རྒྱལ་གཞུང་རྩིས་ཞིབ་དབང་འཛིན།
ROYAL AUDIT AUTHORITY

གློག་ཐོག་ཉེན་སྲུང་གི་གྲ་སྒྲིག།

(ལས་འབྲེལ་རྩིས་ཞིབ།)

Preparedness for Cybersecurity (Performance Audit)

སྤྱི་ལོ་༢༠༢༣ སྤྱི་ཟླ་ ༥ པ་ལུ།

May 2023

DISCLAIMER NOTE

The audit was conducted in accordance with the International Standards of Supreme Audit Institutions (ISSAIs). The audit was conducted based on the audit objectives and criteria determined in the audit plan and programme prepared by the Royal Audit Authority and the findings are based on the information and data made available by the Bhutan Computer Incident Response Team, GovTech Agency, Bhutan InfoComm and Media Authority, Office of Attorney General, Royal Bhutan Police, Bhutan Electricity Authority, Royal Monetary Authority, Financial Institutions, and Telecommunication Service Providers.

This is also to certify that the auditors during the audit had neither yielded to pressure nor dispensed any favour nor resorted to any unethical means that would violate the Royal Audit Authority's Oath of Good Conduct, Ethics, and Secrecy.

རྒྱལ་གཞུང་རྩིས་ཞིབ་དབང་འཛིན།

ROYAL AUDIT AUTHORITY

Bhutan Integrity House

Reporting on Economy, Efficiency & Effectiveness in the use of Public Resources

RAA/DPCA/TAD (PA-Cybersecurity)/2022-23/*825* **Date: 9 May 2023**

The Acting Secretary
Government Technology (GovTech) Agency
Thimphu

<u>Subject: Performance Audit Report on Preparedness for Cybersecurity</u>

Dear Sir,

Enclosed herewith please find the **Performance Audit Report on Preparedness for Cybersecurity** covering the period 1 July 2016 until 30 December 2022. The Royal Audit Authority (RAA) conducted the audit in line with the mandate enshrined in the Constitution of the Kingdom of Bhutan and the Audit Act of Bhutan 2018. The audit was conducted in accordance with the International Standards of Supreme Audit Institutions on Performance Audit (ISSAI 3000). The audit is also conducted in the context of Performance Auditing following the RAA's Performance Audit Guidelines.

The audit objectives were as follows:

- ☑ To ascertain the Government's efforts towards ensuring safe, secure, and resilient cyberspace in Bhutan. The sub-objectives are:
  - ➲ To determine the appropriateness of the cybersecurity program/system in the country.
  - ➲ To examine whether the Critical Information Infrastructure (CII) systems are identified and protected.

The report has been prepared based on the review of available documents, analysis of data, and discussion with relevant officials of the Bhutan Computer Incident Response Team (BtCIRT) under the erstwhile Department of Information Technology and Telecom (DITT), Bhutan InfoComm and Media Authority (BICMA), Office of Attorney General (OAG), Royal Bhutan Police (RBP), erstwhile Bhutan Electricity Authority (BEA), Royal Monetary Authority (RMA), Financial Institutions and Telecommunication Service Providers.

The report contains shortcomings and deficiencies, and recommendations for improving the country's cybersecurity posture. The audit findings were issued in the form of short reports between 4 November 2022 and 27 December 2022 for factual confirmation, comments, and feedback. Similarly, the draft report was issued on 10 April 2023 for factual confirmation, comments and feedback, especially on the relevancy and applicability of the recommendations. The responses received have been incorporated into the report and the GovTech Agency has accepted all the recommendations for implementation.

In line with the Audit Act of Bhutan 2018, the audited agencies are required to submit responses to the Performance Audit Report in the form of a Management Action Plan (MAP). The MAP should specify the action plans for implementing the recommendations with a definite timeframe to address the findings' underlying causes. Further, as specified by Section 55 (16) of the Audit Act of Bhutan 2018, the audited agencies concerned must submit a signed Accountability Statement (AS) to implement the recommendations provided.

The RAA will follow up on the implementation of the corrective actions and recommendations based on the MAP and AS. Failure to comply will result in taking appropriate actions, which may include suspending audit clearances to the official(s) accountable.

Therefore, the RAA would like to request the agencies concerned to submit a MAP for the implementation of recommendations with a definite timeframe ***on or before 29 May 2023*** *along with the signed AS (format attached under Appendix A). In the event of non-submission, the RAA shall invariably fix the overall supervisory accountability on the head of the audited agency in line with Section 55(17) of the Audit Act of Bhutan 2018.*

We take this opportunity to acknowledge the officials of the audited entities for rendering the necessary cooperation and support which facilitated the timely completion of the audit.

Yours sincerely,

(Tashi)
Auditor General of Bhutan

Copy to:

1. Hon'ble Lyonchhen, Royal Government of Bhutan
2. Hon'ble Gyalpoi Zimpon, Office of Gyalpoi Zimpon
3. Hon'ble Speaker, National Assembly of Bhutan
4. Hon'ble Chairperson, National Council of Bhutan
5. Hon'ble Opposition Leader, National Assembly of Bhutan
6. Hon'ble Chairperson, Public Accounts Committee, National Assembly of Bhutan
7. Chief of Police, Royal Bhutan Police
8. The Governor, Royal Monetary Authority
9. The Attorney General, Office of Attorney General
10. The Deputy Chief of Police (Crime and Operation Branch), Royal Bhutan Police
11. The Chief Executive Officer, Electricity Regulatory Authority
12. The Director, Bhutan InfoComm and Media Authority
13. The Chief ICT Officer, Cybersecurity Division, GovTech Agency
14. The Assistant Auditor General, Follow-up and Clearance Division, RAA
15. The Assistant Auditor General, Policy and Planning Division, RAA
16. Office copy

"Every individual must strive to be principled. And individuals in positions of responsibility must even strive harder."

TITLE SHEET

1.	Title of the Report	:	Performance Audit on Preparedness for Cybersecurity
2.	AIN	:	TAD-2022-436
3.	Audited Entity	:	GovTech Agency
4.	Audit Period	:	April 2016 till 30 December 2022
5.	Audit Schedule	:	July 2022 to November 2022
6.	Audit Team	:	1. Kinley Zam, Dy. Chief Auditor
		:	2. Namgay Choden, Sr. Audit Officer
			3. Tandin Phuntsho, Audit Officer
		:	4. Phuntsho Choden, Asstt. Audit Officer
7.	Supervisor	:	Sonam Delma, Asstt. Auditor General
8.	Overall Supervisor	:	Dorji Wangchuk, Deputy Auditor General

ACRONYMS AND ABBREVIATIONS

ACC	:	Anti-Corruption Commission
BCP	:	Business Continuity Plan
BtCIRT	:	Bhutan Computer Incident Response Team
BDBL	:	Bhutan Development Bank Limited
BEA	:	Bhutan Electricity Authority
BICMA	:	Bhutan InfoComm and Media Authority
BIL	:	Bhutan Insurance Limited
BNBL	:	Bhutan National Bank Limited
BoBL	:	Bank of Bhutan Limited
BPCL	:	Bhutan Power Corporation Limited
CCDCOE	:	Cooperative Cyber Defence Centre of Excellence
CII	:	Critical Information Infrastructure
CIIP	:	Critical Information Infrastructure Protection
CIRT	:	Computer Incident Response Team
CNI	:	Critical National Infrastructure
COPWG	:	Child Online Protection Working Group
CSA	:	Cyber Security Agency
DGPC	:	Druk Green Power Corporation
DITT	:	Department of Information Technology and Telecom
DPNBL	:	Druk Punjab National Bank Limited
DRP	:	Disaster Recovery Plan
ENISA	:	European Network and Information Security Agency
ePEMS	:	*electronic* Public Expenditure Management System
FICRT	:	Financial Institutions Cyber Response Team
GDC	:	Government Data Centre
GFCE	:	Global Forum on Cyber Expertise
ICM Act	:	Information Communication and Media Act
ICT	:	Information Communication and Technology
ISO	:	International Organisation for Standardization
ISP	:	Internet Service Provider
ISSAI	:	International Standard for Supreme Audit Institution
IT	:	Information Technology

ITU	:	International Telecommunication Union
JDWNRH	:	Jigme Dorji Wangchuck National Referral Hospital
KPI	:	Key Performance Indicator
LFWG	:	Legal Framework Working Group
MoAF	:	Ministry of Agriculture and Forest
MoE	:	Ministry of Education
MoEA	:	Ministry of Economic Affairs
MoF	:	Ministry of Finance
MoH	:	Ministry of Health
MoIC	:	Ministry of Information and Communication
MoLHR	:	Ministry of Labour and Human Resources
MoWHS	:	Ministry of Works and Human Settlement
NATO	:	North Atlantic Treaty Organisation
NCP	:	National Cybersecurity Policy
NCS	:	National Cybersecurity Strategy
NCSC	:	National Cyber Security Centre
NCWG	:	National Cybersecurity Working Group
NIST	:	National Institute of Standards and Technology
NLC	:	National Land Commission
NPPF	:	National Pension and Provident Fund
OAG	:	Office of Attorney General
PCI-DSS	:	Payment Card Industry Data Security Standard
RAA	:	Royal Audit Authority
RBP	:	Royal Bhutan Police
RGoB	:	Royal Government of Bhutan
RICBL	:	Royal Insurance Corporation of Bhutan Limited
RMA	:	Royal Monetary Authority
T Bank	:	T Bank Limited
USA	:	United States of America
VA	:	Vulnerability Assessment

TABLE OF CONTENTS

Executive Summary **1**

Chapter 1: About the Audit **4**

1.1. Mandate **4**

1.2. Audit Standards **4**

1.3. Audit Objectives **4**

1.4. Audit Scope **4**

1.5. Audit Approach Applied **5**

1.6. Audit Methodology **5**

Chapter 2: Introduction **8**

2.1. The Rationale for this Audit **8**

2.2. Cybersecurity **9**

2.3. Importance of Cybersecurity **9**

2.4. Cybersecurity in Bhutan **9**

2.5. National Cybersecurity Strategy **10**

2.6. Challenges of Cybersecurity in Bhutan **10**

2.7. Legal Framework **10**

Chapter 3: Audit Findings **11**

3.1 Legal and Regulatory Framework **12**

3.1.1 Legal Framework **12**

3.1.2 Regulatory Framework **16**

3.1.3 Mandatory Cyber Incident Reporting **19**

3.1.4 Data Security in Google Workspace **21**

3.2 Institutional Framework **25**

3.2.1 Coordinating Leadership for Cybersecurity **25**

3.2.2 National Agency for Cybersecurity **27**

3.2.3 Institutional Linkages for Cooperation and Information Sharing **30**

3.3 Cybersecurity Governance **37**

3.3.1 National Cybersecurity Strategy **37**

3.3.2 Cybersecurity Framework **45**

3.3.3 Comprehensive National Plan for Securing the Key Resources and Critical Sectors **46**

3.3.4 Identification of Critical Sectors and Critical Information Infrastructure **47**

3.3.5 Protection of Critical Sectors and Critical Information Infrastructure **52**

3.3.6 Baseline Security Measures **53**

3.3.7 Security Audits **55**

3.3.8 Risk Assessment for CIIs 56

3.4 Cybersecurity Awareness and Capabilities 57

3.4.1. Awareness and Advocacy on Cybersecurity 58

3.4.2.The capacity of the BtCIRT 63

3.4.3.National Educational Programmes 65

3.4.4.Cyber Drill Exercises 69

3.5 Incident Handling Mechanism 72

3.5.1 Cyber Incident Handling 72

Chapter 4: Recommendations 75

4.1. Strategic 75

4.1.1. The GovTech Agency should review and improve the regulatory framework for Cybersecurity 75

4.1.2. The GovTech Agency should strengthen the institutional framework for Cybersecurity 75

4.2. Operational 76

4.2.1. The GovTech Agency should endorse and implement the draft National Cybersecurity Strategy 76

4.2.2. The GovTech Agency should expedite the protection of Critical Information Infrastructures (CIIs) in the country 77

4.2.3. The GovTech Agency should take lead to strengthen the legal framework for cybersecurity 78

4.2.4. The GovTech Agency should strengthen the enforcement mechanism for data privacy and data protection 78

Chapter 5: Conclusion 79

Appendix A – *Management Action Plan and Accountability Statement* 80

Executive Summary

On 2 June 1999, coinciding with the Silver Jubilee celebrations of His Majesty the 4th Druk Gyalpo, Internet services were first made available to Bhutanese and ever since then, the use of the Internet in the country has significantly grown and developed in terms of users and infrastructure. The last two decades have seen Bhutan undergo a far-reaching digital transformation, especially in terms of the delivery and adoption of digital services. The government has implemented the national broadband network, national data centre, and national payment gateway and many Bhutanese people have embraced cardless transactions. Similarly, the corporate sector has also increased its investments to effectively leverage ICT to enhance its operational capabilities and efficiencies.

More recently, the onset of the COVID-19 pandemic has led to an increase in the use of the Internet by people as a means of communication and availing services. Government agencies are now increasingly using the Internet to deliver their services more efficiently to citizens. However, with the increase in Internet use, the rate at which users have been exposed to fraud, phishing, scams, data loss, and other cyber threats is also on the rise.

The International Telecommunication Union (ITU), defines cybersecurity as a 'collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organisation and users' assets.' The consequences of digital transformation and the widespread use of technology mean that cybersecurity has become an evitable part of the lives of all Bhutanese citizens and is affected by it daily. Owing to this, the Government instituted the Bhutan Computer Incident Response Team (BtCIRT) in 2016, and as per the Information, Communication and Media Act of Bhutan, 2018, the BtCIRT is identified as the national agency to coordinate cybersecurity activities and be a central point of contact on all cybersecurity matters on national security in the country.

The RAA conducted the performance audit of preparedness for cybersecurity as mandated by the constitution of the Kingdom of Bhutan and the Audit Act of Bhutan 2018. The audit was conducted following the Performance Audit Guidelines, which are in line with the International Standards for Supreme Audit Institutions (ISSAIs). The performance audit of preparedness for cybersecurity was conducted with an overall audit objective of ascertaining the government's efforts toward ensuring safe, secure, and resilient cyberspace in Bhutan.

The performance audit of preparedness for cybersecurity was conducted in BtCIRT, Government Technology Agency (GovTech). The audit covered the period from the inception of the BtCIRT, April 2016 to December 2022. The performance audit of preparedness for cybersecurity assessed the six areas; i) Legal and Regulatory Framework; ii) Institutional Framework; iii) Cybersecurity Governance; iv) Capacity Building and Awareness; v) Risk Assessment of Identified Critical Sectors; and vi) Incident Handling Mechanism.

The RAA noted inadequacies and deficiencies in the six areas, of which the significant findings are briefly highlighted below:

i. The RAA noted inadequacies in the regulatory framework and enforcement mechanisms which has inhibited effective enforcement of legal provisions for cybersecurity.

ii. The cybersecurity initiatives undertaken in the country lack strategic visions and directions, defined principles, and set priorities in managing cybersecurity risks with the National Cybersecurity Strategy (NCS) still in its draft stage. The draft NCS was developed in 2018 and was intended to be implemented from 2021 to 2025 of which two years have already elapsed. The RAA also noted that a risk assessment of the draft NCS had not been conducted, a monitoring and evaluation framework was not developed, Key Performance Indicators were inadequately set, coordination mechanisms were not defined and there is no dedicated budget for implementing the action plans identified in the draft NCS.

iii. There is a lack of adequate attention and focus given to cybersecurity programmes due to the absence of a coordinated higher authority for cybersecurity, the cybersecurity governance committee. The national agency for cybersecurity, the BtCIRT, is also not equipped with sufficient resources leading to its ineffectiveness in delivering their functions.

iv. There is an absence of institutionalised mechanisms of collaboration and coordination with stakeholders resulting in fragmented approaches to cybersecurity.

v. The framework for identifying the Critical Information Infrastructures (CIIs) which is essential for the functioning of the nation in terms of national security, economy, health, social welfare or safety, is still in its draft phase. The delay in the identification of CIIs would result in the exposure of the CIIs to potential cyber threats and the inability to institute adequate CII protection mechanisms.

vi. The inadequate capacity assessment framework to identify the cybersecurity capabilities both at the strategic and operational levels has resulted in the lack of capacity of the BtCIRT.

vii. There is a lack of adequate legal frameworks and mechanisms to address cybercrime. There are no legal provisions defining cybercrime. Bhutan also does not have agreements for cross-border and multi-judicial investigation of cybercrime, with other countries besides India.

To contribute towards ensuring a safe, secure, and resilient cyberspace in the country, the RAA has developed six recommendations which are highlighted below:

A. At the strategic level:

i. The GovTech Agency should review the regulatory framework to ensure that the security controls are implemented and compliance requirements are met leading to enhancing the cybersecurity posture of the country.

ii. The GovTech Agency should take the lead and overcome the present disconnect between the agencies involved in cybersecurity and strengthen the institutional framework. An effective and well-coordinated institutional framework will enable the country to be in a better position to identify, protect and detect cybersecurity threats.

B. At the operational level:

iii. The GovTech Agency should review and implement the draft NCS to act as a guide for the country's vision, high-level objectives, principles, and priorities in enhancing cybersecurity. Implementing the draft NCS would also ensure that adequate resources are made available for the activities defined in the strategy.

iv. The GovTech Agency should expedite the protection of Critical Information Infrastructures (CIIs) in the country which includes developing the identification framework, identifying the CIIs, ensuring that the CII owners implement security measures to protect the CIIs, and develop and implement the CII Regulations.

v. The GovTech Agency should take lead to strengthen the legal framework for cybersecurity through the review of existing Acts, Rules and Regulations on cybersecurity, identification and addressing legal gaps, and harmonising the laws.

vi. The GovTech Agency should strengthen the enforcement mechanism of legal provisions and government executive orders for data privacy and data protection. Further, the GovTech Agency should develop protocols to classify data to ensure that sensitive and confidential information is not uploaded to Google Workspace.

Chapter 1: About the Audit

1.1. Mandate

The RAA conducted the 'Performance Audit of Preparedness for Cybersecurity' as mandated by 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.

Further, Chapter 5, Section 69 of the Audit Act of Bhutan 2018 stipulates, "The Authority shall carry out performance, financial, compliance, special audits and any other form of audits that the Auditor General may consider appropriate."

1.2. Audit Standards

The RAA conducted this audit in accordance with the International Standards of Supreme Audit Institutions on Performance Auditing (ISSAI 3000). The RAA followed audit procedures as prescribed under RAA's Performance Audit Guidelines 2019 to maintain uniformity and consistency of approaches in auditing.

1.3. Audit Objectives

The RAA conducted the 'Performance audit of preparedness for cybersecurity' with the following audit objectives:

☑ To ascertain the Government's efforts towards ensuring safe, secure, and resilient cyberspace in Bhutan. The sub-objectives are:

i. To determine the appropriateness of the cybersecurity program/system in the country;

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

1.4. Audit Scope

The performance audit of preparedness for cybersecurity was conducted in the BtCIRT, GovTech Agency. The audit covered the period from the inception of the BtCIRT, April 2016 to December 2022.

The audit focused on and covered the following thrust areas:

1) Legal and Regulatory Framework;
2) Institutional Framework;
3) Cybersecurity Governance;
4) Capacity Building and Awareness;
5) Risk Assessment of Identified Critical Sectors; and
6) Incident Handling Mechanism.

The stakeholder consultations, assessment and review of documents were conducted from July 2022 to November 2022.

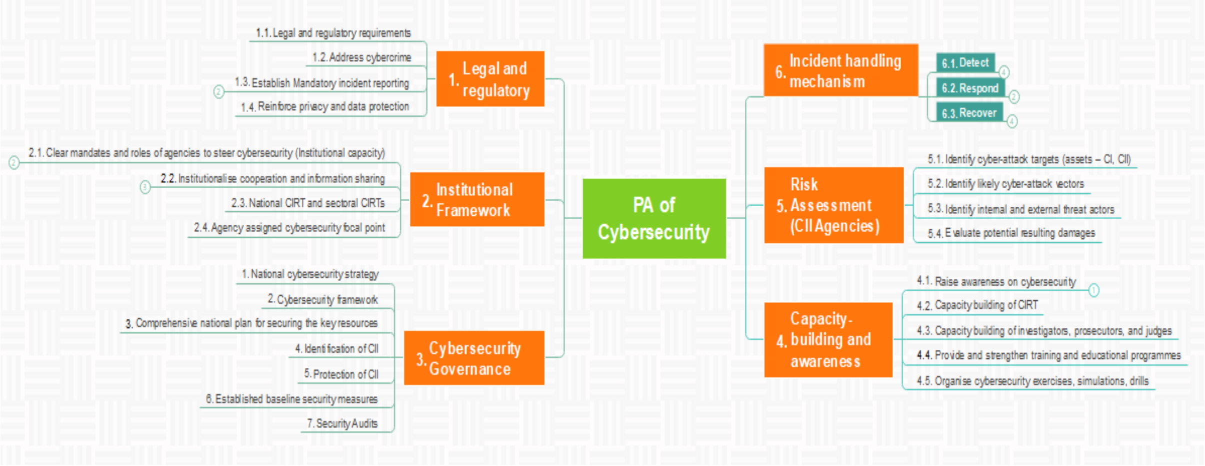
1.5. Audit Approach Applied

The audit applied the system-oriented approach to review the current legislation, regulatory framework, cybersecurity governance, identification of critical infrastructure, compliance with relevant legislation, and capacity to ensure cybersecurity.

The audit focussed on the organisational measures, coordination mechanisms, and institutional linkages amongst the key stakeholders, mechanisms to address cybercrime, and effectiveness of incident handling processes that could lead to safe, secure, and resilient cyberspace in Bhutan.

The system-oriented audit approach was applied using the mind map in the six thrust areas identified in the audit scope as portrayed in figure 1.

