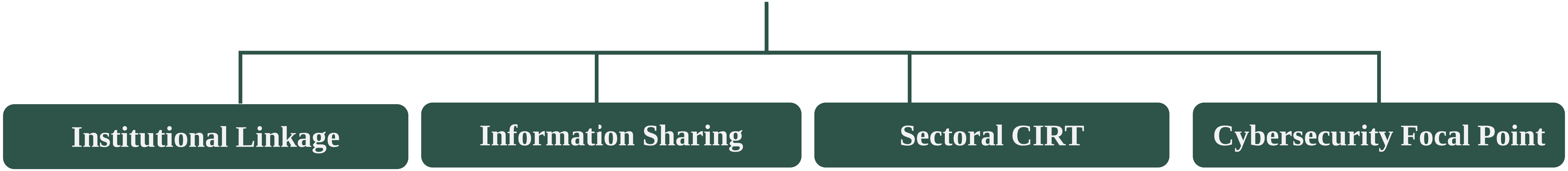
No involvement of High-level Cybersecurity Governance Committee members to provide strategic direction

National Agency for Cybersecurity



Cybersecurity Dept is not capacitated in terms of both human and financial resources to perform its functions in strengthening the cybersecurity posture of our country.

Institutional linkages for Cooperation and Information sharing



Institutional Linkage

Information Sharing

Sectoral CIRT

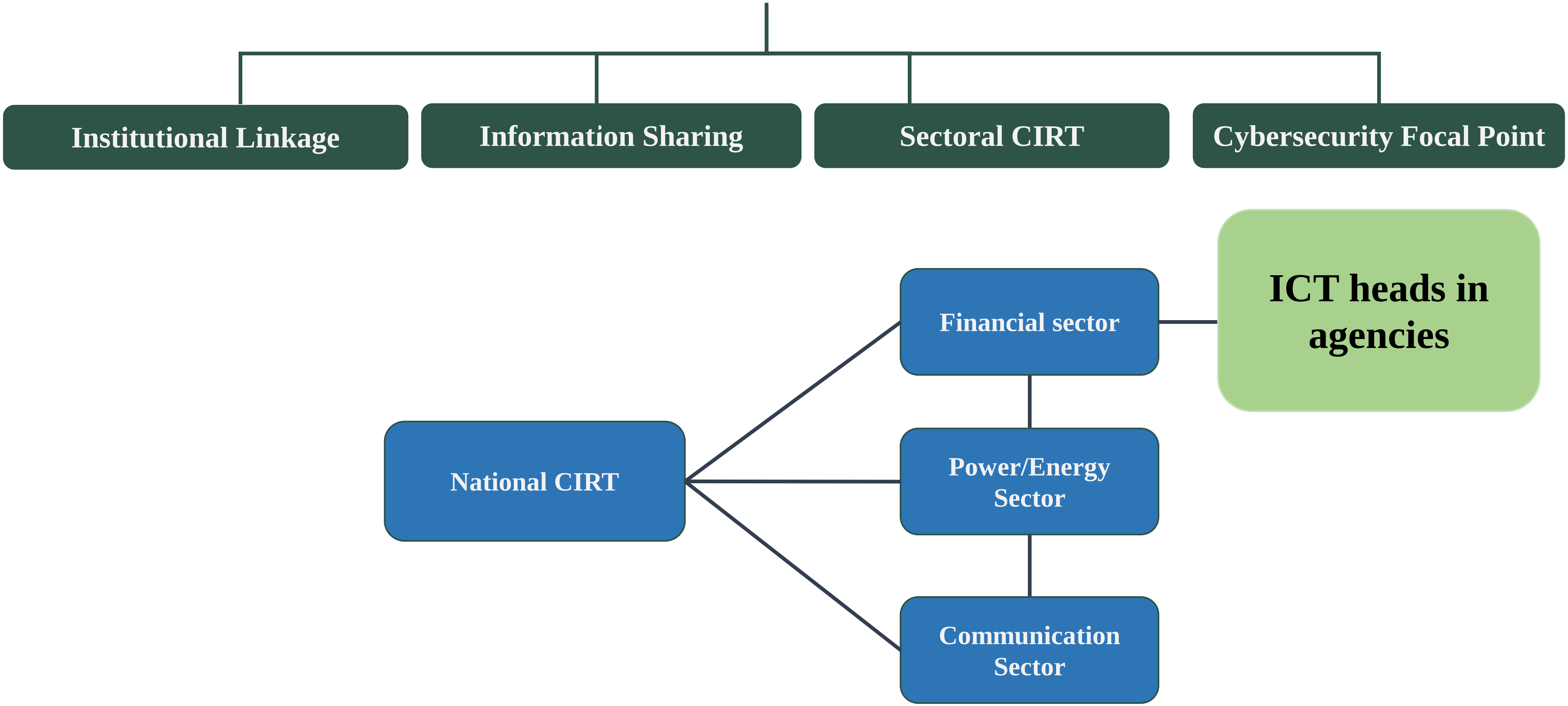
Cybersecurity Focal Point

- BtCIRT and regulators
- BICMA and government agencies having CIIS and essential services
- Among the regulators (BICMA, RMA, BEA)
- BtCIRT does not have coordination mechanism to bring key stakeholders during cyber emergencies

RBP and OAG has signed MoU- clear understanding of their roles in investigation and prosecution

- Only initiated by BtCIRT
- Information sharing is not regulated and identified
- Lack of collaborative efforts led by the BtCIRT with its constituents in implementation of cyber advisories and alerts
- No platform for engagement between SOCs/CIRTs in the country and other jurisdictions or law enforcement bodies for collaboration