Figure 1: Mind map of the thrust areas with the system-oriented audit approach



PA of Cybersecurity
1. Legal and regulatory
1.1. Legal and regulatory requirements
1.2. Address cybercrime
1.3. Establish Mandatory incident reporting
2
1.4. Reinforce privacy and data protection
2. Institutional Framework
2.1. Clear mandates and roles of agencies to steer cybersecurity (Institutional capacity)
2
2.2. Institutionalise cooperation and information sharing
3
2.3. National CIRT and sectoral CIRTs
2.4. Agency assigned cybersecurity focal point
3. Cybersecurity Governance
1. National cybersecurity strategy
2. Cybersecurity framework
3. Comprehensive national plan for securing the key resources
4. Identification of CII
5. Protection of CII
6. Established baseline security measures
7. Security Audits
6. Incident handling mechanism
6.1. Detect
4
6.2. Respond
2
6.3. Recover
4
5. Risk Assessment (CII Agencies)
5.1. Identify cyber-attack targets (assets – CI, CII)
5.2. Identify likely cyber-attack vectors
5.3. Identify internal and external threat actors
5.4. Evaluate potential resulting damages
4. Capacity-building and awareness
4.1. Raise awareness on cybersecurity
1
4.2. Capacity building of CIRT
4.3. Capacity building of investigators, prosecutors, and judges
4.4. Provide and strengthen training and educational programmes
4.5. Organise cybersecurity exercises, simulations, drills

Source: RAA analysis after understanding the subject matter

1.6. Audit Methodology

The RAA applied the following methodologies to gather information, analyse data and derive conclusions:

i. Reviewed relevant legislation related to cybersecurity – Information, Communications and Media Act of Bhutan 2018, Penal Code of Bhutan 2004 (Amendment 2021), Civil and Criminal Procedure Code of Bhutan 2011 (Amendment 2021) and Evidence Act, 2005, Royal Bhutan Police Act 2009.

ii. Reviewed plan documents, policies, and strategy – Government Order for the establishment of BtCIRT, Draft National Cybersecurity Strategy 2021-2025, Critical Infrastructure Information Identification Framework, Draft Child Online Protection guidelines, Rules and Regulations for Licensing and Operations of ISPs, RMA Guideline on Data Privacy and Data Protection 2021, The e-Government Policy for Royal Government of Bhutan 2019, Information Management and Security Policy, MoE ICT Curriculum Framework (Class PP-XII), 11th and 12th Five Year Plans, Digital Drukyul Blueprint draft, BICMA Study Report on Cybersecurity 2020, Social Media Policy for the Royal Government of Bhutan, Financial Accounting Manual 2016, Budget Manual 2016, BtCIRT Operational Framework version 1, Vulnerability Management Process For Government Data Center.

iii. Reviewed other documents and publications – Budapest Convention on Cybercrime, The World Bank Report on Combatting Cybercrime, ITU guide to developing a national cybersecurity strategy, Building Cyber-security Capacity in the Kingdom of Bhutan, ITU Readiness Assessment for Establishing CIRT 2012, NIST Framework 1.1, The European Union Agency for Cybersecurity (ENISA) Evaluation framework for the cybersecurity strategies, NATO National Cyber Security Strategy Guidelines 2013, Global Forum on Cyber Expertise (GFCE) Good Practice Guide on Critical Infrastructure Information Protection (CIIP) for governmental policy-makers 2016, GFCE Global Good Practices-CIIP 2017, Microsoft framework for cybersecurity information sharing and risk reduction, NIST Guide to Cyber Threat Information Sharing, The Country Report Bhutan on the Digital Kids Asia Pacific 2020, ENISA Cybersecurity Skills Development in the EU, ITU guide on establishing national CIRT, UK Cyber Essentials, US Cyber Essentials Toolkit, NIST Guide for conducting security assessments in government agencies, Center for Internet Security – Critical Security Controls V8, NIST Data Protection Framework, Data Protection Act of Singapore 2012, Establishing a Privacy and Data Protection Framework for Middle East and North Africa, General Data Protection Regulation of EU, NIST IT Security Training Requirements, ENISA Raising Awareness of Cybersecurity.

iv. Consulted the BtCIRT on its mandates and activities. The BtCIRT was also consulted on cybersecurity incident handling, cybersecurity awareness, international and local cooperation, and the status of the Draft National Cybersecurity Strategy. Further, the BtCIRT was consulted for their inputs in the questionnaire and they facilitated obtaining the email addresses of the ICT heads for the survey of baseline security measures.

v. Administered a survey to assess and validate the existence of baseline security controls in government agencies using google forms. The survey was sent to all ICT heads in government agencies to assess the current practices in the implementation of minimum measures to prevent, detect, and respond to cyber threats. Received and analysed responses from 62 government agencies including 10 ministries, 20 Dzongkhags, 4 constitutional bodies, Thromdes and autonomous agencies.

vi. Obtained an understanding of cybersecurity and the situational analysis of cybersecurity in the country through a review of documents and discussions.

vii. Conducted Stakeholder Mapping and RACI Analysis.

viii. Reviewed Annual reports of BtCIRT – 2021-2022, 2020-2021, 2018.

ix. Visited the cybercrime unit of the RBP to assess cybercrime in the country in the following areas: 1) Legal framework, 2) Substantive Law, 3) Procedural Law, 4) e-Evidence, 5) Jurisdiction, and 6) Capacity.

x. Visited the city police station of the RBP and conducted a walkthrough of the procedures to handle cybercrime in the RBP.

xi. Analysed the criminalisation of offences in the ICM Act 2018 and Penal Code 2014 to determine the substantive law with regard to cybercrime in the county.

xii. Visited OAG to understand the legal framework for cybersecurity and the prosecution of cybercrime in the country, data protection and privacy, and the capacity of OAG to prosecute cybercrimes.

xiii. Referred websites of ITU, BtCIRT, ENISA, RBP, Gyalpozhing College of Information Technology, National Cyber Security Centre UK, Australian Cybersecurity Centre, U.S. Government Accountability Office, Cyber Security Agency of Singapore.

xiv. Visited BICMA to ascertain the legal and regulatory framework for cybersecurity and also to understand the role of BICMA as a regulator.

xv. Visited Bhutan Electricity Authority to ascertain the legal and regulatory framework of cybersecurity for the energy sector and the role of BEA in regulating the same.

xvi. Conducted a focus group discussion for CII Agencies to obtain a clear understanding of the cybersecurity posture in CII Agencies in order to determine the measures in place to secure and protect the critical infrastructure. 18 officials from 15 CII Agencies attended the focus group discussion.

xvii. Analysed data from the Incident Management System, and HR training data of ICT officials from July 2016 to November 2022.

xviii. Conducted a series of discussions with the BtCIRT to analyse existing methods for raising cybersecurity awareness at a national level. Consulted with the RMA and RBP and a focus group discussion with the CII agencies was held to understand their cybersecurity awareness-raising activities.

xix. Compiled information on all cyber drills, and cybersecurity awareness campaigns conducted in the country based on annual reports of BtCIRT and information obtained from BtCIRT. Evaluated the intensity, regularity and diversity of cybersecurity awareness practices based on the collected information from discussions, annual reports and other documents.

xx. Prepared a checklist to assess the incident handling mechanism for the country.

xxi. Review of privacy and data protection provisions in the ICM Act 2018.

xxii. Reviewed the Google Apps Enterprise Agreement.

xxiii. During the conduct of the performance audit, the RAA consulted the following agencies:

1. BtCIRT, DITT (Now Cybersecurity Divison, GovTech Agency);
2. Cybercrime unit, Royal Bhutan Police;
3. City Police Station, Royal Bhutan Police;
4. Office of Attorney General;
5. Bhutan InfoComm and Media Authority;
6. Bhutan Electricity Authority;
7. Royal Monetary Authority;
8. Bhutan Power Corporation Limited;
9. Druk Green Power Corporation Limited;
10. Bhutan Power System Operator;
11. Bhutan Telecom Limited;
12. Tashi InfoComm Limited;
13. Bank of Bhutan Limited;
14. Bhutan National Bank Limited;
15. Bhutan Development Bank Limited;
16. Druk PNB Bank Limited;
17. T Bank Limited;
18. Royal Insurance Corporation of Bhutan Limited;
19. GIC-Bhutan Reinsurance Company Limited;
20. Ministry of Education;
21. The Royal University of Bhutan;
22. Gyalpozhing College of Information Technology.

Chapter 2: Introduction

2.1. The Rationale for this Audit

Digital transformation is one of the significant drivers of organisational change, inspiring the public sector to initiate new ways of delivering services. Technology is now widespread bringing together data, processes, technology, and people to deliver high-quality and effective services for the citizens, public bodies, delivery partners, and service users.

Cybersecurity affects the daily lives of all Bhutanese citizens, whenever we use personal IT devices such as smartphones, WIFI networks, social media or electronic banking. The threat of electronic data loss from cybercrime, espionage and accidental disclosure has increased considerably, cumulating the risk of deliberate and accidental cyber incidents.

The performance audit of preparedness for cybersecurity has never been conducted and will be a first of its kind. This audit topic was identified in the Performance and Compliance Audit Topics 2021–2025 (Strategic Plan).

The following points give all the more reasons to conduct a performance audit to highlight the issues on cybersecurity and enhance the cybersecurity posture of the country.

a) Nation's Critical Information Infrastructure (CII)

The government agencies and our nation's CII such as energy production and transmission, ICT, and financial (banking) services—are dependent on IT systems and electronic data. The risks to IT systems supporting the nation's critical information infrastructure are increasing.

b) Major ICT initiatives and investments

The RGoB has implemented the national broadband network, national data centre, and the national payment gateway and many Bhutanese people have embraced cardless transactions. Similarly, with the corporate and private sectors, business agencies and individuals adopt digitisation for daily operations.

c) Increased digital usage due to the pandemic

More recently, due to the COVID-19 pandemic, the public sector and most businesses have adopted innovative measures for service delivery. Rapid digitisation does require forward-looking measures to boost cybersecurity.

d) Low capabilities

The ITU's report on the assessment of BtCIRT highlighted Bhutan's lack of necessary capabilities and competencies in dealing with cybersecurity incidents even at the level of government organisations.

e) Top management attitude towards cybersecurity

Despite the great engagement in ICT development, senior management perceives cybersecurity as a purely technological problem with limited impact on other domains.

f) Low awareness of cybersecurity amongst Bhutanese

Most of the Bhutanese public are not internet security conscious and are not well-informed on cyber hygiene.

g) Recent cyberattacks

The rate of compromise is increasing and the methods used by malicious actors are rapidly evolving. There are several cases of cyber-attacks in Bhutan resulting in major damages.

h) Disinformation

The spread of deliberate, systematic large-scale disinformation is an acute strategic challenge for our democracies.

i) Limited cybersecurity professionals

Currently, Bhutan has very limited experts and professionals in the cybersecurity field.

j) Conclusion

All of the aforementioned points give strong reasons for taking up the performance audit of preparedness for cybersecurity. If these vulnerabilities (aforementioned points) are exploited and not addressed, the implications and impact would be perilous for Bhutan as a country. A conclusion can be drawn from this audit on the country's preparedness for cybersecurity and the existence of an effective national cybersecurity framework.

2.2. Cybersecurity

The Information and Communication Media Act (ICM), 2018 defines Cybersecurity as *'protecting information, apparatus, ICT facilities, computer, computer network, and information stored therein from unauthorised access, use, disclosure, disruption, modification or destruction.'*

2.3. Importance of Cybersecurity

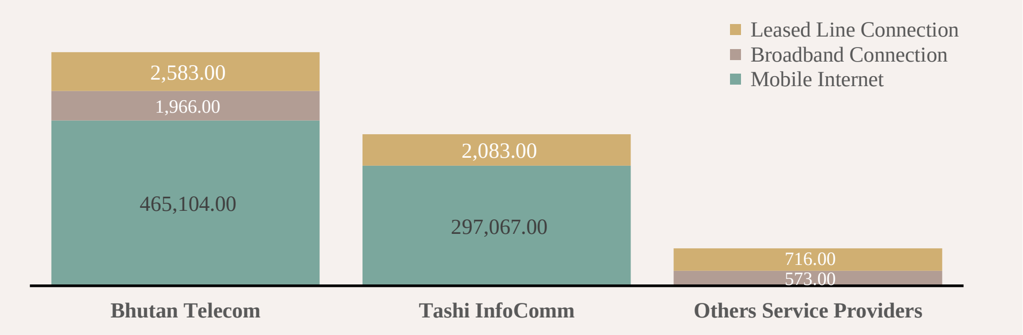
Cybersecurity concerns us all: individuals, businesses, and public authorities. With an increasing number of users, devices, and programs in the modern enterprise, combined with the increasing deluge of data – much of which is sensitive or confidential – the importance of cybersecurity continues to grow. The growing volume and sophistication of cyber attackers and attack techniques compound the problem even further.

2.4. Cybersecurity in Bhutan

Bhutan is becoming increasingly dependent on ICT, especially the Internet for performing the daily activities of governments, businesses, and individuals. In 2017, the ICT Development Index of the ITU ranked Bhutan 121 out of 176 countries.

The total number of mobile internet connections, broadband connections, and leased line connections in Bhutan, as of December 2021, by the service provider is depicted in figure 2.

Figure 2: Total internet connections by service providers



Source: BICMA Note: The Other Service Providers consist of Druk Comm, Supernet InfoComm, Bitcom Systems, Datanet Wifi, Nano and Nilo Fibernet.

A study assessing Bhutan's cybersecurity capability and maturity was conducted by the Global Cyber Security Capacity Centre and the World Bank in 2015. The study findings suggest that Bhutan is at the *start-up level of maturity*, meaning that Bhutan neither has the capacity nor has undertaken concrete actions to enhance cybersecurity.

2.5. National Cybersecurity Strategy

National Cybersecurity Strategy had been under development since late 2018 with initial support from the International Telecommunication Union (ITU). The ITU assessed the cybersecurity state in Bhutan and provided the necessary thrust area.

2.6. Challenges of Cybersecurity in Bhutan

Bhutan's cyber landscape is constantly changing and becoming unpredictable as more people, government, devices, systems and networks are getting interconnected. According to the ITU's experience, while developing Bhutan's first National Cybersecurity Strategy, some of the challenges in Bhutan are:

- ✓ Awareness of the importance of cybersecurity as digital transformation is a work in progress.
- ✓ Senior management perceives cybersecurity as a purely technological problem with limited impact on other domains.
- ✓ Gaining support and buy-in from stakeholders.
- ✓ Visibility, funding and key partnership.

Other challenges are:

- ✓ Lack of sufficient technical and managerial skills to initiate innovative growth in ICT businesses in the government and private sectors.
- ✓ Lack of appropriate national and global organisational structures to deal with cyber incidents
- ✓ Lack of awareness of cyber threats among Bhutanese increases the vectors that target the victims
- ✓ The idea of hiring foreign cybersecurity experts is not favoured due to the lack of trust when it comes to sensitive governmental information.
- ✓ The sale/use of pirated software is widespread in Bhutanese markets.

2.7. Legal Framework

The main legal document for cybersecurity is the ICM Act which was enacted in 2018. For cybersecurity, in particular, the ICM Act has provisions for the protection of online and offline privacy, cybersecurity and data protection, and offences including grading and penalties of computer offences. The Penal Code of Bhutan 2004 (amended 2021) is also referred to in conjunction with ICM Act 2018 if offence grading and penalties are not covered in the Act.

For the cybercrime investigation, the Civil and Criminal Procedure Code of Bhutan (CCPC) 2001 (amended 2021) and Evidence Act, 2005 are referred besides ICM Act 2018.

Chapter 3: Audit Findings

This chapter discusses the issues surrounding the cybersecurity ecosystem in Bhutan. These issues are categorised into five areas of Legal and Regulatory Framework; Institutional Framework; Cybersecurity Governance; Cybersecurity Awareness and Capabilities; and Incident Handling Mechanism as shown below:

Legal and Regulatory Framework

Legal and regulatory framework are the necessary instruments to address and counter the rise of cybercrime and related cyber-incidents, and to protect critical information infrastructure.

Institutional Framework

Effective and well-coordinated institutional framework is one of the key factors that determine the modus operandi of all stakeholders.

Cybersecurity Governance

Cybersecurity governance provides strategic direction to manage security and risk at a national level and build accountability frameworks.

Capacity Awareness and Capabilities

Cybersecurity capacity-building and awareness should take place on different levels – amongst government entities, citizens, businesses and other organisations – and should cover a wide spectrum of cybersecurity knowledge starting from basics to advanced technical knowledge.

Incident Handling Mechanism

Incident handling is crucial for organisations and the country to manage and enhance cybersecurity, and achieve security maturity.

3.1 Legal and Regulatory Framework

An integral component to ensure robust cybersecurity is the adoption of appropriate legislation – which is harmonised with regional and international policies and practices. Legal and regulatory frameworks are the necessary instruments that should be put in place to address and counter the rise of cybercrime and related cyber incidents and to protect critical information infrastructure. A framework as such cannot be limited to general cybersecurity conventions or regulations focused on certain cybersecurity issues but should have a broader perspective aiming to create a legal ecosystem focused on cybersecurity and data protection.

Accordingly, Section 8 (3) of the Information, Communications and Media (ICM) Act of Bhutan, 2018 mandates the Ministry of Information and Communication ((MoIC) to '*formulate legislation, policies, and plans related to ICT and media matters'* and *'approve Rules and Regulations to implement various provisions of this Act.*

The RAA, while assessing the existence and adequacy of the legal and regulatory framework for protecting and safeguarding citizens and their data, businesses, and critical information infrastructure, noted the following:

3.1.1 Legal Framework

The main legal document for cybersecurity or anything related to ICT for that matter is the ICM Act which was enacted in 2018. For cybersecurity, in particular, the act has provisions for the protection of online and offline privacy, cybersecurity and data protection, and offences including grading and penalties of computer offences. The Penal Code of Bhutan 2004 (amended 2021) is also referred to in conjunction with ICM Act 2018 if offence grading and penalties are not covered in the Act. For instance, if the offence is about stealing computer data, the person shall be guilty of possession of the stolen property and this offence is referred to in the penal code. For the cybercrime investigation, the Civil and Criminal Procedure Code of Bhutan (CCPC) 2001 (amended 2021) and Evidence Act, 2005 are referred besides ICM Act 2018.

3.1.1.1. Cybercrime

Cybercrime is any activity in which computers or networks are used as a tool, a target or a place of criminal activity. In other words, cybercrime consists of illegal activities committed in cyberspace that either uses ICT systems to commit the crime or that target ICT systems and the data they store. Developing cybercrime countermeasures requires building a sufficiently robust and flexible legal framework through legislative and regulatory action and that framework needs to provide law enforcement agencies with both procedural means and actual resources to combat cybercrime.

While reviewing the legal framework on cybercrime, the RAA carried out an assessment with the RBP on existing cybercrime laws. Additionally, the RAA consulted the OAG on several occasions for clarifications and confirmation of the reviews carried out by the RAA and the result of the assessment.

The RAA reviewed the following areas of the legal framework pertaining to cybercrime provided in table 1.

Table 1: RAA review and analysis of Legal Framework on cybercrime in Bhutan

Sl. No.	Areas
1.	Definition of Cybercrime
2.	Substantive Law
3.	Procedural Law
4.	Evidential
5.	Jurisdictional
6.	Treaties on Cybercrime
7.	Review and Gap analysis of legal instruments on Cybercrime

The review revealed that for substantive law, which consists of offences and prescribed penalties, there is no law, particularly for the criminalisation of cybercrime and criminal liability of cybercriminals. Nonetheless, the ICM Act 2018 and the Penal Code 2004 (Amended 2021) stipulate the offences, penalties or criminal liabilities for various types of computer-related offences including cyber terrorism.

However, the RAA observed certain deficiencies in other areas as follows.

i. *Definition*

There is no provision specifically defining cybercrime. The ICM Act 2018 does not identify cyber-related crimes like computer-enabled, cyber-dependent, cyber-enabled crimes etc.

ii. *Procedural law*

This law specifies what procedures need to be followed during the investigation and prosecution of the case. For cybercrime, like any other crime, CCPC 2011 (amended 2021) is referred to. The CCPC 2011 does not have legal provisions for access to computer data during the trans-border investigation and likewise, for trans-border prosecution, there is no legal provision for the preservation of stored data including computers or storage media.

iii. *E-evidence*

The Evidence Act 2005 provides the legal provisions in relation to e-evidence which states that evidence is inclusive of e-evidence. However, there are no legal provisions on storing/retaining and transferring e-evidence to prosecutors or courts. The RBP had developed and implemented a guide on the Computer and Mobile Forensic Field which includes the handling and transfer of e-evidence for investigation, and prosecution at the RBP level and by OAG.

iv. *Jurisdictional*

The cross-border and multijurisdictional aspects of cybercrime can make investigation difficult. Thus, a tie with other countries in the form of established conventions, and bilateral and multi-lateral agreements are crucial. International collaboration through conventions is vital to serve warrants to the suspect outside Bhutan and to have the right of extradition. However, the RAA noted that Bhutan does not have established mutual conventions or agreements with other countries besides India. According to RBP, cross-border cyber offences are dealt through International Criminal Police Organisation, commonly known as Interpol.

v. *Review*

The legal provisions on cybercrime has not been reviewed pending the approval of the National Cybersecurity Strategy (NCS). As per the draft NCS, three working groups are to be formed and one such working group is the Legal Framework Working Group (LFWG). The LFWG is required to review existing Acts, Rules and Regulations on cybersecurity, conduct a comprehensive gap analysis, and provide recommendations for strengthening the legal framework in addressing the new age cybercrimes and complexities and safeguarding cyberspace. Accordingly, the LFWG is to be led by PPD, MoIC and the OAG, as per the implementation plan in the NCS, to review and perform a gap analysis. As such, the adequacy and sufficiency of existing cybercrime law cannot be determined.

The BtCIRT, as the recognised agency for cybersecurity activities as accorded under the ICM Act 2018, had not been able to strengthen the existing legislation of cybersecurity.

The absence of an adequate legal framework on cybercrime would not only pose challenges to law enforcement agencies to combat and criminalise cybercrimes including cross-border investigations but also would make the country's cybersecurity more vulnerable to cyberattacks.

It was responded that the BtCIRT was formed in 2016 while the Bhutan ICM Act was endorsed by the government in 2018. However, between 2016 and 2018 the draft Bill remained with the government without the option to revisit the clauses. Since 2018, with the help of ITU, the BtCIRT has initiated the development of the National Cybersecurity Strategy, which includes Cybersecurity Legislation. In addition, BtCIRT did carry out an internal assessment of the gaps in the legal framework looking at the existing legal instruments, particularly the ICM Act 2018 and eGov Policy.

While noting the response provided by the BtCIRT, the RAA stresses that since the draft NCS is yet to be adopted, the inadequacies of the existing legislation remain to be addressed.

3.1.1.2. Privacy and Data Protection

With digital transformation, there is an increasing number of organisations collecting and processing personally identifiable information (PII). This demands that these entities protect information while balancing the need to make information available through digital services.

Personal data or information is a growing concern for customers, organisations, and regulators as it might pose data privacy risks such as unauthorised disclosure of data, data loss, phishing, fraudulent activities, and identity theft. Therefore, it is important that entities possessing personal data effectively safeguard personal data from data breaches while using it for the purposes required by the relevant laws and regulations.

The RAA examined the existence of legal instruments for privacy and data protection in consultation with the OAG and the DITT in the following areas provided in table 2.

Table 2: RAA Review of data privacy and data protection

Sl. No.	Elements of data privacy and data protection
1.	Key Definition
2.	Consent for Data Collection and Processing
3.	Data Disclosure
4.	Data Destruction
5.	Data Transfer
6.	Data Inventory
7.	Breach Notification
8.	Privacy Policy and Privacy Notice
9.	Privacy Impact Assessment

The results of the examination are discussed below.

- There are provisions (Section 384, 385 and 386) in the ICM Act on data protection, particularly for seeking consent while collecting and processing personal data, and for disclosure and destruction of data. Corresponding offences are also specified in the ICM Act.
- Section 336 to 346 of the ICM Act contains provisions on privacy including data protection and information sharing which covers ICT and Media facilities or service providers and vendors to respect and protect information including implementing a privacy policy.
- Section 271(4) of the ICM Act requires all Governmental agencies to conduct privacy impact assessments and ensure that sufficient controls are put in place to protect the privacy of sensitive personal information as it implements e-governance programmes.
- In the ICM Act, Section 464 (76) defines personal data or personal information and 464 (89) defines sensitive personal data or personal information.
- Additionally, the e-Government Policy for the RGoB 2019 stipulates the need for agencies concerned to '*safeguard the security of data, the privacy of users, and the confidentiality of information. The agencies concerned shall classify data based on its confidentiality to facilitate secure access of permissible data by other agencies.*'
- Further, MoIC had issued an executive order vide letter No. MoIC(M)-02/133 dated 1 July 2022 on protecting personal data and sensitive information. The agencies are directed to undertake seven actions comprising of data classification, collecting data for the stated purpose, ensuring confidentiality, not posting personal information on the website and social media, de-identifying or anonymised information, introducing privacy policy or notice, and instituting security measures. These actions are to be undertaken within three months.

The RAA conducted a focus group discussion with the known Critical Information Infrastructure (CIIs), consulted with the erstwhile DITT, and further verified the implementation of security measures to ensure privacy and data protection. It was found that the actual enforcement was not supplemented by adequate mechanisms. Specifically, the RAA noted the following:

i. There is no practice of obtaining consent while collecting personal data or information.

ii. There is no privacy policy implemented nor a privacy notice provided to the users/consumers by the data collecting and processing agencies.

iii. Privacy impact assessment as required for any e-government initiatives (any new G2C, G2B services after the enactment of the ICM Act or the national digital identity project) has never been carried out.

iv. There is no practice of data classification in the agencies as data inventories[1] are not performed by the agencies.

v. 39 agencies had submitted the action taken report on the seven actions as per the MoIC executive order. However, these actions are yet to be validated.

vi. Moreover, protection of personal data transfer to a third party and cross-border transfers of personal data outside of Bhutan are not provided in the Act.

vii. There is no obligation for the data controller to notify the regulator or the individual concerned in the event of a data security breach.

The RAA noted that the enforcement mechanism is lacking in design and operation to ensure compliance with the aforementioned legal instruments. Moreover, the MoIC executive order was issued four years after the enactment of the ICM Act.

Weak enforcement mechanisms for data protection and privacy will have operational risks for organisations. Moreover, the data subjects will become vulnerable to identity theft, and scams. These will ultimately increase reputational risk and loss of citizens' trust in digital services, hindering the nation's objective in digital transformation. Most importantly, data breaches at the government level would result in the security of the nation at stake.

The BtCIRT agreed that while ICM Act stipulates data protection and privacy, it is quite the contrary in practice in agencies across the board. The BtCIRT further responded that the MoIC initiated the push for limiting the sharing of personal and sensitive information online by issuing the executive order on 1 July 2022. They mentioned that there should be a balance between the need to protect the organisational and citizen data while ensuring it does not inhibit innovation and digital transformation.

The Department also stated in its response that they have started working on developing data management guidelines that will cover best practices related to data governance and data management. Currently, the department is working with the support of the World Bank.

Although there are adequate legal provisions for data privacy and data protection, the inadequacies in the enforcement mechanisms had inhibited the effective enforcement of the intent of, and compliance with, the ICM Act.

3.1.2 Regulatory Framework

A strong regulatory framework for cybersecurity is important to provide effective and strong enforcement mechanisms to ensure compliance with various provisions of the law and also to safeguard information and computer networks from cyberattacks. Recognising the importance

[1] Data inventories are performed to identify

- the personal data processed by the organisation
- the processes that use (collect, store, disclose, transfer, etc.) personal data
- the systems involved in the processing
- the persons involved in the processing (including employees who have access to the data as well as external recipients).

of cybersecurity, the Bhutan InfoComm and Media Authority (BICMA) Act 2006 was repealed and a new ICM Act was enacted in 2018 with provisions for cybersecurity.

Besides Acts, it is also imperative for the regulating agencies to develop or revise rules and regulations, policies and guidelines aligning with the Act for effective enforcement of the various provisions stipulated in the Act.

On review of the existing regulatory framework for cybersecurity, the following observations were noted:

i. Although BICMA is identified as an autonomous regulatory authority and entrusted to regulate ICT and media facilities and services, BICMA currently regulates only telecommunications and ISPs. Besides BICMA, the Royal Monetary Authority (RMA) is the regulatory body for financial institutions including cybersecurity.

ii. The RAA also noted that BICMA does not have codes of practice and standards established to ensure that required cybersecurity measures and systems are in place by the owners of critical information infrastructure even though the ICM Act stipulates the need to prescribe, regulate and monitor compliance with national codes and standards pertaining to ICT. Nonetheless, BICMA, as the regulator of ISPs and Telecommunication Operators, and a few agencies concerned along with BtCIRT have initiated framing laws and regulations as shown in table 3.

Table 3: Rules and Regulations to implement the ICM Act

Sl. No.	Rules and Regulations, Policies and Guidelines	Developing Agencies	Status
1	eCommerce Policy	Ministry of Economic Affairs	Drafting
2	National Digital Identity Act	Application Development Division, DITT, MoIC	Drafting
3	Child Online Protection guideline	BtCIRT, DITT in consultation with stakeholders including National Commission for Women and Children	Drafting
4	Data Governance, privacy and protection	Application Management Division, MoIC	Drafting
5	Rules and Regulations for Licensing and Operations of ISPs	BICMA	Developed
6	Licensing Terms and Conditions for telecom operators	BICMA	Revised but not yet enforced. It is to be enforced from 2023.
7	Guideline on Data Privacy and Data Protection 2021	RMA	Developed

Source: BtCIRT, BICMA, RMA

As shown in table 3, even after four years since the enactment of the ICM Act, most of the regulations are in the drafting stage and not implemented yet to give effect to the cybersecurity provisions in the ICM Act 2018.

iii. With regard to established codes of practice and standards for cybersecurity, it is of utmost importance for critical information infrastructure operators, operators of essential services, digital service providers, and public administrators to comply with and meet the established requirements. However, the RAA noted that the Ministry is still in the process of identifying critical information infrastructure.

iv. In the case of financial institutions, the RAA noted that the RMA had issued a directive vide letter No. RMA/DIT/Cybersecurity/1819/5857 dated 2 April 2019 to put in place a robust cybersecurity framework in all financial institutions. Through this directive, the banks are required to:

1. Implement EMV[2] at the ATMs and PoS terminals;
2. Replace magnetic strip-based cards with EMV chip and PIN-based cards;
3. Cybersecurity measures and responses: to assess compliance to PCI-DSS and may even consider compliance to ISO 27001;
4. Formation of a Financial Institutions Cyber Response Team (FICRT); and
5. Implement basic cybersecurity controls and measures.

The RMA also conducts regular on-site inspections to check compliance with the directives. Further, the financial institutions are required to submit the status quarterly.

v. With regard to Internet Service Providers (ISP), the Rules and Regulations for licensing and operation of ISP in Bhutan 2021, section 3.4.1b requires the ISPs to “Install in its ISP system the required certified cybersecurity systems to ensure resilient cybersecurity features”. Even though there is a requirement, there are no specific mechanisms instituted by BICMA to assess and validate whether the required certified cybersecurity systems are implemented by the ISPs.

Currently, the requirement is not included in the terms and conditions of the license. Since the previous BICM Act 2006 did not have specific provisions on cybersecurity, the Telecom License Terms and Conditions developed and signed in 2007, did not have specific clauses on cybersecurity. It was noted that BICMA has incorporated the requirement for cybersecurity systems under the ‘*Obligations for Telecom providers*’ provision in the new Telecom Terms and Conditions which is stated to be signed during the license renewal falling due in 2023. Nevertheless, BICMA has not renewed the terms and conditions to incorporate the provisions on cybersecurity immediately following the enactment of the ICM Act in 2018.

For cybersecurity, it is apparent that there is no strong regulatory framework instituted by regulatory bodies. In absence of a regulatory framework, cybersecurity cannot be ensured exposing our computer systems and networks to cyber-attacks. Most importantly, it is of great concern, if the critical sectors and essential service providers fall victim to cyberattacks, then the energy, financial, and banking services could be disrupted. Citizens could be denied or delayed in accessing critical resources like electricity and access to their bank accounts. Ultimately, the consequences could be devastating with the potential to cripple national security.

The BICMA stated that the ICM Act of Bhutan 2018 does not mandate the Authority to regulate cybersecurity in the country. In fact, section 382 and 383 of the Act clearly states that BtCIRT shall be established as the national agency to coordinate cybersecurity activities and be a central point of contact on all cybersecurity matters pertinent to

[2] EMV is short for Europay, Mastercard and Visa. EMV cards store cardholder information on a metallic chip instead of in a magnetic stripe. These chips can only be authenticated by special readers, making them more secure than stripe-only cards. A primary benefit of EMV chip technology is preventing counterfeit fraud.

national security in the country. Moreover, the BtCIRT shall also establish policies and procedures to implement its functions under this Act.

Additionally, the BICMA has been prescribing codes and standards pertaining to ICT and Media services in addition to ICM Act. However, the codes and standards for the CIIs could not be established since the CIIs are yet to be identified.

Moreover, BICMA is of the view that there will be CIIs under the jurisdiction of other regulating agencies like RMA and BEA which will monitor respective CIIs under them.

Despite limited competence in cybersecurity, BICMA periodically monitors the service providers to ensure the implementation of cybersecurity measures, including getting information on the cybersecurity measures installed and field inspection of their ICT facilities.

All the telecom services providers and ISPs have required firewalls. Should ISPs require any additional security arrangements, the requirements should come from the financial or energy sectors which are not communicated to date.

In the absence of a specific agency taking a lead role to regulate cybersecurity, there is no assurance that the critical information infrastructure is properly identified and secured. Such a disintegrated approach may lead to a diffusion of responsibilities in ensuring the implementation and enforcement of cybersecurity requirements and thus, exposing the CIIs to perpetual vulnerabilities and threats.

3.1.3 Mandatory Cyber Incident Reporting

Timely reporting of cyber incidents to both internal and external stakeholders plays a critical role in providing the opportunity to understand the threat environment, assess the impact on the organisations, and strengthen the contingency plans and procedures, thereby enhancing the resilience to cyber threats.

A defined threshold for reporting cyber incidents, a timeframe and an appropriate channel will enable the relevant entities to provide timely assistance to the victim, investigate cyber-attacks and provide immediate actions to mitigate the effects. Additionally, it will enable the response team to keep abreast of the developing cyber threats, enhance a better response plan, work in partnership with the relevant entities, and educate and mitigate against cyber threats that can impact critical services and businesses.

Furthermore, the categorisation of cyber incidents is also important to better manage the allocation of resources to the containment and remediation of incidents. The following are additional benefits of institutionalising cyber incident reporting:

- ✓ Coordinating response and quick dissemination of information among interested parties;
- ✓ Providing access to a wide pool of expertise about incidents that national authorities can follow up with the infrastructure managers in a regulatory capacity;
- ✓ Analysing threats and risk profile;
- ✓ Identifying good response and recovery practice through documenting lessons learnt;
- ✓ Enhancing stakeholder’s knowledge of the actual security problem at stake;
- ✓ Preventing incidents; and
- ✓ Enabling categorisation and prioritisation.

Therefore, a regulation requiring critical infrastructure entities on what, when, how and whom to report cyber incidents would encourage to report cybercrime and the government to understand the threat environment. Further, it will enhance the resilience of the public communication network and the ability to respond to future cases and strengthen the contingency plans and procedures.

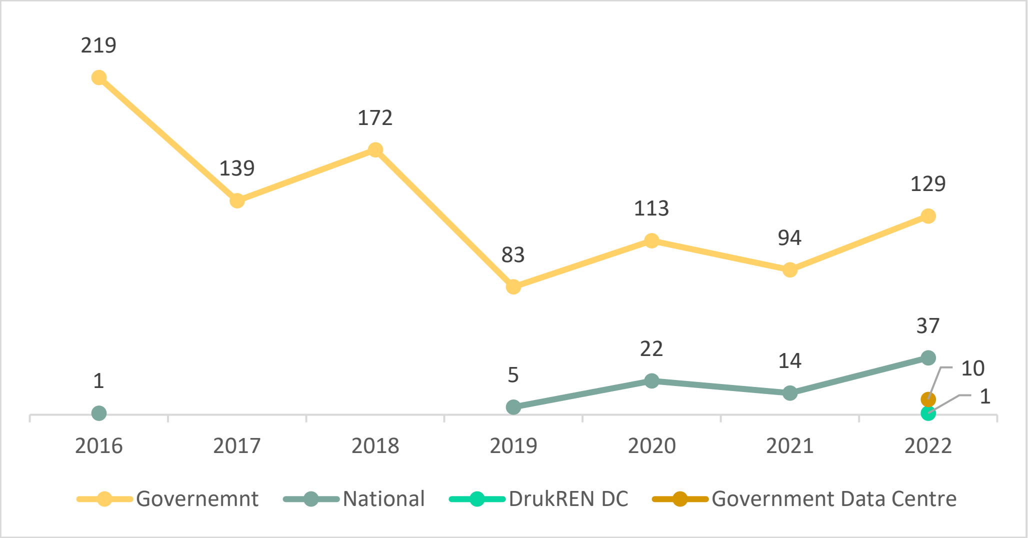
The RAA reviewed the established policies in terms of incident reporting and observed the following:

i. The e-Government Policy for the Royal Government of Bhutan, section 5.5 clause 5.4.4 includes, "*MoIC (BtCIRT) shall coordinate incident handling related to cybersecurity. MoIC shall also develop guidelines concerning the protection of privacy and confidentiality of data, and disseminate information on cybersecurity threats received from both regional and international bodies. In the event of security threats found by agencies, the concerned agency shall alert and properly report it to the BtCIRT.*"

   However, the threshold and timeframe to report cyber incidents for critical infrastructure or government agencies are not identified. Moreover, the types of cyber incidents that should be reported are also not defined in the policy.

   The cyber incidents reported from 2016 to 2022 are depicted in figure 3 below and the graph shows that the number of incidents reported by constituent *'National',* which is incidents reported other than government agencies, is significantly lower than that of *'Government'*.

Figure 3: Incidents reported by Constituencies by year



Source: RAA analysis of incidents recorded in Incident Management System

ii. For instance, if there is a cyber incident, the general practice is to report it to their ISP and not BtCIRT.

iii. The RMA has developed a *'Guideline on Data Privacy and Data Protection 2021'* to provide standard guidelines for Financial Service Providers (FSP).

   The guidelines require FSP to implement data breach management procedures as a part of the information security incident management process. Clause 4.11.4, *'FSPs shall report personal data breaches to Authority within 48 hours of becoming aware of the data breach,'* defines the timeframe within which the incident should be reported. The guideline also mentions the required information while reporting breaches and the need to maintain breach records with sufficient information.

However, the RAA learnt that the guideline was issued on 18 July 2022 and FSPs are in the process of implementing the guideline. Furthermore, FSPs have stated that they have not encountered any cyber incidents except for some instances of online financial/investment scams. Such scams are shared informally with the BtCIRT and FICRT in social media groups to disseminate the scams and corresponding preventive measures.

In the future should there be any cyber incidents, the RMA is planning to report and share the incident with the BtCIRT after checking the nature and confidentiality of the incident and with consent from the FSPs.

Cyber incidents in Bhutan are often unreported because of the lower number of cyber victims, less awareness of cyber threats, and potential disclosure mechanisms not being made clear to the population.[3] Additionally, the lack of identified critical information infrastructure and mandatory requirement of reporting cyber incidents along with the defined timeframe, and low visibility of BtCIRT have resulted in confusion among the entities regarding what, when, how and whom to report cyber incidents.

If the entities are not encouraged to report cyber incidents, it will be difficult to design better responses and understand the threat and risk profile of the country. Also, the resource allocations, contingency plans and policy development, and building of capacities to mitigate and respond to cyber incidents will be affected thus, affecting the cyber resilience of the country against cybercrime.

The BtCIRT responded stating that the strict timeline and threshold for Critical Agencies cannot be defined since the BtCIRT cannot designate agencies as critical agencies through risk assessment and development of acceptance criteria.

In absence of protocols for cyber incident reporting, there is a lack of common understanding among the agencies to report cyber incidents and in the process, many cases would go unreported. At the national level, it would be difficult to assess the country's threat environment and design strategic responses to cyber-attacks.

3.1.4 Data Security in Google Workspace

The Google Apps/G Suite, which consists of tools such as Google Docs, Slides, Sheets, and Mail was deployed by the Government on 27 January 2014 for effective communication and collaborative engagement to gain efficiency and save resources. The adoption of Google Apps/G Suite came after approval by the Cabinet as per letter No. C-3/16/204 dated 12 December 2013. Accordingly, the contract between the MoIC and Google was signed on 30 December 2013.

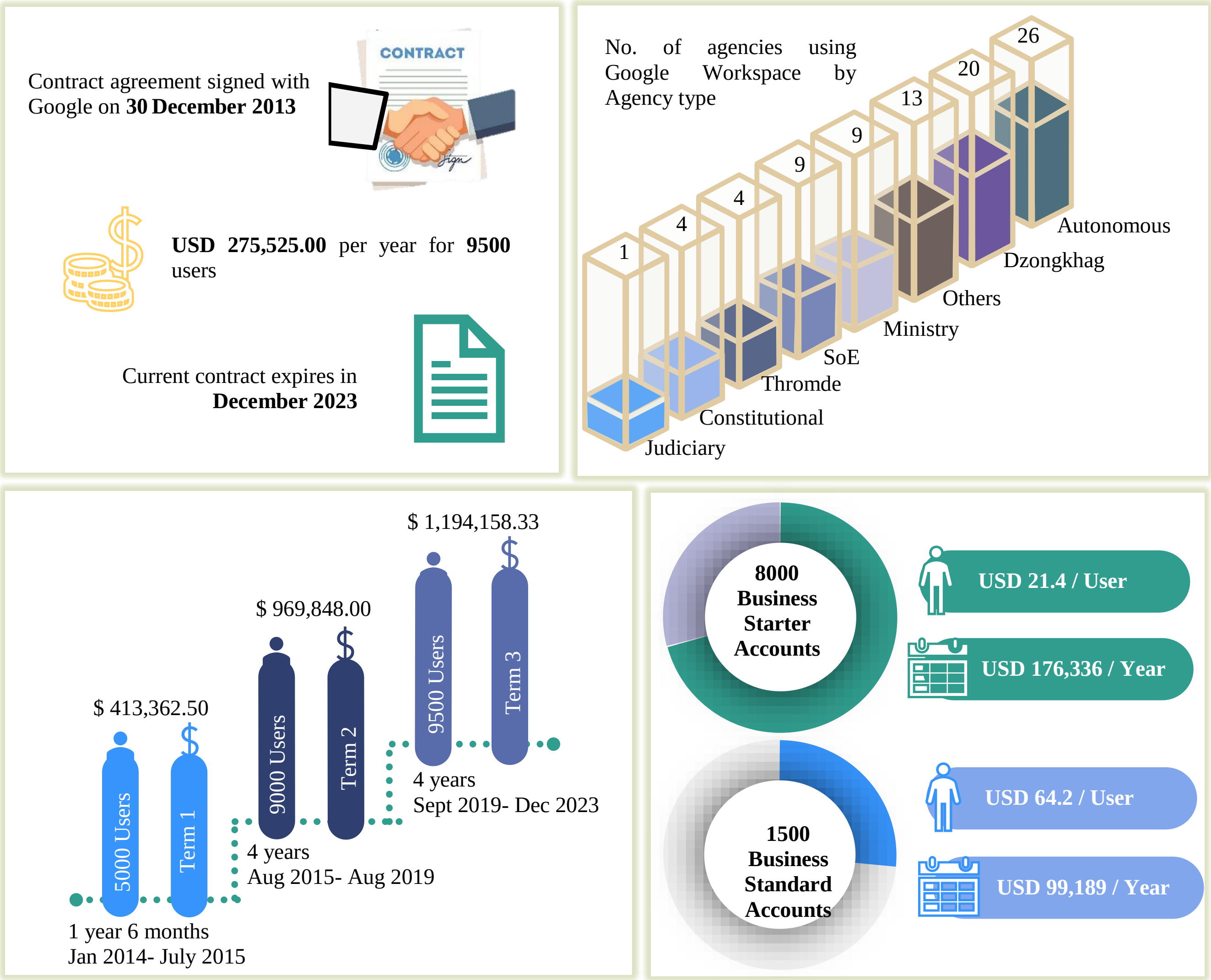
In 2020, Google Apps/G Suite was rebranded by Google into Google Workspace, and accordingly, Google recommended the government migrate to Google Workspace. The move was recommended by Google based on the following:

[3] Global Cyber Security Capacity Centre

- ✓ The newer features of Google Workspace would not be available for customers on legacy pricing models;
- ✓ Google Meet recording feature (which was available only for enterprise license holders) was added to the Business Standard Plan; and
- ✓ Pooled storage was possible for Business Standard Plan, although unlimited storage is discontinued. This also comes with the flexibility to provide the correct storage as per the requirement of the users.