Institutional linkages for Cooperation and Information sharing



Audit Findings

Cyber Governance

Legal and regulatory framework

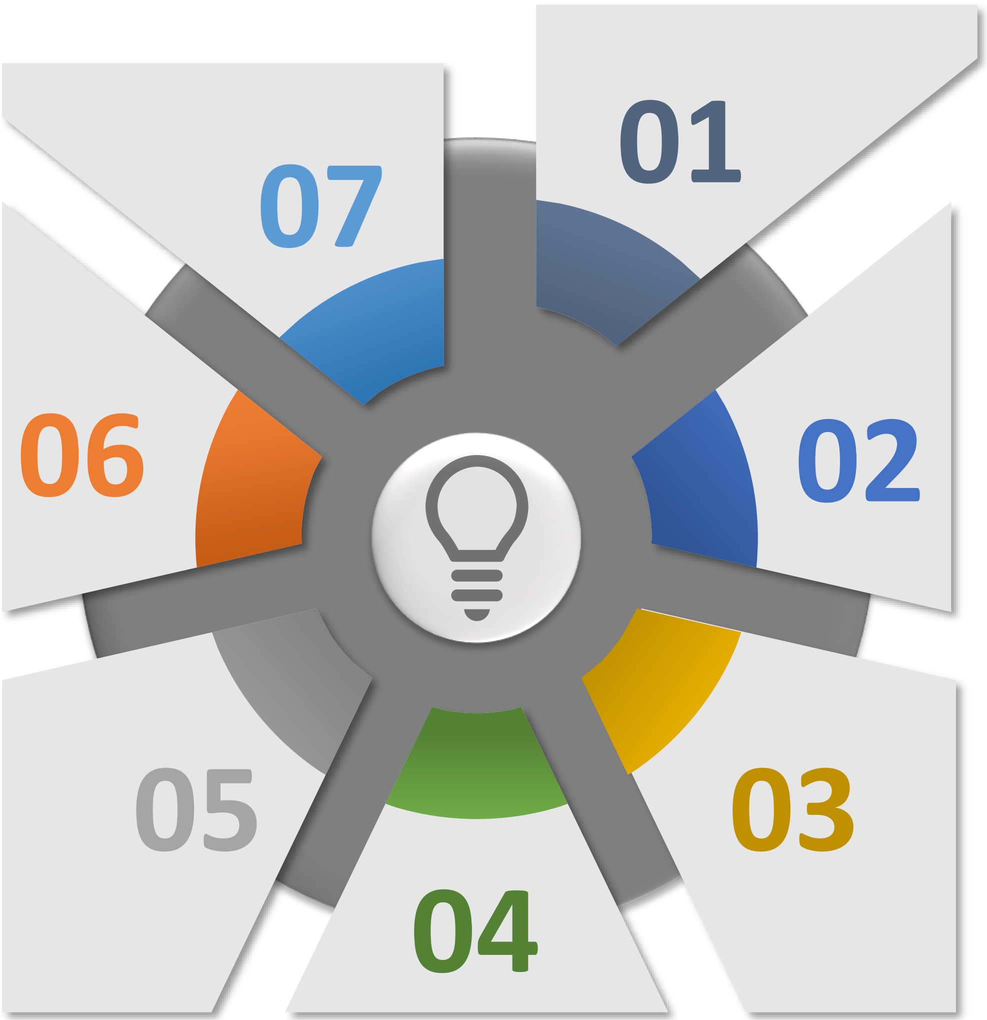
Cybersecurity Awareness and Capability

Institutional Framework

Incident Handling Mechanism

INCIDENT
PROCESS
DETECTION
ANALYSIS
INITIAL SUPPORT
RESTORE
REPORTING

Cyber Governance



NATIONAL CYBERSECURITY STRATEGY (NCS)