As per the Note for Approval to the Hon'ble Prime Minister dated 25 December 2020, a total of 9500 users in 87 agencies (Government and SoEs) are registered with access to secure email and productivity tools in Google Workspace. The details are provided in figure 4.

Figure 4: Google Workspace Contract Agreement details and Usage



Source: The GovTech Agency

As per the Note for Approval, the user accounts are made up of two new subscription plans which consist of the Business Standard plan, which is provided to officials at the P1 level and above, and the Business Starter plan which is provided to the remaining users and were offered by Google for the same price as the previous plans.

The Note for Approval also stated Google has agreed to allow the government to subscribe 8000 users to the Business Starter Plan beyond its ceiling of 300 users. Above this ceiling, organisations would have to move to the Enterprise Plan at a very high cost. Google Workspace for Education has also been provided free of cost by Google for the duration of the license. A total of 187,306 Google Workspace for education users are active as of 13 December 2022 and are assigned to schools, (teachers, supporting staff and students), Dzongkhags (Dzongkhag education officials), Ministry of Education (ministry officials), and RUB Colleges.

The benefits of deploying Google Workspace are apparent and the huge investment made by the government has led to efficiency and the saving of government resources. The Google Workspace for education has also enabled access to education during the Covid-19 pandemic. When the RAA enquired about the legality of storing government data in the cloud since such practices are prevalent, the DITT responded that the terms and conditions of the contract with Google have been vetted by the OAG and the DITT further added that only authorized users with right credentials can see the contents of the email, Google docs, and other productivity tools, and is far more secure than any other solution providers within the region. Additionally, the DITT stated that it was more economic and secure to store sensitive data online in Google servers when compared to hosting it in Bhutan.

Through the RAA's enquiry and review of the contract documents, the following was noted.

i. Consent to transfer, processing and storage

Clause 1.1. Services, Facilities and Data Transfer, of the Google Apps Enterprise Agreement between the MoIC and Google, states that *"....As part of providing the Services, Google may transfer, store and process Customer Data in the United States or any other country in which Google or its agents maintain facilities. By using the Services, Customer consents to this transfer, processing and storage of Customer Data."*

The OAG, in its review of the agreement, raised concern regarding this clause through letter No. OAG/LSD/806 dated 25 November 2013, stating that since the definition of Customer Data as per Google referred to Customer's Confidential Information, the consenting to the processing of such confidential information would have to be "*thought over*" before signing the agreement.

Despite raising concerns by the OAG, the MoIC made no changes to the clause and signed the agreement with Google on 30 December 2013. Agreeing to the clause could result in confidential government information being exposed to data processing by Google.

ii. Data Protection Impact Assessment

The General Data Protection Regulation (GDPR) of the EU defines a Data Protection Impact Assessment (DPIA) as *"Where a type of processing, in particular, using technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. A single assessment may address a set of similar processing operations that present similar high risks."*

A DPIA is designed to identify and minimise risks arising from the processing of personal data and consists of:

a) Identifying the personal data handled by the system or process, as well as the reasons for collecting the personal data;

b) Identifying how the personal data flows through the system or process;

c) Identifying data protection risks by analysing the personal data handled and its data flow against data protection best practices;

d) Addressing the identified risks by amending the system or process design, or introducing new organisation policies; and

e) Checking to ensure that identified risks are adequately addressed before the system or process is in effect or implemented[4]

Contrary to the international best practices, while deploying the Google Workspace, the MoIC did not conduct a DPIA. In place of a DPIA, during the initial adoption of Google Workspace, the DITT conducted sensitisation to restrict the uploading of sensitive data or information by the users. However, it was left to the organisation to determine which data or information to be considered sensitive.

Without DPIA being conducted, the risk of getting government data exposed to unauthorised data processing by service providers cannot be assessed and appropriate corrective actions cannot be instituted.

Despite bringing in operational efficiencies, the security of using Google Workspace in the RGoB and SoEs, is a concern particularly in terms of data privacy and protection.

The DITT responded that in 2013, there were only two companies that provided collaborative suites for offices: Microsoft (Office 365) and Google (G-Suites). The DITT, MoIC conducted a study and presented it to the government and approved in 16 Lhengye Zhungtshog held on 4 December 2012 vide letter No. C-3/16/204 dated 12 December 2013. However, the last renewable quotation was requested from Microsoft.

The DITT stated that by agreeing to these clauses, it is the responsibility of Google to ensure our data is stored and transferred securely, is timely, and ensures our services (mail and collaboration suites - documents, drive, calendars) are full. Google is not allowed to process our data for advertising purposes and should RGoB stop using their services, Google needs to transfer all our data and destroy all copies since they are GDPR compliant. However, since Google is registered in the USA and falls under the FISA act, our communication data may be shared with the US government if someone is somehow found connected to terrorism activity and poses national security to the US government.

We acknowledge the concern raised by the RAA on data protection and data security using Google Workspace, on the contrary, the adoption of the Google Workspace (then G-suites) for the government was to ensure our communication data is protected at the highest international standards. For the record, in 9 years of Google Workspace used, officially or unofficially, our data has never been breached.

As Google Workspace is on the cloud, there is a risk to data security and privacy as government agencies are storing information in Google Workspace. Since there is no data classification at the national as well as agency levels, the confidentiality of sensitive information may not be ensured as agencies use Google Workspace for processing, storing, and communicating all official information.

[4] Guide to Data Protection Impact Assessment, Personal Data Protection Commission, Singapore

3.2 Institutional Framework

Building upon the basis of a strong and mature legal framework, robust cybersecurity requires an institutional framework that supports the legislative and executive mandates created under the legal framework, appropriately assigning specific roles to various agencies involved in the cybersecurity system.

Organisational measures include ensuring that cybersecurity is sustained at the highest level of the executive and assigning relevant roles and responsibilities to various national entities and making them accountable for the national cybersecurity posture.

Recognising the importance of an institutional framework, the RAA reviewed the adequacy of the institutional framework for cybersecurity, evaluated the cooperation and information sharing between different stakeholders based on best practices, and noted the following:

3.2.1 Coordinating Leadership to provide Strategic Direction and Steer Strategies for Cybersecurity

The responsibility and accountability for improving and ensuring the effectiveness of cybersecurity governance rest at the highest level which in our case would be the high-level governance committee as per the draft NCS. The committee is required to provide a strategic view in controlling security, defining and managing risks, building accountability frameworks and establishing who is responsible for making decisions. Further, the governance committee is tasked to manage and oversee the cybersecurity team responsible for mitigating the cyber risks and establishing and maintaining a security framework to ensure that the security strategies including information security strategies align with and support the national objectives.

The essential functions of the cybersecurity governance committee are to:

- Develop and maintain appropriate cybersecurity programs;
- Understand cybersecurity regulations, document ownership of regulatory compliance and address regulatory requirements through the development, execution, and maintenance of best practices;
- Serve as a forum for discussion, updates, and upgrades related to information security initiatives, security policies and procedures, security controls, security metrics and KPIs, current security assessment and investigation of data security risks, and strategic security issues.

Some of the benefits of establishing a cybersecurity committee are:

- Effective management of risks including internal and external threats and vulnerabilities;
- Enhance compliance initiatives to meet all relevant regulatory requirements;
- Ensure successful response to advances in technology, shifts in security regulations and best practices, and changes in key security leadership;
- Enable intelligent and optimal allocation of security budget based on national security needs and priorities.

An effective governance committee would provide valuable high-level authoritative attention and collaborative guidance for the security programs. Therefore, a governance committee should be established with a formal role and defined process for governing the national information security program.

The draft NCS emphasises the need to establish Cybersecurity Governance Structure with clear roles and responsibilities in collaboration with both corporate and private partners. Accordingly, the strategy considers the existing High-level ICT Steering Committee as *'the highest governing and decision -making body to oversee the implementation of cybersecurity strategy as well as any new cybersecurity initiatives.'* The High-level ICT Steering Committee comprises of following members:

1. Prime Minister (Chairperson)
2. Minister, MoIC
3. Secretary, MoIC
4. Secretary, GNHC
5. Chairperson, RCSC
6. Governor, RMA
7. Eminent Independent member
8. Director, Royal Office of Media
9. Director, DITT

The High-Level ICT Committee is to oversee the implementation of NCS and govern the three working groups formed as per the strategy. However, the RAA observed the following:

i. The draft NCS has proposed to leverage the existing High-Level ICT Steering Committee as High-Level Cybersecurity Governance Committee, considering cybersecurity as a subset of Information Technology instead of treating it as a distinct field from ICT which would attract equal attention and focus in terms of allocating resources and providing strategic direction;

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

iii. There are no documents to indicate the involvement of High-level Cybersecurity Governance Committee members to provide strategic direction to ensure legal and regulatory framework, to protect critical information infrastructure, and for robust incident handling mechanisms in the country.

The lack of an effective cybersecurity governance committee would result in decision-making without focus and management support. Further, there could be the risk of not giving adequate focus and attention to cybersecurity strategies and programs which could potentially result in a weak cybersecurity posture of the country.

Moreover, successfully translating the national cybersecurity strategy and vision into action requires the support and commitment of an effective cybersecurity governance committee that can make decisions about allocating resources, prioritising and providing directions for implementing cybersecurity activities in the country.

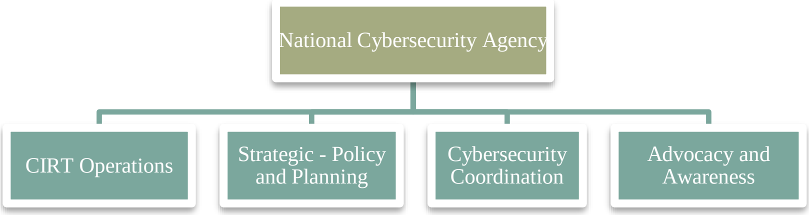
The BtCIRT explained that the membership and functions of the High-Level ICT Steering Committee were updated from that of the eGovernance framework. The committee discusses all ICT matters of importance including cybersecurity. The BtCIRT further explained that approval related to cybersecurity programs and issues will be through the existing High Level ICT Steering Committee.

3.2.2 National Agency for Cybersecurity

The national agency to ensure the cybersecurity of the nation must implement a comprehensive cybersecurity strategy, perform effective oversight, secure government systems, and protect cyber critical infrastructure, privacy, and sensitive data. The agency should be able to provide comprehensive national situational awareness and adequate incident responses. Thus, the agency should have clear mandates with statutory power and sufficient resources.

To manage cybersecurity at the national level, the organisation structure should be adequately designed. Figure 5 shows an example of an organisational structure of an agency with different units established to effectively carry out their multiple functions.

Figure 5: Organisational structure of a National Agency for Cybersecurity


National Cybersecurity Agency
CIRT Operations
Strategic - Policy and Planning
Cybersecurity Coordination
Advocacy and Awareness

Source: RAA depiction based on RAA review of organisational structures for a national agency for cybersecurity

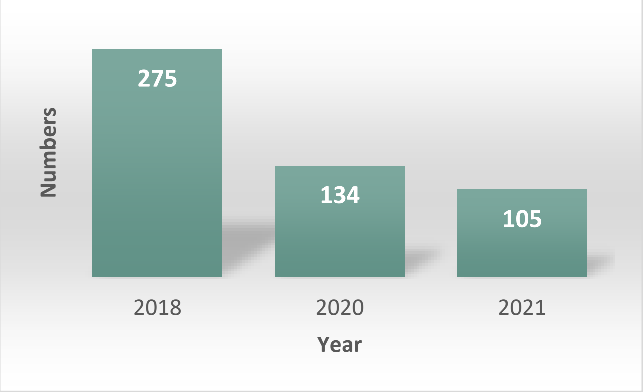
The BtCIRT was established in May 2016 as a national and governmental Computer Incident Response Team. It was upgraded to a division in 2021. As per the ICM Act 2018, the BtCIRT '*shall serve as the national agency to coordinate cybersecurity activities and be a central point of contact on all cybersecurity matters pertinent to national security in the country'*. Further, the BtCIRT is required to establish policies and procedures required to implement its functions entrusted by the act. As per the government order on the establishment of BtCIRT, some of the functions of the BtCIRT are to act as a central agency for cybersecurity, BtCIRT is expected to seek a vibrant business environment supporting the government in assessment, management and prevention of cybersecurity-related emergencies and coordinate incident response efforts. The security and vulnerability assessment of government systems will enable quick and efficient responses to cyberattacks, regaining control and minimising damage.

As per the Government order vide C-2/104/310 dated 20 May 2016, to further strengthen the cybersecurity in the country, the MoIC was entrusted with the responsibility to govern and supervise the BtCIRT's activities and ensure adequate capabilities in terms of human, technological and financial resources.

BtCIRT as a national point of contact for cybersecurity has carried out the following activities.

1. Drafted the NCS.
2. Handled cybersecurity incidents from both internal and external sources. In the past three years, from 2018-2021, a total of 514 incidents were handled as shown in figure 6.

Figure 6: Total incidents handled



Source: BtCIRT Annual Reports

3. Conducted Advocacy and Awareness programs using various means such as animation videos, media channels like BBS and posters.
4. Published security advisories and alerts on its websites and Facebook page to keep its constituents informed on cybersecurity news and vulnerabilities.
5. Tried identifying the CIIs in consultation with Task force members from Bhutan Power Corporation, TashiCell, Bhutan Telecom, Royal Monitory Authority and critical government sectors.
6. Organised and hosted workshops, drills and exercises related to cybersecurity.
7. Collaborated with international organisations in enhancing cybersecurity and implementations.
8. Hosted the monitoring system in Government Data Centre (GDC) for attacks and vulnerabilities with timely reports on the GDC operating team along with system administrators.
9. Periodic security assessment of government systems and on request for non-government systems.

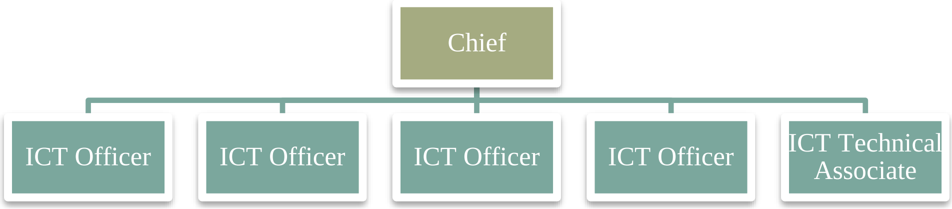
The RAA also observed some discrepancies in carrying out their functions;

i. In 2015, an assessment was carried out on cybersecurity maturity by the Global Cybersecurity Capacity Centre (GCSCC), University of Oxford before the enactment of the ICM Act. The GCSCC recommended providing mandates and assigning the erstwhile DITT as the coordinator for cybersecurity issues and to take lead in the development of a national cybersecurity strategy. Further, the assessment team made it clear that DITT should be differentiated from BtCIRT and their functions should not overlap with the BtCIRT, which is responding to incidents. Nonetheless, BtCIRT is functioning as a division of DITT.

ii. The ICM Act 2018 recognises BtCIRT as the national agency and mandates BtCIRT to coordinate cybersecurity activities and be a central point of contact on all cybersecurity matters at the national level. BtCIRT has now the dual responsibilities of being the national coordinator for cybersecurity as well as carrying out Computer Incident Response Team (CIRT) operations.

iii. On further review of the organogram of BtCIRT in terms of capacities, the RAA found out that the division has only five staff as portrayed in figure 7.

Figure 7: Organogram of BtCIRT



Source: DITT Website

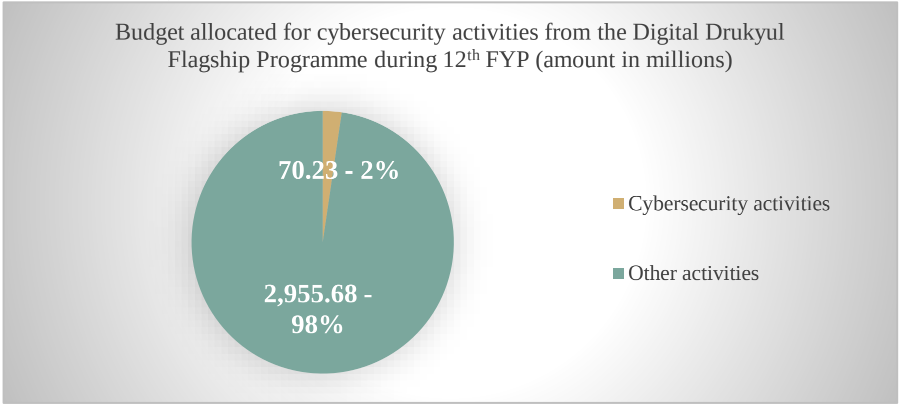
There were only two ICT Officers with master's degrees in cybersecurity.

iv. The 11th FYP identified the lack of qualified professionals, particularly in specialised ICT skills such as network security, cyber laws, software development and programming in the ICT. Accordingly, the creation of a talent pool and strengthening ICT human resource management were prioritised but apparently, the knowledge gap still exists in BtCIRT.

v. Although BtCIRT was upgraded to a division in 2020, the staff strength remained the same. Considering the current staff strength, BtCIRT does not have the resources to address and focus on strategic areas or activities for achieving effective cybersecurity in the country.

vi. Furthermore, the RAA noted that the division does not have adequate financial support to carry out its activities. Additionally, on review of the Digital Drukyul Flagship Programme from the 12th FYP, only 2.3% (Nu. 70.23 million) of the budget accounts for the outputs pertaining to enhancing cybersecurity (Safety of national cyberspace and environment strengthened and the Capability of ICT industry enhanced) of the flagship programme. Figure 8 depicts the budget allocation.

Figure 8: Budget allocation for cybersecurity activities



Source: Digital Drukyul Blueprint

On further review of the expenditure incurred by DITT, it was noted that only Nu**. 3.20 million** was expended on activities related to cybersecurity during the 12th FYP till 2020-2021.

Although BtCIRT has critical responsibilities for securing and strengthening the nation's resilience against cyberattacks through the development and implementation of national-level cybersecurity policies and strategies, spearheading cybersecurity awareness including responding to incidents, the division is not equipped with adequate resources to shoulder its roles and responsibilities to function as the national authority for cybersecurity. This is because, before the establishment of BtCIRT, the Ministry and the DITT have not assessed if the division has adequate capabilities in terms of human, technological and financial resources to effectively carry out their functions.

With the existing organisational arrangement of the BtCIRT, the development of NCS which was initiated in 2018 as a roadmap for cybersecurity is still in the draft stage and more than half of the operational period of the strategy has elapsed. Furthermore, BtCIRT is not able to take up the major role in strengthening cybersecurity in an integrated and coordinated manner. Their functions are still mostly limited to incident management response and conducting awareness programs.

When the national agency is not sufficiently equipped to manage the cybersecurity of the nation, the nation will become more vulnerable to cyberattacks ensuing into severe reputational damage and loss of trust. Ultimately, the national cybersecurity efforts would be derailed impeding the country's cybersecurity posture.

In their response, BtCIRT stated that with the recent transformation initiatives, the need for the National Cybersecurity Agency with increased manpower was discussed but it was instructed to be placed under the GovTech Agency as the creation of more agencies is not recommended.

The BICMA, in their response, argued that the provision of the ICM Act mandates to regulate only those ICT facilities and service providers licensed by BICMA. There is no mention of requiring to regulate the service provided by the Government agencies unless they are licensed by BICMA. Further, BICMA stated that they do not have full authority to monitor the e-services since they do not issue licenses for the e-services.

Given the current status, the RAA feels that the BtCIRT is not capacitated in terms of both human and financial resources to perform its functions in strengthening the cybersecurity posture of our country.

3.2.3 Institutional Linkages for Cooperation and Information Sharing

3.2.3.1 Institutional Linkages

Cybersecurity is a cross-cutting issue that affects or involves all sectors using ICTs and engaging in cyberspace. Thus, it is important to establish an integrated and coordinated approach involving key stakeholders having different experiences and expertise to improve the cybersecurity posture of the country to safeguard its critical infrastructures, high-priority sectors, and government services. It is also essential in the response to and recovery from cybersecurity incidents.

Further, a comprehensive national cybersecurity effort requires the establishment of coordination and cooperation linkages through which stakeholders can collaborate in the development and refinement of cybersecurity policy and cooperate in the management and implementation of cybersecurity operational efforts.