CYBERSECURITY FRAMEWORK

COMPREHENSIVE NATIONAL PLAN FOR SECURING KEY RESOURCES AND CRITICAL SECTORS

IDENTIFICATION OF CRITICAL SECTORS AND CRITICAL INFORMATION INFRASTRUCTURE

PROTECTION OF CRITICAL SECTORS AND CRITICAL INFORMATION INFRASTRUCTURES

BASELINE SECURITY MEASURES

SECURITY AUDITS

Audit Findings

Cyber Governance

Legal and regulatory framework

Regulations

Legal System

Standards

Law

Rules

Requirements

Cybersecurity Awareness and Capability

Institutional Framework

Incident Handling Mechanism

INCIDENT

PROCESS

DETECTION

ANALYSIS

INITIAL SUPPORT

RESTORE

REPORTING

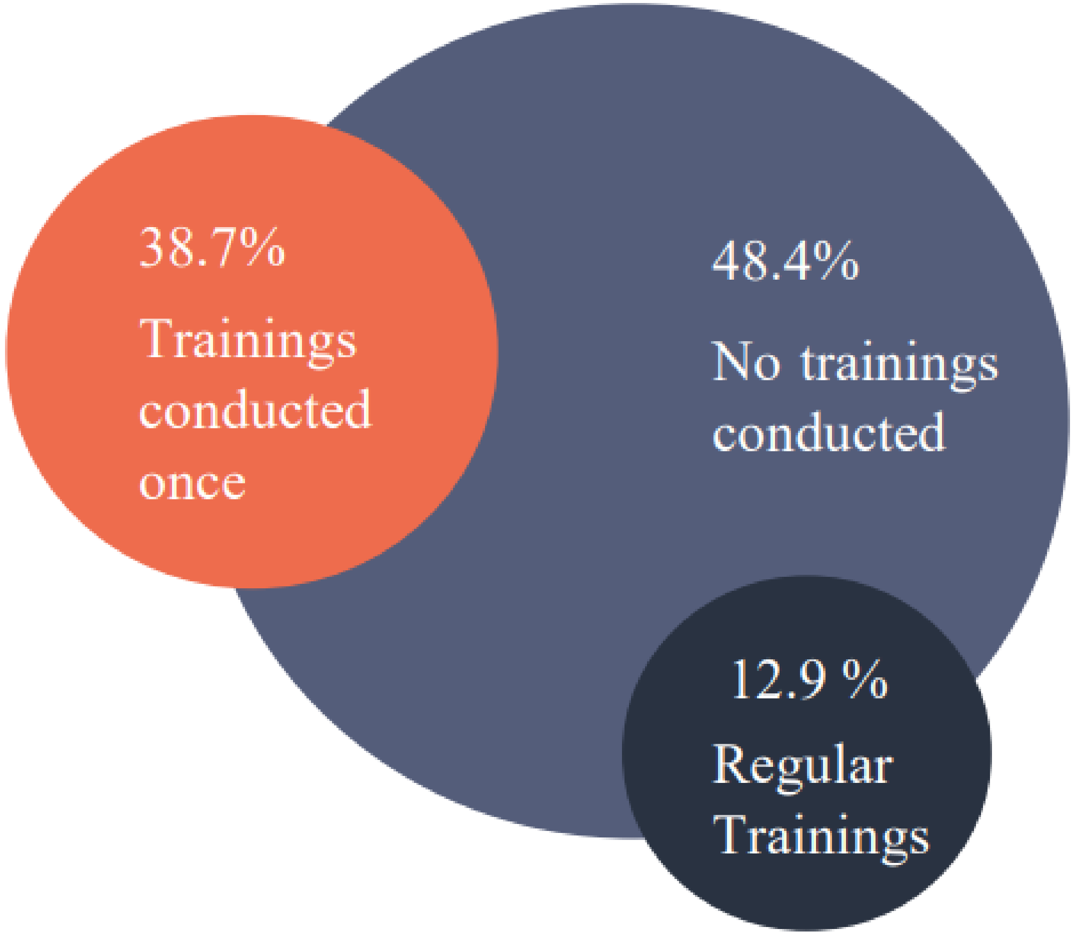
Cybersecurity Awareness and Capability

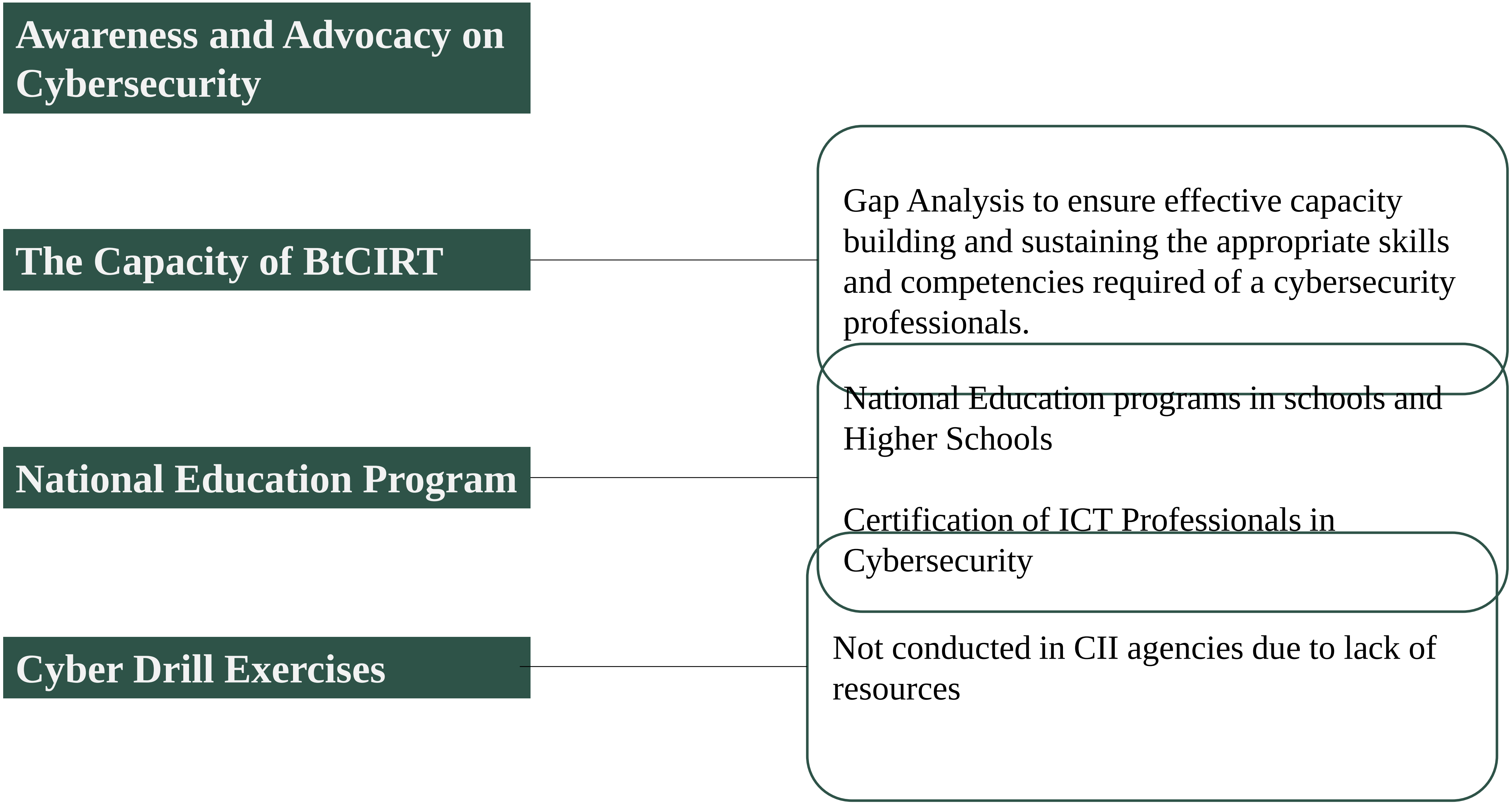
Awareness and advocacy on cybersecurity

General Awareness and Educational Activities

Employee Training and Cyber Hygiene

Limited coverage on legal and financial consequences of cyber





Awareness and Advocacy on Cybersecurity

The Capacity of BtCIRT

Gap Analysis to ensure effective capacity building and sustaining the appropriate skills and competencies required of a cybersecurity professionals.

National Education Program

National Education programs in schools and Higher Schools

Certification of ICT Professionals in Cybersecurity

Cyber Drill Exercises

Not conducted in CII agencies due to lack of resources

Audit Findings

Cyber Governance

Legal and regulatory framework

Regulations
Legal System
Standards
Law
Rules
Requirements

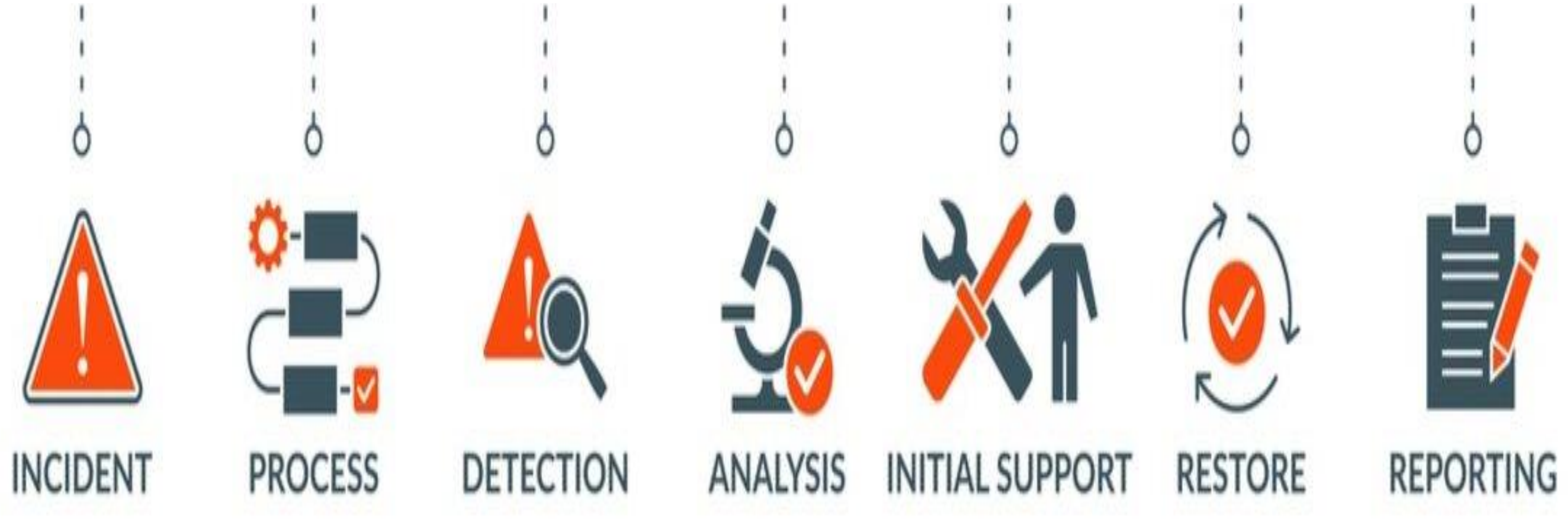
Cybersecurity Awareness and Capability

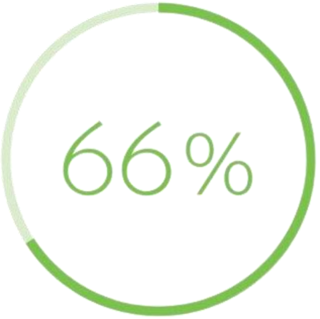