Such an enabling environment depends on robust institutional mechanisms and instruments with vertical and horizontal coordination of actions. Therefore, as mandated in the ICM Act 2018, BtCIRT must coordinate and engage with relevant/key stakeholders in securing the cyberspace of the nation. The stakeholders pertaining to cybersecurity and their roles are detailed in table 4:

Table 4: Stakeholders and their roles in securing cyberspace

Stakeholders	Role
Ministry of Information and Communication	• Guide BtCIRT in the formulation of laws, policies and regulations related to cybersecurity. • Govern and supervise BtCIRT's activities. • Ensure BtCIRT has adequate capabilities in terms of human, technological and financial resources. • May declare any ICT and media infrastructure as Critical Information Infrastructure (CII) in consultation with BICMA.
BtCIRT	• National agency to coordinate cybersecurity activities and be a central point of contact on all cybersecurity matters pertaining to national security in the country. • Establish policies, guidelines, and procedures required to implement its functions.
Bhutan InfoComm and Media Authority	• The regulatory body for providers of ICT facilities and services. • Put in place license terms and conditions on data protection, legal interception, and online and offline privacy while issuing licenses/permits to telecom service providers, network vendors or service providers.
Bhutan Electricity Authority	• The regulatory body for the energy sector.
Royal Monetary Authority	• The regulatory body for financial institutions. • Direct FIs to implement cybersecurity framework. • Facilitate in developing and strengthening of cybersecurity surveillance and response by embedding cybersecurity in the risk management framework of financial service providers • Conduct cybersecurity assessment of all critical systems and application • Strengthen collaboration and information sharing on cybersecurity through FICRT
FICRT	• Safeguard critical information and critical assets of the financial sector • Monitor cybersecurity threats to plan for and coordinate counter-threat measures to prevent the types of cybersecurity risks • Train cyber experts through training and education programs on effective cyber practices and assessment to make FIs more resilient • Active collaboration and effective information sharing pertaining to cybersecurity • Exchange of cybersecurity issues and offer lesson learnt advice and expertise
CII Agencies (Bhutan Telecom, Tashi InfoComm, ISPs, BPC, DGPC, Banks, government CIIs, G2C, etc.)	• Enforce the provisions of cybersecurity as per terms and conditions set by the regulators in accordance with ICM Act 2018 and other laws & regulations. • Safeguard critical information and critical assets from cyberattacks.
Royal Bhutan Police	• Investigate all types of cybercrimes. • Prosecute cybercrimes with petty misdemeanour and misdemeanour offences. • Forward cybercrime cases with misdemeanour and above offences to OAG.
Office of Attorney General	• Support BtCIRT in reviewing laws, regulations and policies regarding cybersecurity. • Prosecute cybercrime cases forwarded by the RBP.
Royal Courts of Justice	• Conduct hearing on cybercrime cases. • Pass judgement on cybercrime cases.
Ministry of Education & Royal University of Bhutan	• Educational programs for cybersecurity. • Awareness and advocacy for students.

Source: RAA analysis based on stakeholder mapping and RACI analysis

As shown in table 4, each stakeholder has an important role in securing the nation's cyberspace. However, the RAA noted a lack of coordination amongst these key stakeholders in the following:

i. There are no formal coordination mechanisms instituted amongst the agencies. Currently, there are ad-hoc and informal relations established based on practices and experience among these institutions. There are no protocols for eliminating silos, thereby creating cross-cutting knowledge, skills, and capability needed to underpin cybersecurity at large. Furthermore, there is no clear delineation of responsibility and/or shared responsibility framework between the MoIC (responsible for policy and planning), CII agencies (implementors), and regulators.

ii. The BtCIRT does not have proper linkages with regulators to have effective information sharing and to institute cybersecurity requirements. Moreover, regulators do not share information with the BtCIRT to keep informed on the CII agencies' compliance with the cybersecurity requirements and other important aspects such as challenges and issues faced in their effort to secure their CIIs from cyberattacks.

iii. The BICMA does not have mechanisms established with the government agencies having CIIs and those providing essential e-services to monitor the implementation of cybersecurity requirements stipulated in the ICM Act 2018.

iv. There are no linkages among the regulators. Despite cybersecurity being a cross-cutting issue and requiring integrated effort from regulators in handling cyber incidents and breaches through sharing each other's expertise and good practices, regulators are functioning independently. Similarly, the CII agencies only share emerging cyber threats through the BtCIRT and FICRT but do not share good practices and expertise.

v. Regarding linkages between the RBP and OAG during the investigation and prosecution of cybercrimes, there is a clear understanding of their roles and they have also signed an MoU.

vi. There is no clarity on who will lead and investigate financial and investment scams. Such scams were reported to BtCIRT and BtCIRT tried to investigate in coordination with RMA, Office of the Consumer Protection, RBP, and related banks.

vii. BtCIRT also does not have coordination mechanisms to bring in all the key stakeholders such as CII agencies through regulators, RBP, and private vendors during cyber emergencies. For example, there is no common understanding of the execution of the procedures of the whole process of detection, response, and prevention of cyber incidents at the national level.

viii. With regard to awareness and capacity building, the BtCIRT has not established linkages with the MoE, the Royal University of Bhutan, and other stakeholders such as the private sector to develop cybersecurity capacities and awareness in the country.

The absence of formal institutional linkage arises from differences in establishment laws of institutions which articulate the functional objectives of these institutions without considering the integrated cybersecurity approach. Lack of proper coordination among stakeholders will result in fragmented efforts of the stakeholders in ensuring the cybersecurity of the nation and ultimately wasting resources, creating inefficiencies and delays in solving cybersecurity matters.

The BtCIRT justified that regulators of CIIs are consulted and corresponded when necessary and whenever relevant.

While acknowledging the response and noting some form of collaboration pursued, there are no institutionalised mechanisms of collaboration and coordination with different stakeholders to ensure formalised channel and integrated approach towards securing Bhutan's cyberspace.

3.2.3.2 Information Sharing

Effective mechanisms and institutional structures at the national level are necessary to reliably deal with cyber threats and incidents. The absence of such institutions and lack of national capacities pose a genuine problem in adequately and effectively responding to cyber incidents. CIRT play an important role in the solution. CIRT should establish and facilitate information-sharing mechanisms.

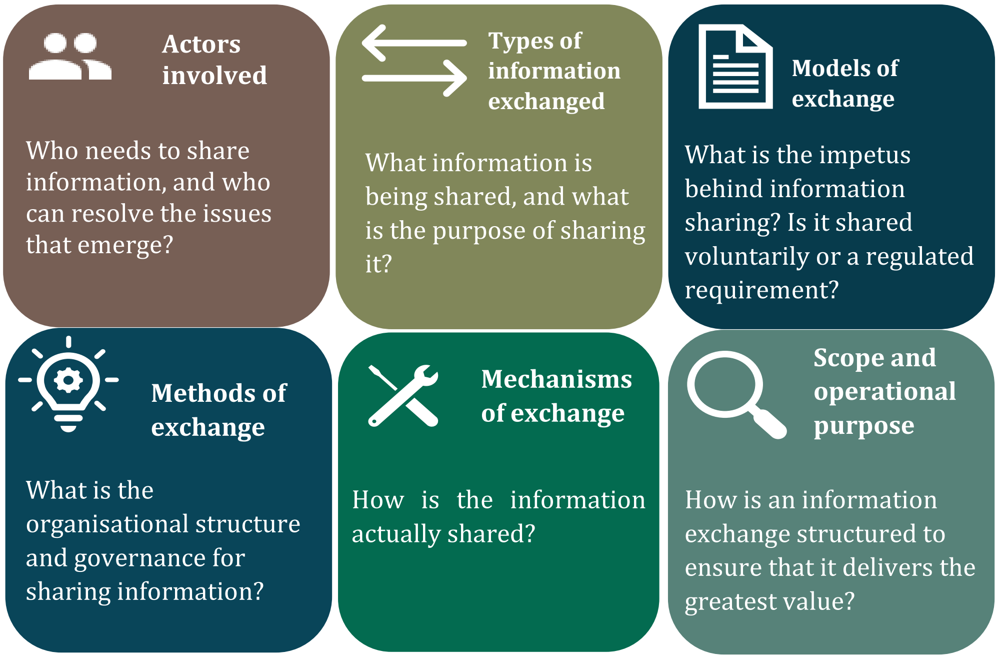
As per the ITU's Guide to Developing a national cybersecurity strategy, *"Formal and informal information-sharing programmes can help foster effective coordination and consistent, accurate and appropriate communications during incident response and recovery activities; facilitate rapid sharing of threat and intelligence information among affected parties and other stakeholders; help improve the understanding of how and which sectors have been targeted; disseminate information on the methods that can be used to defend and mitigate damage on the affected assets; and ultimately reduce vulnerabilities and exposure along with their attendant risks."*

Similarly, the Guide to Cyber Threat Information Sharing of the National Institute of Standards and Technology (NIST) mentions the following benefits of sharing information:

- ✓ **Shared Situational Awareness:** Information sharing enables organisations to leverage the collective knowledge, experience, and analytic capabilities of their sharing partners within a community of interest, thereby enhancing the defensive capabilities of multiple organisations.
- ✓ **Improved Security Posture:** As organisations share information and subsequently mitigate threats, those organisations can improve their overall cybersecurity posture, even providing a degree of protection to other organisations, including those who may not have responded to the threat information, by reducing the number of viable attack vectors for actors.
- ✓ **Knowledge Maturation:** When information relating to incidents are shared and analysed by organisations, the knowledge of tactics, techniques and procedures used by threat actors for specific incidents and threats can be enriched.
- ✓ **Greater Defensive Ability:** Organisations that share information are often better informed about changing tactics, technique and procedures of threat actors and the need to rapidly detect and respond to threats and reduce the probability of a successful attack.

A framework for cybersecurity information sharing requires an effective and sustainable information sharing program and the framework should consist of a detailed understanding of the following elements depicted in figure 9.

Figure 9: Elements for cybersecurity information sharing framework



Actors involved

Who needs to share information, and who can resolve the issues that emerge?

Types of information exchanged

What information is being shared, and what is the purpose of sharing it?

Models of exchange

What is the impetus behind information sharing? Is it shared voluntarily or a regulated requirement?

Methods of exchange

What is the organisational structure and governance for sharing information?

Mechanisms of exchange

How is the information actually shared?

Scope and operational purpose

How is an information exchange structured to ensure that it delivers the greatest value?

Source: RAA interpretation based on RAA review on cybersecurity information sharing best practices

With regard to information sharing on cybersecurity, BtCIRT has established various platforms as discussed below:

1. *BtCIRT Website*: The website is used to disseminate public information (advisories, best practices and alerts). As per the BtCIRT annual report 2021, a total of 73 alerts and advisories were published of which a significant proportion was released to address critical patches released by software vendors to fix the vulnerabilities.
2. *Facebook*: To reach more users, BtCIRT also created its Facebook page to publish alerts and information related to cybersecurity activities (capacity development, awareness, guides).
3. *Email*: BtCIRT also sends security updates and advisories via email to ICT Officers, when there is the presence of severe threats and during emergency cases. Email or system (authenticated and authorized) feeds are used to disseminate confidential and internal information (dedicated advisories, alerts, and threat information).
4. *WhatsApp*: A WhatsApp group comprised of the task force members for drafting the NCS and also government and public IT officials, familiar to the BtCIRT, has been created to share information on malicious links and scams, whenever cases arise, in an informal manner.

The information shared on these platforms comprises advisories (official good practice documents), threat information, vulnerability reports, awareness programs, and any other initiatives and updates. These platforms are also used to coordinate efforts and share expertise to respond to threats. From the banking sector, BtCIRT only collects information related to how the FICRT handled incidents.

The RAA reviewed the current practices of information sharing and noted the following:

i. The participants in the platforms are not inclusive of all the IT professionals from all the essential sectors. Although information-sharing exercises require the sharing of information from all the parties involved, the RAA noted that the information sharing is only initiated by the BtCIRT.

ii. The type of information that is shared on these platforms is not properly identified and regulated. Some information shared may be used outside of the intended purpose and therefore any such information must be adequately protected.

iii. The Draft NCS identifies BtCIRT to develop a platform for engagement between Security Operations Centers (SOCs)/CIRTs in the country and other jurisdictions or law enforcement bodies for collaboration, in accessing resources, methodologies and information references on global cybersecurity practices. The Draft NCS also identifies BtCIRT and the National Cybersecurity Working Group (NCWG) (after its formation) to draw action plans for collaboration with private and public entities to report cyber incidents effectively and share experiences of cyber-attacks. However, budgetary constraints and the priority of the management have curtailed such development.

iv. As per the annual report of the BtCIRT 2021, the division published the latest cybersecurity news and vulnerabilities to keep its constituents well informed about the latest development in the area of cybersecurity on its website and Facebook page. A total of 73 alerts and advisories were published of which a significant proportion was to address critical patches released by software vendors to fix the vulnerabilities. However, the RAA did not find any evidence demonstrating collaborative efforts led by the BtCIRT with its constituents in implementing these alerts and advisories.

The absence of a collective approach in information-sharing practices can be attributed to the non-formulation of a proper information-sharing mechanism. The lack of such an approach will incapacitate the agencies or organisations in using shared resources and expertise in protecting, responding, and recovering from cyber threats and cybercrimes. Further, due to poor information sharing, it was noted, during the focus group discussions conducted with CII agencies and consultation with BEA, that the ICM Act 2018 is not referred to across the BEA and CII agencies, which may result in weak compliance with the Act.

BtCIRT justified that it is not possible to ensure that the alerts and advisories published are adhered to by every constituent but they do follow up for some agencies. With regard to information sharing, BtCIRT said that they follow Traffic Light Protocol (TLP) to encourage greater sharing of sensitive information.

While noting the initiatives taken by BTCIRT, there is no proper information-sharing mechanism to institute a collective approach in information-sharing practices like involving IT professionals from all the essential sectors and proper identification of types of information to be shared. Further, there is no platform for engagement between SOCs/CIRTs in the country and other jurisdictions or law enforcement bodies for collaboration, in accessing resources, methodologies and information references on global cybersecurity practices as per the draft NCS.

3.2.3.3 Sectoral Computer Incident Response Team

Sectoral CIRTs are entities responding and managing to computer security or cybersecurity incidents affecting a smaller subset of the country or specific sectors such as banking, energy, education, and communications. National CIRT serves at a national level while the sectoral CIRTs provide services to constituents from a single sector.

Sectoral CIRTS are important players in organising sectoral exercises with a good communication channel and closer relationship with the main sectoral stakeholders. Further, it aids in maintaining subject matter expertise, specialized knowledge and skills, and incident response capacity. The stakeholders are encouraged to come together in addressing the risks, threats, and relevant challenges unique to the particular sectors, enabling the national CIRT to focus on coordinating across sectors in the cybersecurity ecosystem.

Some of the key advantages of instituting sectoral CIRTS are:

- Bridging the gap between public and private sectors;
- Provide platforms for information sharing and lessons learned before and after an incident;
- Leading and facilitating incident response;
- Ensuring trust and confidentiality among members;
- Convening meetings and facilitating discussions among stakeholders;
- Provide sector-specific expertise in addition to generic services provided by national CIRT;
- Faster sectoral communication channel, as their constituency base is smaller than the National CSIRT;
- Coordinating with national CIRT within the national cybersecurity ecosystem.

Therefore, establishing sectoral CIRTs will enhance coordinated response in dealing with cyber threats in a particular sector.

However, the RAA noted that the FICRT is the only sectoral CIRT formed in the country. Druk Holding and Investments has plans to form a CIRT within its incorporated companies.

The lack of sectoral CIRTs instituted by the CII agencies will not only result in weak information sharing and awareness of emerging cyber threats between sectors but also lead to uncoordinated responses to similar threats and vulnerabilities.

3.2.3.4 Cybersecurity Focal Point in Government Agencies

Public agencies and organisations are making significant investments in information and communication technology (ICT) to enhance efficiency and better service delivery. Increased use and dependency on ICT have also made organisations the targets for cyber-attacks and vulnerable to cyber threats. Thus, organisations should not only implement cybersecurity strategies to protect computers and networks from these threats but also need to understand the cyber risks landscape and issues at the leadership level.

At a bare minimum, organisations should know what to do and whom to contact in the event of cyber incidents. Further, there should be a dedicated information security focal point within the organisations, which is responsible for information sharing, monitoring and responding to cyber threats. The focal point should be able to engage external subject matter experts (external or BtCIRT) as required.

During the review, the RAA noted that there were no formal cyber or information security focal points appointed in government agencies but BtCIRT communicates directly with the ICT heads and system administrators regarding cyber threats, vulnerability assessment reports, and alerts.

As for the financial sector, there are six Information Security Officers (ISO) from member banks and representatives from non-banking financial service providers in FICRT. These ISOs represent their respective organisations in the FICRT quarterly meets to share information on cyber threats and alerts and share experiences and vulnerabilities. Furthermore, as a focal point, they also conduct ISO internal audits, surveillance audits, PCI DSS surveillance audits, and review the policies.

The non-identification of cyber or information security focal persons in agencies is due to a lack of initiatives that may result in the implementation of inadequate cybersecurity measures in organisations. This will ultimately lead to reactive cyber incident handling procedures rather than proactive procedures.

The BtCIRT stated that the focal for all ICT-related tasks including security is the ICT head for any government agencies.

The RAA accepts the response provided by the BtCIRT.

3.3 Cybersecurity Governance

Cybersecurity governance provides strategic direction to manage security and risk at a national level and build accountability frameworks. Effective cybersecurity governance would ensure that resources are available; national strategy and plans, processes and procedures are in place; security controls are implemented; compliance requirements are met; and there is business continuity in the event of cyber-attacks.

The RAA, during the course of the audit, assessed the adequacy and effectiveness of cybersecurity governance and noted the following:

3.3.1 National Cybersecurity Strategy

The RAA reviewed the draft NCS and the implementation plan against desirable characteristics of national strategies and found that these documents addressed some of the desirable characteristics, but lacked certain key elements for addressing others as provided in table 5.

Table 5: Review of Draft NCS

Sl. No.	Characteristics	Coverage in the Draft NCS
1.	Purpose and Scope	Addressed
2.	Problem definition, situational analysis	Addressed
3.	Assumptions and Risk Assessment	Not addressed
4.	Goals, sub-goals, action plans, and performance measures	Partially addressed
5.	Resourcing and risk management	Partially addressed
6.	Monitoring and Evaluation framework	Not addressed
7.	Organisational roles, responsibilities, and Coordination	Partially addressed

Source: RAA review and analysis of Draft NCS and Implementation Plan

3.3.1.1 Draft National Cybersecurity Strategy

An NCS expresses the vision, high-level objectives, principles and priorities that guide a country in enhancing cybersecurity. It provides an overview of the roles and responsibilities of the stakeholders involved in improving cybersecurity and a description of the steps, programmes and initiatives that a country will undertake to protect its national cyberinfrastructure and, in the process, increase its security and resilience (International Telecommunications Union (ITU), 2018)

As per the report for Readiness Assessment for Establishing Computer Incident Response Team (CIRT) conducted by the ITU in 2012, Bhutan does not have a defined NCS in place to manage and mitigate cybersecurity incidents in case of a coordinated cyber-attack on critical national infrastructure. The assessment recommended that Bhutan:

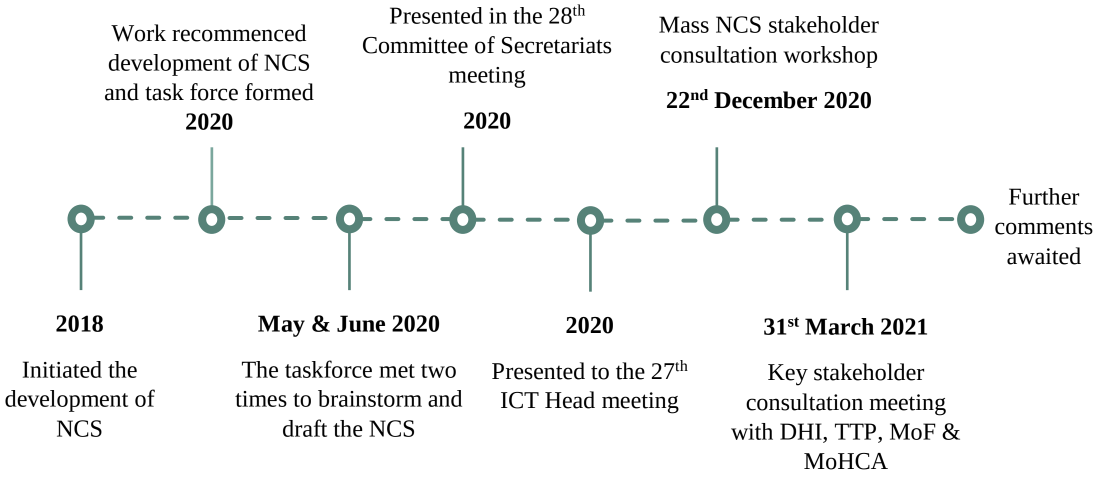
1. should start formulating national strategies such as a National Cybersecurity Policy (NCP) to safeguard its Critical National Information Infrastructures/CII sectors.
2. that the NCP should recognise the critical and highly interdependent nature of the CII and aim to develop and establish a comprehensive programme and a series of frameworks that will ensure the effectiveness of cybersecurity controls over vital assets. The policy should be developed to ensure that CII is protected to a level that is commensurate with the risks faced.
3. The terms of reference for the NCP should include, but not be limited to:
   - standard cybersecurity systems across all elements of the CII,
   - strong monitoring and enforcement of standards, and
   - the development of a standard cybersecurity risk assessment framework for the country.

Recognising its importance, the BtCIRT along with the support from ITU initiated the development of an NCS in 2018. The NCS was based on the ITU's assessment of the country's cybersecurity situation, and the ITU's International Cybersecurity Strategy Development guidelines. The draft NCS has seven goals and 27 sub-goals with an implementation plan. Under the implementation plan, there are 36 action plans to achieve the strategic intents of the seven strategic goals. The seven strategic goals in the draft NCS are as follows:

1. Goal 1: National Cybersecurity Governance and Coordination.
2. Goal 2: Protection of CII.
3. Goal 3: Legal Framework, Regulation, and Policy.
4. Goal 4: Cybersecurity Awareness and Capacity Building.
5. Goal 5: Robust Incident Handling.
6. Goal 6: Promote international and local cooperation.
7. Goal 7: Development of Cybersecurity Guidelines.

The timeline of activities carried out for the development of the NCS of Bhutan is depicted in figure 10.

Figure 10: Timeline of drafting the NCS



2018
Initiated the development of NCS
Work recommenced development of NCS and task force formed
2020
May & June 2020
The taskforce met two times to brainstorm and draft the NCS
Presented in the 28th Committee of Secretariats meeting
2020
2020
Presented to the 27th ICT Head meeting
Mass NCS stakeholder consultation workshop
22nd December 2020
31st March 2021
Key stakeholder consultation meeting with DHI, TTP, MoF & MoHCA
Further comments awaited

Source: RAA representation based on Annual Report 2020, BtCIRT

As of the date of the audit, the RAA found that the NCS is still in its draft stage and is awaiting further comments and has not been finalised as depicted in figure 10. Nine years had already passed since ITU recommended to formulate an NCS for ensuring cybersecurity in the country.