Institutional Framework

Incident Handling Mechanism

INCIDENT
PROCESS
DETECTION
ANALYSIS
INITIAL SUPPORT
RESTORE
REPORTING

Incident Handling Mechanism



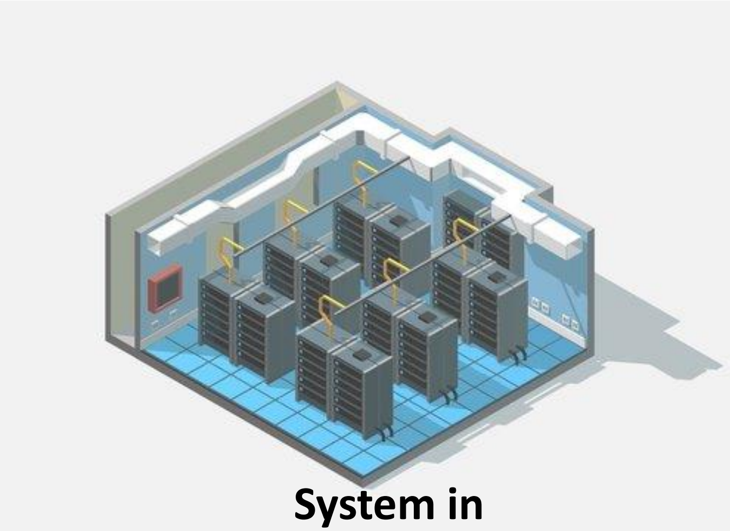


Some agencies do not have intrusion detection and prevention system

BtCIRT
Bhutan Computer Incident Response Team

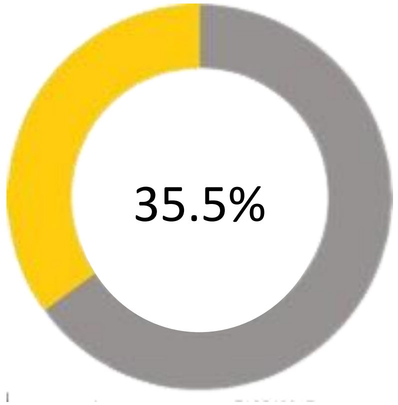
1. Vulnerability Scan of IT Systems

2. Vulnerability Assessment Report



System in Government Data Centre (GDC)