In addition, the ICM Act 2018, also grants BtCIRT, the authority to '*establish policies and procedures required to implement its functions under this Act.*' However, six years had elapsed since the establishment of the BtCIRT (as per the government order vide letter No. C-2/104/310 dated 20 May 2016), and the NCS is still in its draft stage and awaiting further comments from the various stakeholder.

Further, the RAA noted that there is no definite timeline to indicate the end date of this activity. Moreover, the draft NCS is meant for 2021-2025, and less than half of the timeline to implement the strategy had already elapsed in the drafting of the NCS.

Without a finalised NCS, the cybersecurity initiatives undertaken in the country will lack strategic visions and directions, defined principles, and set priorities in managing cybersecurity risks. Additionally, in the absence of an overall strategy, the roles and responsibilities of the agencies involved in cybersecurity management would be uncoordinated leading to overlapping and duplication of the roles and responsibilities, and fragmented initiatives ultimately creating vulnerabilities in the CII against cyber threats. This, in turn, will weaken the national crisis response and recovery from cyber-attacks.

3.3.1.2 Risk Assessment for the NCS

Making assumptions and managing risks are key components in crafting a strategy. The BtCIRT should analyse all assumptions and risks that could become an impediment to the achievement of the strategic goals of the NCS. Accordingly, the BtCIRT should formulate assumptions that enable the presumed cause-effect linkages that are fulfilling the required capacities (institutional, organisational and professional) to achieve the identified strategic goals in the draft NCS. Then the risks associated with the assumptions should be identified and assessed along with the likelihood of occurrence and impact of the risks to be able to manage (prioritise) and mitigate the risks with appropriate strategies, thereby reducing/minimising the impact on the achievement of strategic goals.

However, the RAA could not find any evidence of the BtCIRT having formulated assumptions and identified and managed the risks. Even with the drafting of NCS taking place, the risk assessment was not carried out to mitigate and manage the challenges to achieve the strategic goals.

The BtCIRT replied that the draft strategy established and provided by the cybersecurity expert is the baseline from which the task force started drafting the NCS.

Even though the baseline was drawn during the drafting of the NCS at the initial phase, the relevance of risks and assumptions would have changed which would require review and update to enhance relevance to the current situations and context.

3.3.1.3 Budget for the Implementation Plan of the NCS

The ITU guide to developing an NCS mentions the good practice of allocating a dedicated budget and resources for the implementation, maintenance and revision of the strategy. The resources for the strategy should be defined in terms of money, people, material as well as partnerships, and continued political commitment and leadership required for successful execution. The guide further mentions that resourcing the tasks and objectives of strategy should not be viewed as a one-time initiative but the overall programme should be managed and tracked by milestones to ensure successful implementation of the strategy.

The logic model of the evaluation framework for the cybersecurity strategies, developed by the ENISA (European Union Agency for Network and Information Security), shows that NCS with its budget line and review of the spending results in transparency in spending. Besides, it will also ensure that the activities planned for its implementation are fulfilled leading to the overall achievement of the strategic intents of the NCS. Further, the Financial Accounting Manual 2016, states that to obtain budget appropriations, budgetary agencies must prepare a 'preliminary estimate'.

Therefore, there should be adequate resources made available to implement NCS. Accordingly, the draft NCS in its implementation plan outlays the indicative budget required for the execution of the action plans under each strategic goal. As per the implementation plan, the indicative budget for the following action plans is stated in table 6.

Table 6: Indicative budget provided for only two action plans in the draft NCS

Sl. No.	Strategic Goal	Action Plan	Indicative Budget (Nu.)
1.	**Strategic Goal 2:** To protect the CII and services of Bhutan.	Identify National Information Infrastructure and conduct a risk assessment	7.5 million
2.	**Strategic Goal 4**: To improve cybersecurity perceptions of every citizen and enhance their skills through Cybersecurity Awareness and Capacity Building	Promote cybersecurity in School curriculum and Tertiary level courses (Certificate, Diploma, Degree)	2.5 million (estimate) in MoE

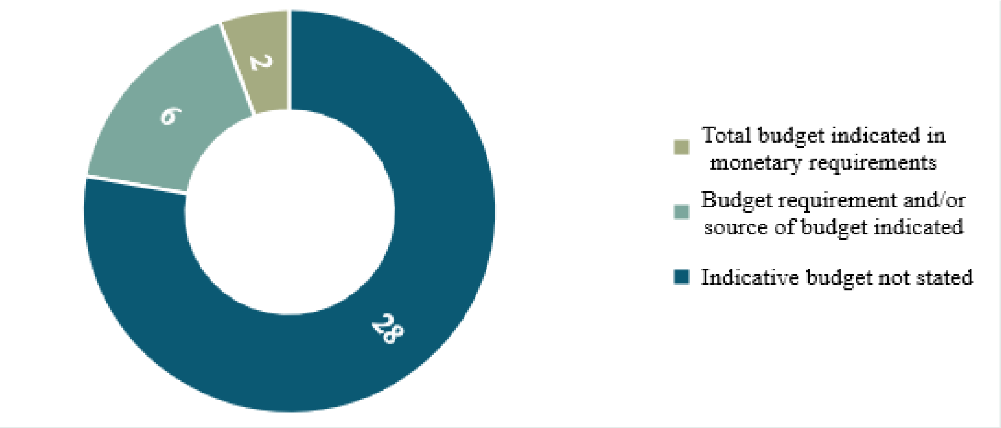
Other action plans' indicative budget is stated in terms of activities for which only the requirement of the budget or availability of budget sources is mentioned instead of actual budget estimate for implementation of the strategy as shown in table 7.

Table 7: Actual budget requirement/estimate is not provided for some action plans in the draft NCS

Sl. No.	Strategic Goal	Action Plan	Indicative Budget (Nu.)
1.	**Strategic Goal 1:** To enhance National Cybersecurity Governance and Coordination for successful management and implementation of NCS and other cybersecurity initiatives.	Formation of: i. National Cyber Working Group ii. Legal Framework Working Group iii. Child Online Protection Working Group	Budget for Meetings
2.	**Strategic Goal 4**: To improve cybersecurity perceptions of every citizen and enhance their skills through Cybersecurity Awareness and Capacity Building	Cybersecurity Awareness in educational institutes	Budget Available till 2023
		Initiate National Cybersecurity Week to promote cybersecurity awareness	RGoB Fund for First "Cybersecurity Week"
		Develop capacity development roadmap (Cybersecurity Skills Framework)	Budget Available till 2023

From a total of 36 actions in the implementation plan, the RAA found that only two action plans with indicative budgets while six action plans either stated activities for which the budget is required or mentioned only the source of the budget. In addition, 28 action plans have not stated the indicative budget required in terms of monetary, human or any other resources in order to implement the action plans as shown in figure 11.

Figure 11: Action plans with and without an indicative budget

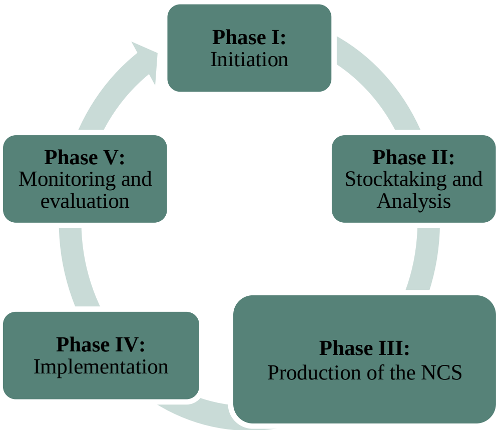


As per the Budget Manual 2016, budgeting is essentially carried out to determine what is to be done, what is to be accomplished, the manner in which it is to be done, and the cost of doing it in the future. Not having an indicative budget in the draft NCS shows a lack of assessment carried out for implementing the action plans stated in the draft NCS. Without a preliminary estimate or indicative budget, there is no basis for approval of a budget for appropriating the activities of the action plan. Without budgetary support, there is a risk of not implementing activities or actions identified in the NCS.

3.3.1.4 Monitoring and Evaluation Framework

The ITU guide identifies five phases in the lifecycle of an NCS, as depicted in figure 12**.** In the final phase (Phase V), a formal process to monitor and evaluate the NCS must be developed by a competent authority. The process should monitor whether the implementation of the NCS by the government is in accordance with the action plans, and evaluate whether the NCS is still relevant in light of the changing risk environment and whether it still reflects the government's objectives.

Figure 12: Lifecycle of NCS


Phase I: Initiation
Phase II: Stocktaking and Analysis
Phase III: Production of the NCS
Phase IV: Implementation
Phase V: Monitoring and evaluation

Source: ITU Guide

The guide states that to ensure effective monitoring and evaluation, the government must identify an independent entity responsible for monitoring and evaluating the implementation progress and efficiency and should be involved in defining appropriate monitoring and evaluation metrics/key performance indicators (KPI) during the initiation (Phase I) and production (Phase III) phases.

a) Monitoring Framework

As per the ITU guide, the monitoring of the implementation of the NCS should be done based on the agreed timeline and the outcome of the monitoring should note any deviations and include reasons for delays. The monitoring entity should also review the periodic updates of the agencies responsible for the different strands of the NCS implementation, submitted to the lead agency. This will ensure that the relevant agencies are held accountable for the implementation of the action plans and also help to identify any challenges in the implementation and accordingly, allow for rectification or adoption of its implementation plan based on the lessons learned. Additionally, it is important to establish a baseline metric because these metrics will enable better monitoring of actions and highlight areas of improvement.

As per the BtCIRT and draft NCS, the existing High-Level Information Communication Technology (ICT) Committee would oversee the implementation of the NCS and form three other working groups: National Cybersecurity working group (NCWG), LFWG, and Child Online Protection Working group (COPWG). The High-level committee will govern all three working groups and BtCIRT will orchestrate the implementation of the strategy.

However, the draft NCS does not mention a formal monitoring framework that will be utilised to monitor the implementation of the action plans of the NCS. Although the BtCIRT has been identified for monitoring the implementation progress of the NCS, the RAA noted that there is neither requirement of the BtCIRT to report the implementation progress of the action plans to the government nor a requirement on the progress by the responsible agencies to the BtCIRT. In addition, the lead agencies are not identified for each action plan and no baseline metrics have been established.

The lack of inclusion of a proper monitoring framework in the draft NCS is also not in line with the ITU guide which specifies a need for a clear monitoring framework and identification of an independent entity to review the progress of the responsible agencies.

In the absence of an effective monitoring framework, there could be no means to determine whether the action plans of the strategic goals are on track, compare the progress made with baseline metrics, and rectify or adopt action plans based on lessons learned. It could also lead to the lack of accountability for the non-fulfilment of the commitments ultimately resulting in the non-achievement of the objectives of the NCS.

b) Evaluation Framework

The ITU guide states that besides assessing the progress made upon the agreed metrics, it is also critical to evaluate whether the outcomes achieved are contributing to the objectives of the NCS or whether different actions should be considered. As part of this process, the broader risk environment also needs to be regularly re-evaluated to understand any external changes or factors affecting the outcomes of the NCS.

A report should be produced for the lead authority of the strategy, consisting of the results of the assessment and appropriate recommendations, including ways to update the action plan to ensure that it is relevant and responsive to the changing policy and the risk landscape. The report should be the basis for the review of the NCS, which should not only consider the progress made and the changes in the external environment but also re-assess the government’s own priorities and objectives.

As per the National Cyber Security Strategy Guidelines, 2013, developed by the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE), the independent entity identified to carry out the evaluation should have an appropriate mandate, roles and responsibilities, and may be different from the body coordinating the implementation and review. In addition to the entity in charge of the evaluation, other stakeholders should also be encouraged to take part in the evaluation process.

Upon the review of the evaluation framework for the NCS, the RAA observed the following:

i. The BtCIRT is not only responsible for the implementation and monitoring of the NCS but has also been identified as the responsible entity for evaluation which is not in line with best practices for an evaluation framework. The evaluation entity has to be independent of the implementation entity;

ii. The timeline for the evaluation has not been mentioned;

iii. Plans to review the NCS after evaluation in accordance with the change in policy and environment have not been planned or mentioned.

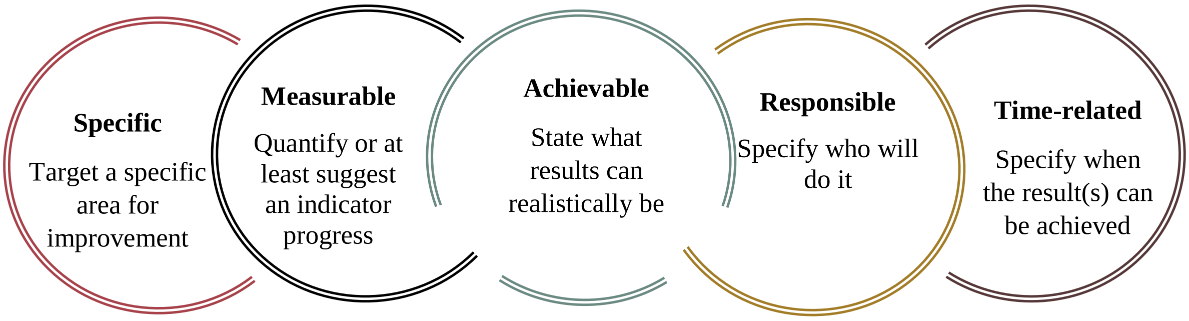
The lack of an evaluation framework is attributed to the lack of understanding of the need to have such a framework and the absence of national frameworks and guidelines. The lack of an identified independent entity to carry out the evaluation of the NCS is due to the lack of appropriate stakeholder engagement and assessment during the development of the strategy.

In the absence of an evaluation framework, there are no mechanisms in place to measure the outcomes of the action plans in contributing to the realisation of the objectives of the strategy and to identify areas that need rectification or modification and implement changes accordingly. The lack of plans to review the NCS would result in the NCS becoming outdated and non-applicable to the changing environment and also to the changes in the priorities of the government.

c) Key Performance Indicators

The ITU guide states that the Key Performance Indicator (KPI) should be defined by near-term, mid-term and long-term objectives in order to reinforce governance and management mechanisms such as the accountability for action plans and should include the SMART criteria as given in figure 13.

Figure 13: SMART Criteria for setting KPIs


Specific
Target a specific area for improvement
Measurable
Quantify or at least suggest an indicator progress
Achievable
State what results can realistically be
Responsible
Specify who will do it
Time-related
Specify when the result(s) can be achieved

The implementation plan of the draft NCS has identified KPIs for each of the action plans under each strategic goal with indicative timelines. The RAA reviewed the KPIs and noted that although the KPIs are specific, time-related, and indicate responsible agencies, it does not suggest indicators on what is to be measured and what resources are required to achieve realistic results. The RAA also noted that the KPIs are generic and do not specify near-term, mid-term, or long-term objectives.

The inadequate setting of the KPIs is mainly due to improper assessment carried out during the initiation and production phases of the lifecycle of the strategy. As per the guide, KPI development should also be undertaken after proper consultation and partnership with the relevant stakeholders by BtCIRT, however, evidence of such consultations or partnerships does not exist.

KPIs that do not include indicators for measuring progress do not facilitate monitoring and evaluation mechanisms. Similarly, KPIs, that have not been defined realistically based on the available resources, will result in the improper allocation of resources and improper fulfilment of the commitments set by the respective owners of the action plans.

The BtCIRT mentioned that the task force presented and discussed the generic KPIs with the relevant stakeholders during the task force meeting. It is also reported that the BtCIRT had several consultation meetings and discussions with various agencies, and private sectors.

While noting the response, the fact is that there is no monitoring and evaluation framework to monitor the progress of the strategy in achieving the intended objectives of cybersecurity.

3.3.1.5 Coordination Mechanisms

The ITU guide identifies that one of the good practices to ensure an effective and comprehensive strategy is to identify a competent national cybersecurity authority, at the highest level of the government. The competent national cybersecurity authority should provide direction, coordinate actions, and monitor the implementation of the strategy through clear delineation of roles and responsibilities, and defined processes.

The guide further states that a mechanism should be established in the NCS for intragovernmental commitment, coordination and cooperation, which are core functions required to ensure that the governance mechanisms (that is the rules) and resources yield the desired outcomes of the NCS. Effective communication and coordination ensure that all ministries and government agencies are aware of their respective authorities, roles and tasks.

Besides the inter-governmental cooperation, the NCS should reflect on how the government will engage other relevant stakeholders from the private and public sectors and define their responsibilities.

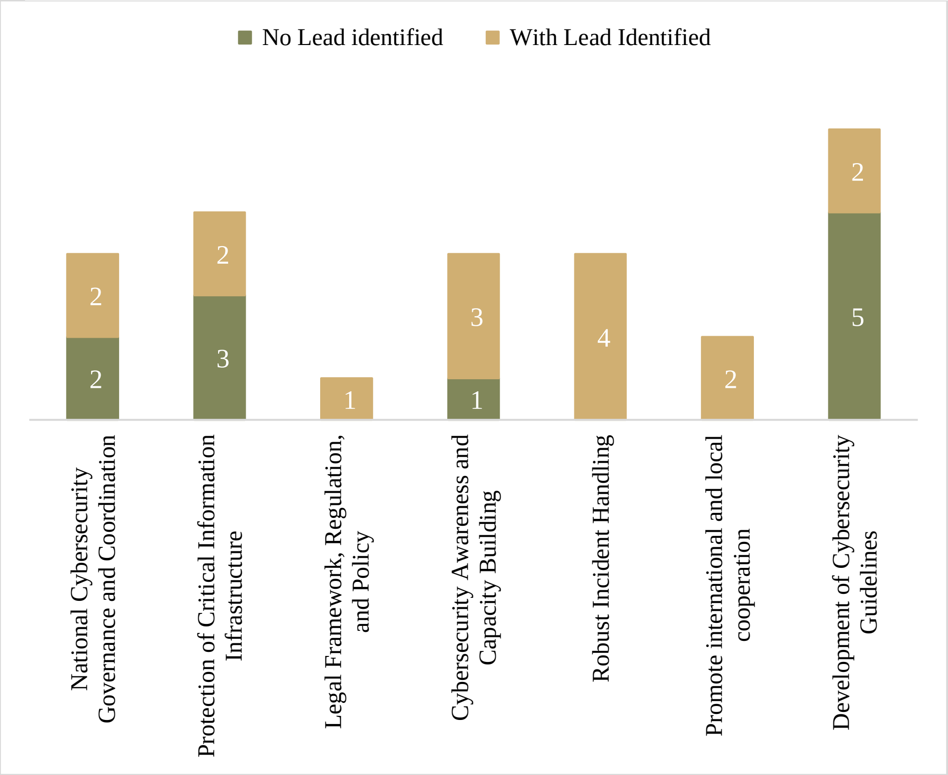
As per the ICM Act 2018, the BtCIRT is identified as the national agency to coordinate cyber security activities in the country. The draft NCS also entrusts the BtCIRT with the responsibility for the overall implementation of the strategy.

Nevertheless, from the total of 27 sub-goals, under the seven strategic goals in the draft NCS, a lead agency has not been identified for 11 sub-goals. Figure 14 describes the number of sub-goals with and without lead agency. Moreover, the coordination and communication mechanisms between the various lead and responsible agencies of the action plan have not been reflected in the draft NCS.

The lack of a lead agency for 11 sub-goals and the non-incorporation of communication and coordination mechanisms is due to not following the proper methodology and framework for crafting strategy during the development of the draft NCS.

Cybersecurity requires a whole-of-society approach wherein government agencies not only work within their mandates and responsibilities but must work across institutional remits and with non-government agencies. Without an identified lead agency for 11 sub-goals to guide the responsible agencies, and mechanisms for the lead and the responsible agencies to coordinate and communicate, there could be the risk of non-realisation of the desired results.

Figure 14: Number of sub-goals with and without lead agency



Source: RAA's analysis based on the action plan of the draft NCS

3.3.2 Cybersecurity Framework

Cybersecurity frameworks are sets of guidelines, standards, and best practices designed for cybersecurity management. The frameworks or cybersecurity systems provide procedures and practices to better understand, manage, and reduce cybersecurity risks of a country or organisation and to protect data and CII from cyber-attacks.

Managing cybersecurity is a challenge which entails timely addressing of vulnerabilities, risks and threats – particularly to CIIs. The cybersecurity framework provides a reliable, standardised and systematic way to mitigate cyber risks regardless of the environment's complexity. It further helps in addressing cybersecurity challenges, providing a comprehensive approach to protecting data, infrastructure and information systems and providing the basis for cybersecurity compliance checks.

A robust cybersecurity program and framework is often seen as a task too difficult because of the resources required. Nonetheless, the benefits greatly outweigh the cost, as establishing a proactive cybersecurity program through a framework would result in achieving a strong cybersecurity posture and preventing data breaches. Hence, there is a need to adopt, customise, develop, and implement a cybersecurity framework.

Even the ITU report for Readiness Assessment for Establishing CIRT had recommended Bhutan to formulate an NCP which should include, among others, the development of a standard cybersecurity risk assessment framework for the country.

However, the RAA noted that there is no cybersecurity framework adopted and implemented by government agencies to improve their cybersecurity posture. This is because neither there is a requirement from BICMA, which is the regulatory body for ICT and Media including cybersecurity, to implement such a framework by the government agencies nor have the BtCIRT developed and/or identified a cybersecurity framework for all agencies to implement.

In the case of financial institutions, the RAA noted that the RMA, being a regulatory body, had issued a directive vide letter No. RMA/DIT/Cybersecurity/1819/5857 dated 2 April 2019 to put in place a robust cybersecurity framework in all financial institutions. The RMA also conducts on-site inspections to check the implementation status of the actions mentioned in the directive. Further, the financial institutions are required to submit the status every quarter.

With regards to Internet Service Providers (ISP), the Rules and Regulations for licensing and operation of ISP in Bhutan 2021, section 3.4.1b require the ISPs to "*Install in its ISP system the required certified cybersecurity systems to ensure resilient cybersecurity features*". Even though there is a requirement, there are no specific mechanisms instituted by BICMA to assess whether the required certified cybersecurity systems are implemented by the ISPs.