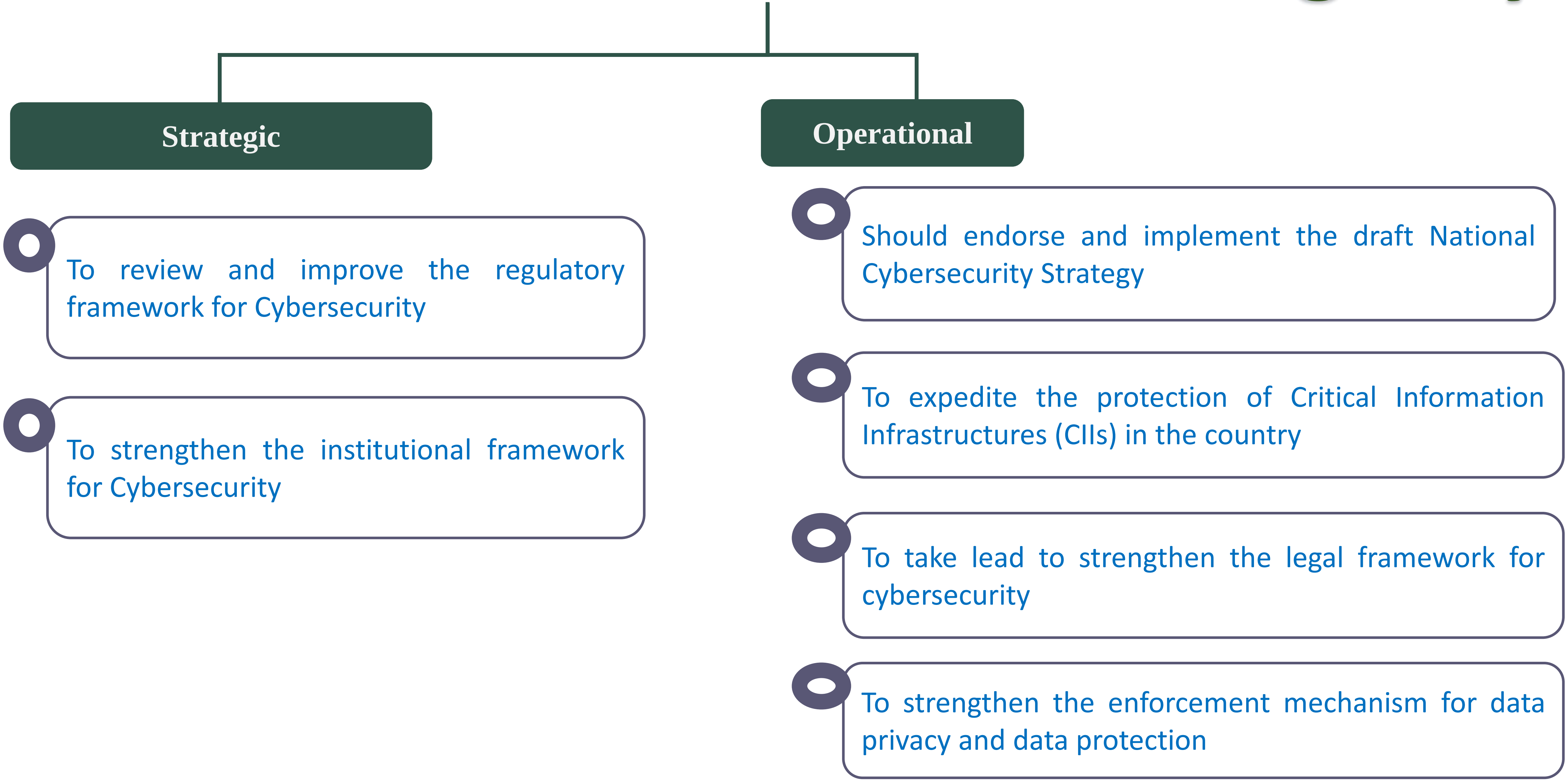
No follow-up mechanism to ensure the remedies are implemented.



Do not update and apply patches to mitigate vulnerabilities.

6 Recommendations

Recommendations: GovTech Agency



Strategic

- To review and improve the regulatory framework for Cybersecurity
- To strengthen the institutional framework for Cybersecurity

Operational

- Should endorse and implement the draft National Cybersecurity Strategy
- To expedite the protection of Critical Information Infrastructures (CIIs) in the country
- To take lead to strengthen the legal framework for cybersecurity
- To strengthen the enforcement mechanism for data privacy and data protection

100% endorsed by the Parliament

POSITIVE CHANGES

- ✓ **Funding from Donors**
- ✓ **Importance from the Government**
- ✓ **Cybersecurity Strategy – Finalizing**
- ✓ **Working Group on Legal Group formed**
- ✓ **Reinforced data protection**
- ✓ **Working group formed for CIIs**

Thank You

QUESTIONS