There should be an overall strategic direction for the requirement to adopt or implement a robust cybersecurity framework or system which is currently lacking. Not implementing a cybersecurity framework could result in reactive rather than proactive cybersecurity management, not understanding the current cybersecurity status of CII and government agencies, application of inconsistent and unstandardised cybersecurity measures or practices across agencies, and opening vulnerabilities in the systems or networks for cyber-attacks.

3.3.3 Comprehensive National Plan for Securing the Key Resources and Critical Sectors

Securing the key resources and critical sectors and ensuring their continuity is essential to the overall nation's security, public health and safety, and economic vitality. As such, a comprehensive national plan is required to provide clear direction and protect critical infrastructure to deter threats and minimise the consequences of cyber-attacks. The national plan should specify how the government and private sector in the critical infrastructure community work together to manage risks and assure security and resilience. To facilitate effective critical infrastructure security and resilience, it is also important to include funding mechanisms aspects and assure sufficient funding.

Many countries have national plans or strategies for protecting critical infrastructure. These strategies generally define critical infrastructure as physical or intangible assets whose destruction or disruption would seriously undermine public safety, social order and the fulfilment of key government responsibilities. Such damage would generally be catastrophic and far-reaching. The plans should seek to improve coordination among relevant agencies and with private sector operators of critical infrastructure facilities in order to manage risks associated with critical infrastructure.

The policy frameworks for critical infrastructure protection generally include a comprehensive approach to risk. It covers major threats to infrastructure and consists of coordination among a diverse range of stakeholders which includes public, private and government agencies. This approach helps governments to identify key security assets, assess risks and establish strategies and priorities for mitigating these risks. Generally, the risk management strategy involves prevention, preparedness, response and recovery measures.

Along the same line, the ITU's Readiness Assessment for Establishing CIRT Report recommended Bhutan recognise the critical and highly interdependent nature of the CII and aim to develop and establish a comprehensive programme and a series of frameworks that will ensure the effectiveness of cybersecurity controls over vital assets.

Upon review, the RAA found that there is no comprehensive national plan for securing the key resources and critical sectors of the country. The role of the government in ensuring the cybersecurity of critical infrastructure, the government support and mechanisms required to protect CII, and the level of government intervention to ensure compliance with security standards are not specified. The funding mechanisms to protect and secure these critical sectors that are of vital importance to society, such as energy, transport, banking, telecommunications, and finance, are not clear.

Presently, it is not clear if the existing protection programmes implemented by individual critical agencies would be sufficient in dealing with the effects of a sophisticated cyber-attack. An absence of such critical national plans indicates that there is no one to take the lead and provide strategic direction.

In the absence of a clear plan, a secure and resilient critical infrastructure cannot be maintained. The disruption of critical infrastructure would have an immediate and direct impact on the economic activity, day-to-day life, and safety of those affected. Furthermore, the interdependence within critical infrastructures will have major setbacks. An attack on one sector could have ripple effects on the other sectors that depend on it.

3.3.4 Identification of Critical Sectors and Critical Information Infrastructure

Digital transformation in Bhutan is at a rapid pace. With an increasing number of service providers opting for digital platforms, citizens are becoming more reliant on the use of electronic media and the Internet. Simultaneously, this has also led to an increase in cyber threats to these services. Disruption of information infrastructure is capable of causing a major impact on a nation in terms of jeopardising national security and stability, economic growth, citizen prosperity, and daily life.

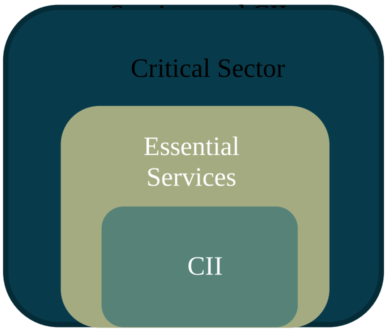
The ICM Act, 2018 defines CII as the *"ICT and media infrastructure, the incapacitation or destruction of which, shall have a debilitating impact on national security, economy, public health, social welfare or safety."* Therefore, there is an increasing need to identify these CII in order to implement effective CII Protection (CIIP) strategies, policies and activities.

CII is the ICT component of the **Essential Services,** which is defined in the Draft CII Identification Framework of Bhutan, as *"services vital to a critical sector and to the country at large, the loss or compromise of which would lead to debilitating impact on security, economy or public health and safety."*

Various essential services are provided in **Critical Sectors,** which are defined in the Draft CII Identification Framework of Bhutan as the *"Core sector that provide essential services, e.g., Finance, Health, Energy, Water, InfoComm, where a large-scale interruption would have a devastating effect on the country."*

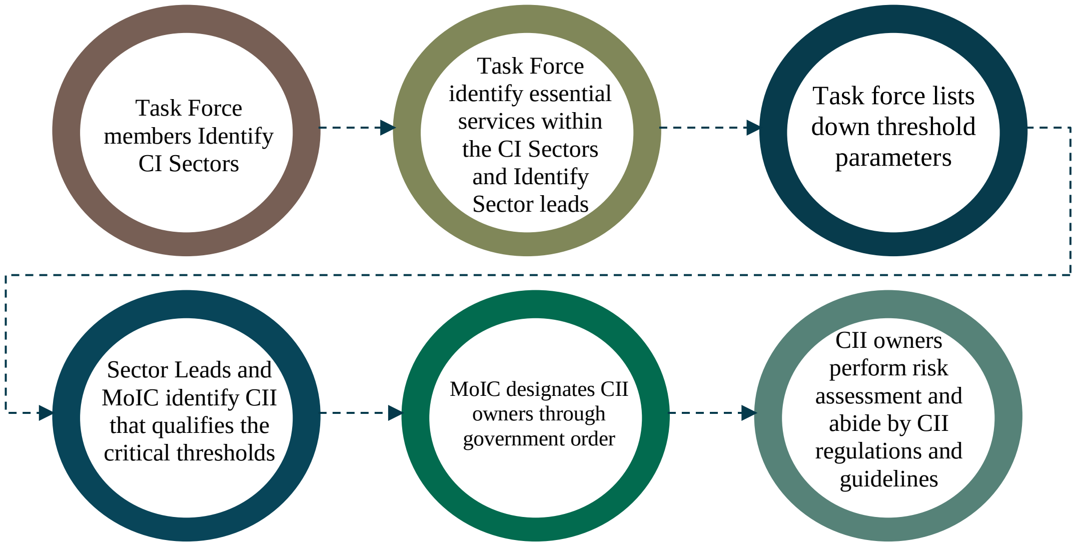
In summary, the **CIIs** are the digitalised components of **essential services** provided by the **critical sectors** as depicted in figure 15. For example, the Bhutan Financial Switch is used for intra-bank transactions, and the SWIFT system is used for international payments in the banks are CIIs, then the essential service would be banking and the critical sector would be banking and finance.

Figure 15: Relationship of Critical Sectors, Essential



Source: RAA representation based on Good Practice Guide on CIIP for governmental policy-makers, 2016

Figure 16: CII identification framework


Task Force members Identify CI Sectors
Task Force identify essential services within the CI Sectors and Identify Sector leads
Task force lists down threshold parameters
Sector Leads and MoIC identify CII that qualifies the critical thresholds
MoIC designates CII owners through government order
CII owners perform risk assessment and abide by CII regulations and guidelines

Source: RAA’s representation based on the draft CII

In the draft CII identification framework of Bhutan, 11 sectors were identified as critical as listed in table 8.

Table 8: Critical sectors of Bhutan as per the Draft CII Identification Framework

Sl. No.	Critical Sector	Remarks
1	Information Communication Technology (ICT)	Prioritised
2	Banking and Finance	Prioritised
3	Health	Prioritised
4	Energy	Prioritised
5	Transport	
6	Water	
7	Food	
8	Civil Administration	
9	Defence	
10	Public Safety and Rescue	
11	Industry	

As per the ICM Act 2018, the MoIC has the authority, in consultation with BICMA, to declare any ICT and Media Infrastructure as CIIs. Further, the ICM Act 2018 stipulates that the Cabinet may, on the recommendation of the MoIC, designate an ICT and Media infrastructure as National Critical ICT or Media infrastructure. In line with these sections, the erstwhile DITT formed a task force with relevant officials from critical sectors in the country to research and study different global criteria and methodologies and develop a draft framework to identify CII sectors/services in Bhutan.

Subsequently, as per the BtCIRT, the framework has been endorsed by the DITT on 24 June 2021. As per the draft framework, the following steps, shown in figure 16, have been developed to identify CIIs.

3.3.4.1 Identification of Essential Services

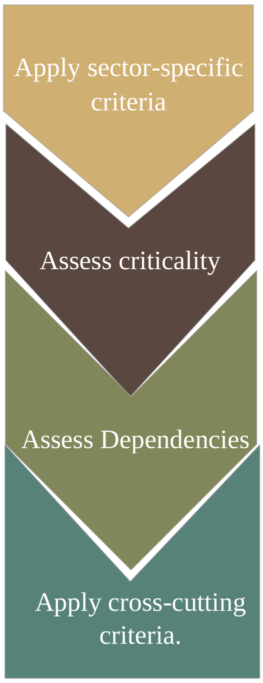
The Global Forum on Cyber Expertise (GFCE), in its Good Practice Guide on CIIP for governmental policy-makers, 2016, defines a methodology to identify essential services within sectors. The steps involved in the process is depicted in figure 17 (the order of these steps depends on the information that is available to national policy-makers).

Alternatively, the ITU guide, in its good practice for Critical Infrastructure services and essential services, states that a detailed risk assessment should guide the identification of national CIs and CIIs and services.

The draft framework, developed by the task force, defines steps in which the CI sectors and essential services should be identified. The initial process was to identify critical sectors by the task force members based on the definition mentioned in the ICM Act, 2018 and the next step is to identify the essential services that are necessary for the functioning of the respective sectors and identify the sector leads.

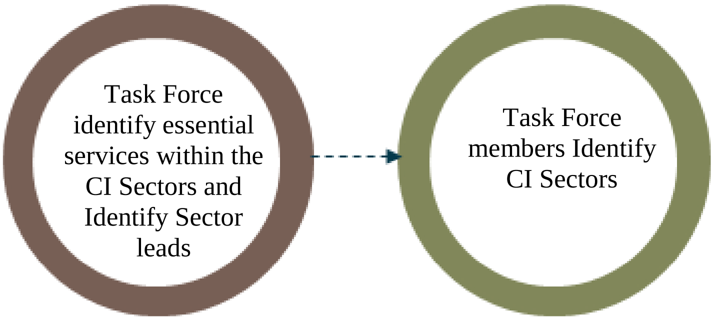
This process is depicted in the first two steps of the draft CII identification framework of Bhutan, as shown figure 18.

Figure 17: Steps to identify essential services



Source: RAA's representation of the systematic steps mentioned in the GFCE Guide

Figure 18: Process of identifying essential services


Task Force identify essential services within the CI Sectors and Identify Sector leads
Task Force members Identify CI Sectors

However, the process of identifying essential services mentioned in the draft framework does not mention a systematic approach. Rather, the task force has simply resorted to identifying essential services that they deem essential.

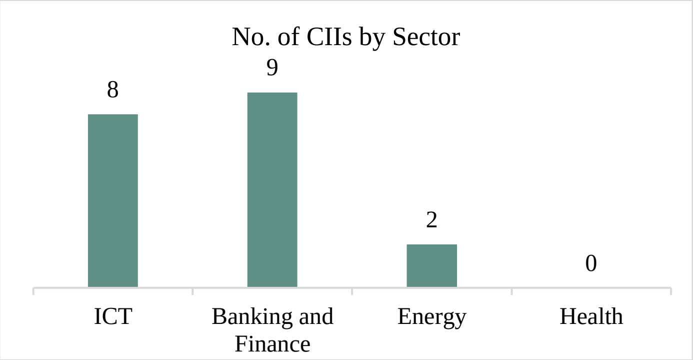
The absence of a systematic approach will lead to the missing out/overlooking of essential services that would be potentially critical and the non-conducting of a detailed risk assessment will result in the non-identification of risks and implementation of mitigation measures for the unidentified essential services.

3.3.4.2 Identification Methodology for Critical Information Infrastructure

The GFCE, Global Good Practices-CIIP, 2017 calls for an adoption of a methodology to systematically identify CIIs. The guide suggests the application of a four-step process (1. Apply sector-specific criteria, 2. Assess criticality, 3. Assess dependencies and 4. Apply cross-cutting criteria) in identifying CIIs. As per the good practices of GFCE, the application of cross-cutting criteria underpins the assessment of the criticality of critical sectors and sector-specific criteria are used to specify CII operators and services. The guide also suggests referencing other nations that are similar in societal, geographical, and technical development structure for a set of sectors and services defined as critical. Alternatively, the use of a risk assessment to guide the identified CIIs is also mentioned in the ITU guide 2018. In the draft CII identification framework of Bhutan, the task force identified four criteria (Impact, Distribution, Timeframe and Dependency) to assess the criticality of the CIIs across all of the four prioritised sectors (ICT, Banking and Finance, Energy and Health). Based on the criterion the task force has initially identified CIIs depicted in figure 19.

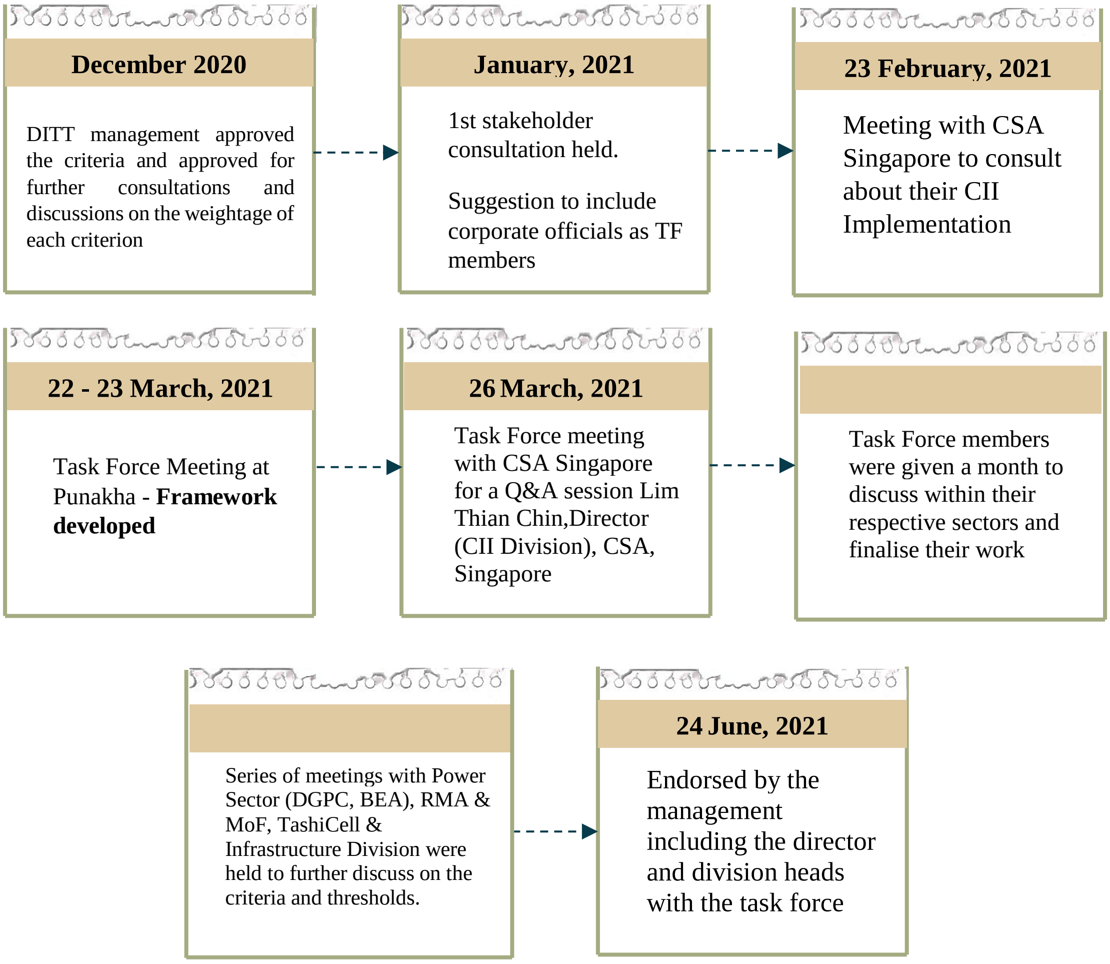
However, as per the BtCIRT, the criterion and threshold mentioned in the draft framework were not agreed by all the stakeholders and a consensus could not be reached. This was because the identified criteria/thresholds did not accommodate the needs of different sectors. The task force has therefore planned to conduct risk assessment (RA) in the identification of the CIIs without the involvement of CII owners.

Figure 19: No. of CIIs identified in the draft CII identification framework



As per the BtCIRT, the following is the timeline for the development of the draft CII identification framework (figure 20).

Figure 20: Timeline for the development of the draft CII Identification Framework of Bhutan



December 2020

DITT management approved the criteria and approved for further consultations and discussions on the weightage of each criterion

January, 2021

1st stakeholder consultation held.

Suggestion to include corporate officials as TF members

23 February, 2021

Meeting with CSA Singapore to consult about their CII Implementation

22 - 23 March, 2021

Task Force Meeting at Punakha - **Framework developed**

26 March, 2021

Task Force meeting with CSA Singapore for a Q&A session Lim Thian Chin,Director (CII Division), CSA, Singapore

Task Force members were given a month to discuss within their respective sectors and finalise their work

Series of meetings with Power Sector (DGPC, BEA), RMA & MoF, TashiCell & Infrastructure Division were held to further discuss on the criteria and thresholds.

24 June, 2021

Endorsed by the management including the director and division heads with the task force

Source: RAA's interpretation of the information received from BtCIRT

A total of **7 months** was taken for the development of the draft framework. The Cyber Security Agency (CSA), Singapore was consulted through a series of webinars on 23 February 2021 and on 26 March 2021 and their CII Identification Framework was used as a guide to developing the identification framework of CIIs in Bhutan.

The GCFE states that sector-specific criteria used by other nations may be treated as classified as they would reveal dependencies, vulnerabilities and sensitivities and thus would not be available to use as a reference. Similarly, Singapore CSA did not share such sector-specific criteria, deeming it confidential when Singapore CSA's framework was referenced for the development of the draft CII identification framework.

Subsequently, the task force decided to forgo the process of identifying thresholds and criteria for respective sectors since it will be an arduous task to conduct stakeholder consultations and reach a consensus. It was also because of a lack of knowledge in the area and difficulty in referencing such exercises as the criteria/thresholds vary from country to country and sector to sector. The task force instead resorted to conducting a risk assessment to identify sectors and assets after consultation with CIRT Malaysia & INCD Israel, on 23 August 2021 and 28 October 2021 respectively, who suggested RA would be an easier task for the team. The RA would be conducted in consultation with the ITU and the engagement of other experts.

Considering all situations and conditions, the RAA is of the view that difficulty in the application of sector-specific criteria for identifying CII should have been foreseen by the task force and accordingly, alternative methods for the identification should have been planned. However, the identification of such difficulties after the development of the framework and resorting to conducting a risk assessment after the fact is due to inadequate planning on part of the task force. Additionally, the use of the framework of a country that has a cybersecurity maturity that is higher than that of Bhutan may not be applicable due to varying technical development and capacity among others.

The improper identification and application of an identification methodology have resulted in the delay of the identification of CIIs by a total of **20 months (December 2020 to August 2022)** from the date of the approval of criteria and threshold by the DITT management till the date of the audit.

In 2015, through a collaboration agreement with The World Bank, The Global Cyber Security Capacity Centre facilitated a self-assessment of cybersecurity capacity in Bhutan. The assessment report titled "The Building Cyber-Security Capacity in the Kingdom of Bhutan", stated that for the capacity factor "Critical Information Infrastructure" Bhutan is at the maturity level of "Start-up" as the CIIs are yet to be identified.

Thus, there has been no significant improvement in the stage of maturity for CII over a period of **seven years** (the stage of maturity for CII was "start-up" as per the assessment report of Global Cyber Security Capacity Centre, 2015), as the CIIs are yet to be identified. As a result, Bhutan does not have a CII identification framework to identify the CIIs.

As per the definition of CIIs in the ICM Act 2018, CIIs are the essential ICT services, infrastructure, and media facilities that underpin Bhutan's society and serve as a backbone of the nation's security, economy, public health, social welfare, and safety. The substantial delay in the identification of these CIIs will result in exposing these CIIs to cyber threats and attacks, which could jeopardize national security and stability, economic growth, citizen welfare and safety.

BtCIRT mentioned that the team had considered all the good practices pertaining to CII identification, including ENISA, ITU and GFCE. Moreover, the task force formed within

the department on Nov 2022 referenced all countries with similar geographical and technical structures to Bhutan.

The criteria for the CII identification were determined through the ICM Act 2018, the definition of CII and 11 sectors was identified as CII. However, consultation with the corporate sectors resulted in including corporate sectors in the task force, taking into consideration.

Nonetheless, the consensus could not be met during the subsequent meetings when the stakeholders were asked to consult their management. For example, the ICT sector had TashiCell & Bhutan Telecom, both organisations having varied customer-based, industry experience and annual income/expenditure, as was the Energy sector with DGPC, BPC and BEA, with each sector having different business models, assets etc.

The BtCIRT could have conducted a series of meetings with both sectors with additional expenditure from the government but since the team had foreseen such meetings to have similar outcomes (through the past meetings), the decision was reached to conduct a risk assessment with experts.

The team had put in efforts to consult international organisations from Singapore, Malaysia, ITU, etc, through our initiatives, all free of cost which otherwise would have incurred millions in the form of consultancy service.

Rather than inadequacy of planning, it was insufficient knowledge of the job that was tasked to do. Bhutan does not have criteria but we do have assets identified in the Financial, Power and Communication Sectors. Moreover, other countries' methodology and international standards do not fit the purpose of Bhutan.

The identification of CII entailed trial and error and it is a good indication that rather than adopting a methodology in haste, the task force has gone through difficulty in the application of any of the methodologies.

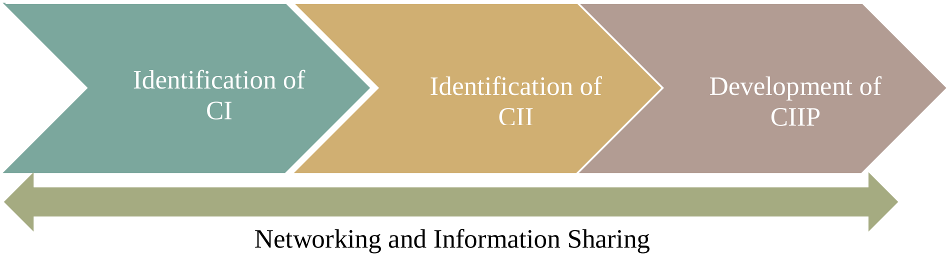
Two different methods were implemented as indicated through the above comments, including the methods espoused by the RAA.

While acknowledging the responses, the RAA is of the view that there is a substantial delay in identifying the CIIs despite the formation of the task force and this could result in not securing the critical infrastructure that is essential for critical services from cyber-attacks.

3.3.5 Protection of Critical Sectors and Critical Information Infrastructure

After the identification of CIIs, it is important to implement protection mechanisms for the identified CIIs. Critical Information Infrastructure Protection (CIIP) is defined in the GFCE Global Good Practices-CIIP, 2017, as *"All activities aimed at ensuring the functionality, continuity and integrity of CII to deter, mitigate and neutralise a threat, risk or vulnerability or minimise the impact of an incident".* The GCFE outlines the process for the development of CIIP as portrayed in figure 21.

Figure 21: The process of the development of CIIP



Source: RAA's interpretation of the steps for development of CIIP as per the GCFE

In Bhutan, the identification process of CIIs is yet to be implemented. The Draft NCS identifies the protection of CIIs under goal 2 which states that a CII regulation is to be developed through a comprehensive study of the requirements of CII regulation.

However, as per the steps mentioned in good practice, without the identification of CIIs, the implementation of the CIIP and the setting up of a coordinating body for CIIP cannot be commenced.

The improper selection of a methodology for the identification of CII has resulted in the delay in the identification of CIIs, further resulting in a lack of institution of protection mechanisms for potential CIIs. The absence of protection measures for CIIs could enable them to be exposed to cyber-attacks with debilitating impact on the critical sectors that support national security and stability, economic growth, citizen welfare, and safety. Therefore, the identification of CII is urgent to implement the protection of the CII.

The BtCIRT disagreed with the audit finding and explained that the first task is to identify the CIIs to protect the CIIs which is under goal 2 of the strategy.

The RAA also agrees that the identification of CIIs and protection of CIIs are laid down in the draft NCS. Nonetheless, the fact is that the NCS is not yet endorsed to implement these activities.

3.3.6 Baseline Security Measures

Baseline security measures are a set of bare-minimum security controls that an organisation needs to implement in order to sufficiently protect itself from vulnerabilities and cyber threats while still being able to work efficiently and effectively.

According to the ***National Institute of Standards and Technology (NIST)***, a “security control baseline” refers to “the set of minimum security controls defined for a low-impact, moderate-impact, or high-impact information system. A set of information security controls that have been established through information security strategic planning activities to address one or more specified security categorizations.”

The baseline security measures/controls assist an organisation to understand its cybersecurity posture and identify security measures that should be in place to provide adequate protection against cyber threats. Controls underpin all cybersecurity initiatives and can be composed of people, processes or technology.

BtCIRT, being the national point of contact for cybersecurity issues in Bhutan, is responsible for ensuring cybersecurity in government agencies, and national CIIs. Thus, BtCIRT should define generic baseline security measures for government agencies with low-impact ICT systems, government agencies with high-impact ICT systems, national CIIs and for e-services.

Upon review, the RAA noted most of the government agencies did not have a standard set of policies, procedures or solutions to implement solid baseline security controls. The RAA administered a survey to assess and validate the existence of baseline security controls in government agencies. The survey was sent to all the ministries, dzongkhags, and agencies. The survey assessed the following categories of security controls:

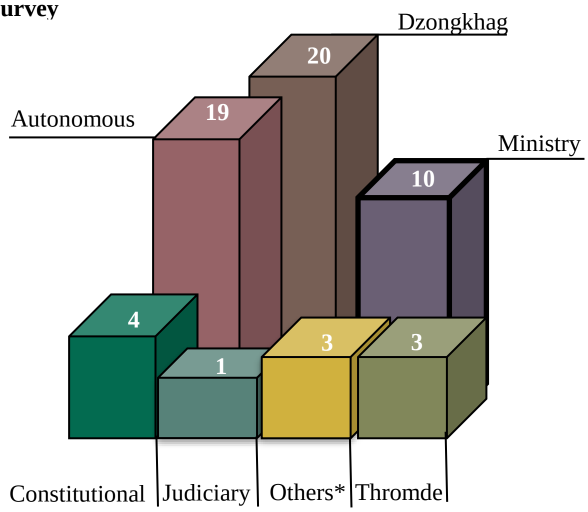
1. Network Monitoring and Defences;
2. Malware Defences and Continuous Vulnerability Management;
3. Access Control Management and Configuration;
4. Data Recovery;

5. Security Awareness;
6. Cybersecurity Incident Handling and Response Management; and
7. Incident Reporting

These seven categories of security controls were selected out of several security controls based on reviews of CIS Critical Security Controls V8, UK Cyber Essentials, CISA Cyber Essentials of the USA, and the Essential Eight Maturity Model of the Australian Cyber Security Centre. Further, these controls were reviewed and finalised considering their applicability in government agencies.

The RAA received 60 responses (10 ministries, 20 Dzongkhags, four constitutional bodies, Thromdes and autonomous agencies depicted in figure 22). Overall, the results of the survey revealed that most government agencies had embraced a fragmented approach focusing on one or two areas and did not have a holistic approach to security encompassing all categories of security controls to constitute baseline security controls.

Figure 22: Number of respondents for the RAA-administered survey



***Others category comprises of the Cabinet Secretary, the NAB and the NC**

On the other hand, the RAA noted that the financial institutions are required to implement 15 security controls as directed by the RMA as mentioned in the observation no.3.3.2. Further, the RMA conducted an on-site inspection on 29 June 2022 to ascertain the implementation of 15 security controls in the five banks (BOBL, BNBL, BDBL, T Bank, and DPNBL).

The RAA observed that even the CIIs as well as the government e-services which are paramount to security, the economic well-being of our citizens, and the efficient functioning of our government, did not have well-defined baseline security controls despite the necessity to implement them. Instead, the CIIs and e-services owners/operators have initiated the implementation of the security measures on their own. It is not clear if these would be adequate against cyber-attacks. Similarly, there are no defined security measures for private applications such as e-commerce web-based systems and/or apps in the market, OTT (over-the-top) platforms, etc.

Even though BtCIRT is the nodal agency for cybersecurity in Bhutan, BtCIRT has not yet defined a clear national baseline security controls/measures to ensure a bare minimum level of security including network and application security in the government agencies, national CIIs, state-owned corporations, or the media infrastructure agencies.

As the minimum set of application security measures is not defined, the system developers develop the application system considering only the business and application performance requirements. Later when vulnerabilities are detected in the application system, it becomes cumbersome and difficult to implement security measures as the platform of the application system is not supported and/or for fear of disrupting the services facilitated by the application system.

Since Bhutan does not have clearly defined baseline security controls, our government agencies and national CIIs do not have a consistent set of procedures or policies to adopt for ensuring adequate protection/security of data, networks, and information systems. If the security of our national CIIs is compromised, there will be huge repercussions or cascading effects on our population and economy. For instance, cyber-attacks could potentially cause our power, telecommunications and banking systems to shut down, disrupting operations and enabling attackers to remotely control the affected systems. This would not only create a huge reputational disaster but also could cripple our economy and set us back a few decades in our efforts to become an ICT-enabled knowledge society.

3.3.7 Security Audits

With cyberspace being ripe with threats and risks, organisations must implement plans and procedures to secure and defend the ICT infrastructure from cyber-attacks. However, it is not adequate to have security plans and controls in place; they must be audited consistently.

A security audit involves a comprehensive analysis and review of the IT infrastructure and proactively assesses the organisation’s security capabilities. It detects vulnerabilities and threats and displays weak links, and high-risk practices. It is also a primary method for examining compliance.

There are several reasons to undertake a security audit. They include these six goals:

- ✓ Identify security problems and gaps, as well as system weaknesses.
- ✓ Establish a security baseline that future audits can be compared with.
- ✓ Comply with internal organisation security policies.
- ✓ Comply with external regulatory requirements.
- ✓ Determine if security training is adequate.
- ✓ Identify unnecessary resources.

In a nutshell, security audits add a line of sight to evaluate as well as enhance security management. Therefore, security audits should feature in the operational plans of organisations as it helps protect critical data, identify security loopholes, create new security policies, and track the effectiveness of security strategies. As with other significant issues, top management must ensure independent validation and testing of their believed cybersecurity posture.

The RAA noted that in terms of security audits, there is no requirement for government agencies to conduct security audits. Moreover, except for the Ministry of Finance (MoF), none of the government agencies has conducted a security assessment to assess the strength of their critical controls and systems.

During the review, the RAA found that the MoF had contracted out the audit of the Public Financial Management information systems to Norway Registers Development AS in the Fiscal year 2020-2021. The IT audit was carried out to provide an independent opinion about the security posture of information systems in MoF. The following information systems were reviewed:

1. Multi-Year Rolling Budget System;
2. Public Expenditure and Management System;
3. Revenue and Administration Management System;
4. Bhutan Automated Customs System;
5. Electronic Government Procurement System; and
6. Asset Inventory Management System.

The scope included:

1. Systems audit (organisational and technical security controls);
2. Source code analysis;
3. Penetration testing;
4. IT risk assessment;
5. Gap analysis for international standards compliance (ISO 27001, COBIT);
6. Security policy;
7. Internal control; and
8. Audit trails.

With regards to financial service providers, the RAA observed that the RMA had directed the institutions to assess compliance with PCI-DSS and to even consider compliance with ISO 27001. As per the RMA, security audits are being conducted in all financial service providers annually. Likewise, the BPC undergoes a security audit annually.

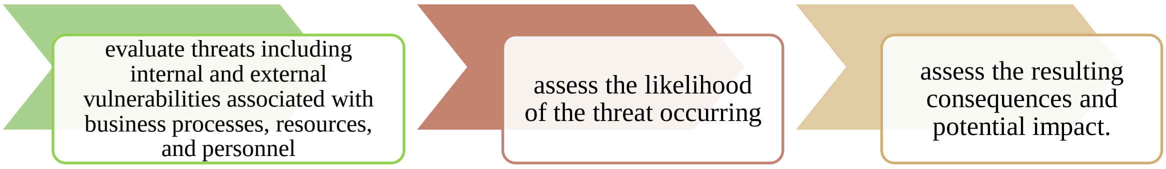
Other than financial institutions, security audits are not a regular activity in the operational plans of organisations with critical infrastructure. Without security audits, there is no way to ensure that the implemented security measures are effective, and inadequate or slow response against an attack could result in dire consequences.

3.3.8 Risk Assessment for CIIs

Performing an effective and well-organised risk assessment in an organisation is vital as it will ensure that the management can identify security gaps and implement suitable controls to improve security efforts and more importantly, ensure business continuity. Having a periodic risk assessment practice would ensure timely identification, categorization and treatment of risks. In addition, risk assessment is crucial to managing, and maintaining business operations and protecting critical information of an organisation.

The NIST explains risk assessment as a systematic method to identify and manage risks (depicted in figure 23).

Figure 23: Risk assessment process as per NIST.



evaluate threats including internal and external vulnerabilities associated with business processes, resources, and personnel

assess the likelihood of the threat occurring

assess the resulting consequences and potential impact.

Source: RAA representation based on NIST

Hence, all the CIIs should undergo risk assessment regularly and the results should be documented, reviewed, and mitigated by applying countermeasures. Moreover, a good risk assessment will result in the efficient allocation of resources and a more secure environment for the protection and continuity of the CIIs.

A case in point is a number of our government websites (MoWHS, MoH, MoE, MoFA, MoLHR) including financial banking websites were hacked in the past. Such incidents not only reiterate the point that Bhutan's information and computer systems are susceptible to cyber threats but also indicate a lack of preparedness to prevent such attacks from happening. One preventative mechanism for such a situation is carrying out periodic risk assessments.

Upon review, the RAA noted that conducting a risk assessment of the entire country was not feasible as it requires a lot of resources in terms of time and manpower. Nonetheless, a risk assessment of the national CIIs would have been timely and feasible.

The RAA found out that the BtCIRT had conducted numerous stakeholders' meetings to identify the national CIIs and recognised some of the agencies as the CIIs of Bhutan. However, the BtCIRT had never conducted any risk assessment of the CIIs so far. Since its inception, the BtCIRT did not have a clear strategic direction to carry out risk assessments of government agencies, national CIIs, and state-owned organisations. The banks (BOBL, BNBL, BDBL, T Bank, and DPNBL), BPCL, DGPC, and BPSO have themselves initiated to conduct periodic risk assessments by third parties.

Not carrying out risk assessment could result in neglecting critical risks that require immediate action or appropriate measures to be implemented by the organisations, which will cripple the business operations of the organisations.

For instance, if a CII such as ePEMS is compromised, there would be a significant setback in the ability of RGoB to carry out its crucial activities and government services would be greatly impacted in terms of financial services.

Similarly, if there is a major cyber-attack on the BPCL, the whole country would be affected since it is the backbone of the functioning of all the critical sectors such as the ISPs, banks, telecommunications, financial institutions, and government agencies.

The BtCIRT responded that it can only spearhead high-level nationwide risk assessment with the same guideline but cannot lead risk assessment. Risk assessments require the organisation/agencies to know its assets and identify risks. Further, risk assessment is not possible or feasible owing to the limited capability and capacity.

Additionally, the absence of qualified manpower in technical, strategic and legal aspects including lack of awareness and capacity at the management and leadership is a major challenge.

Taking note of the response, the RAA is of the view that there is no clear strategic direction to carry out a risk assessment of selected government agencies, national CIIs and SOEs. Moreover, periodic risk assessment is not conducted to identify critical risks and relevant measures to mitigate risks for ensuring a secure environment for the continuity of the CIIs.

3.4 Cybersecurity Awareness and Capabilities

The 'Guide to Developing a National Cybersecurity Strategy' by the ITU emphasises the importance of cybersecurity capacity building and awareness raising to enable a country's digital economy and ensure cybersecurity in the country.

Cybersecurity capacity-building and awareness-raising efforts should take place on different levels – amongst government entities, citizens, businesses and other organisations – and should cover a wide spectrum of cybersecurity knowledge starting from initial cybersecurity awareness to advanced technical cybersecurity aspects.

The RAA noted that the importance of cybersecurity awareness raising and capacity building has been recognised in the draft NCS under goal number 4.

The RAA, during the course of the audit, assessed the availability and provision of cybersecurity awareness and education programmes and observed the following:

3.4.1. Awareness and Advocacy on Cybersecurity

Education about the threats and risks that come with cyberspace is essential with the escalating use of cyberspace. Human actions account for a far greater degree of computer-related loss than all other sources combined. The key to addressing human factors is awareness, training, and education. Such programs enhance security by creating awareness of the need to protect system resources and develop skills and knowledge to assist computer users to perform their jobs or tasks securely.

Moreover, the advocacy and awareness programs also enhance the awareness of threats and teach Internet users to avoid scams and safeguard themselves from cybercrimes. Awareness and advocacy programs stimulate and motivate the audience about security, reminding them of essential security practices.

To improve awareness at all levels, advocacy and awareness programs should be designed and implemented at a national level in a coordinated and integrated approach. Additionally, as per the NIST and ENISA, the following elements should be considered to have effective national cybersecurity awareness and advocacy programs.

- single competent and dedicated agency to coordinate activities of the cybersecurity awareness program;
- clear vision in national cybersecurity strategy mentioning the need to conduct awareness, and assigning clear roles and responsibilities to relevant stakeholders;
- synergistic actions in all areas such as legal, organisational, technical, educational and cooperation between public and private sectors in raising cybersecurity awareness at both national and regional levels;
- sufficient, consistent and continuous funding to ensure the successful implementation of public awareness activities;
- provide regular analysis and report of threat environment to inform citizens, ICT experts, decision-makers, and society;
- accessible and comprehensible to the non-technical audience to enable outreach to a wider audience;
- provide regular employee training for cyber hygiene and awareness;
- quantitative data across the whole society on cybersecurity behaviour to understand the background of cybersecurity thinking and behavioural patterns of people;
- analyse data from relevant agencies and law enforcement agencies about cyber incidents and cybercrime to identify and build situational awareness;
- better methodologies and mechanisms to identify, understand, and reach target audiences;
- appropriate message framing to ensure a better understanding to address the human factor in cybersecurity;
- creative and frequently changed awareness techniques; and
- evaluation of awareness and advocacy programs to evaluate and ascertain the amount of information retained and general attitude towards cybersecurity.

As part of the audit, the RAA conducted a series of discussions with the BtCIRT to analyse existing methods for raising cybersecurity awareness at a national level. Further, the RMA and

RBP were consulted and a focus group discussion with the CII agencies was also held to understand their cybersecurity awareness-raising activities. The RAA evaluated the intensity, regularity and diversity of cybersecurity awareness practices based on the collected information from discussions, annual reports, and other documents. Upon review, the RAA noted the following:

3.4.1.1 General Awareness and Public Educational Activities

The BtCIRT, as the national point of contact for any cybersecurity issues, has the responsibility to carry out cybersecurity awareness in the country. Accordingly, the BtCIRT conducts awareness and advocacy programs including observation of Cybersecurity week.

Table 9 shows the list of cybersecurity awareness and advocacy programs conducted by BtCIRT since 2016.

Table 9: List of awareness and advocacy programs conducted by BtCIRT

Target Audience	Mode of awareness	Areas Covered
General Public	Panel Discussion in BBS English program	Public prevalent scams, Online scams, BtCIRT's roles and initiatives, basic cyber hygiene
General Public	live demonstration and a brief presentation	Secure communication using emails and social media services, protection of personal information to avoid social engineering attacks, recognising and identify phishing emails, and the good habits to become safer Internet users.
General Public	Videos, panel discussions, BtCIRT Facebook page, national television channel	WhatsApp OTP Scam and How to recover from such scams
General Public	Six articles Kuensel, Bhutan Today, The Bhutanese, Business Bhutan and Bhutan Today	Security topics such as BtCIRT initiatives, online threats, crimes and scam
General Public	Quizzes and cybercrime victim stories	Open awareness program and Cyber hygiene awareness program as a part of cybersecurity week
High School students		
Local Banks	FICRT	
Primary, Middle, and Higher Secondary Schools	Awareness videos and Animation	Social media phishing and scams, password security and email security Online predators, privacy and identity theft and gaining scams
Children	Digital comic book	Online privacy, cyberbullying and the role of parents and guardians
General Public	Videos	Secure Mobile Banking, Banking frauds and the use of OTP/ (One Time Password)/2FA (2 Factor Authentication).
Students from Royal Thimphu College and Khesar Gyalpo University of Medical Science		Basic Cyber hygiene awareness workshops were conducted
National Scout Center, Paro for class 12 graduates		Advocacy on cyber hygiene

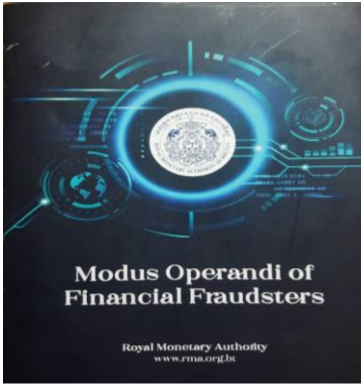
High school students	Four-page article Happiness Journal, local magazines (local magazine)	Online safety Top Tips
General Public	Four awareness videos and three animation videos broadcasted through National television channels and social media platforms	Social media phishing and scams, password security and email security
School going children		Online predators, privacy and identity theft and gaining scams
Primary, Middle, and Higher Secondary Schools	Posters (A1 and A2 sized) Distributed through Bhutan Post	

Source: RAA compilation based on BtCIRT and DITT Annual Reports

The Cyber Crime Unit of RBP shares emerging cyber threats, cyber-crime and scams to the general public through their Facebook page, "Cybercrime Awareness, Keeping Informed".

Similarly, the RMA has published the Modus Operandi of Financial Fraudsters (figure 24) to ensure cyber-safety. The modus operandi is divided into two parts, part A covers the cyber fraud in FSPs such as phishing, vishing, frauds via online selling platforms, QR code scams, OTP-based frauds, impersonation vis social media, and lottery fraud. Part B provides general precautions to be taken during a financial transaction. The modus operandi is distributed to schools, national libraries and national newspapers.

Figure 24: Modus Operandi of Financial Fraudsters published by RMA



During the focus group discussion, the RAA learnt that financial institutions share emerging threats and cyber news with their clients and customers through their respective social media pages, national television channel and newspapers.

Despite numerous awareness and advocacy programs, there were several incidents reported in the newspaper on individuals becoming victims of computer scams. Additionally, the following were observed:

i. According to the draft NCS, the National Cybersecurity Working Group (NCWG) will *'develop a roadmap that lists different capacity building and awareness programs that the country requires and other recommendations to match the capacity requirements. The roadmap will be developed based on the prior information and statistics related to cybersecurity awareness and training existing in all relevant agencies.'* Further, the draft strategy mentioned that the Child Online Protection Working Group (COPWG) *'shall develop and provide recommendations with regard to training material for children as well as for guardians and teachers.'* However, the activities related to the awareness program are yet to be implemented pending the approval of NCS.

ii. Different agencies conduct awareness and advocacy programs independently. This indicates the lack of coordination among the public and private sectors in raising cybersecurity awareness, resulting in duplication in efforts. Additionally, the awareness programs by the banking sectors are reactive.

iii. Awareness of the BtCIRT and its responsibilities was conducted twice but it has been noted that some private sectors and individuals are not aware of its existence. *For* *instance*, if there is a cyber incident in a State-Owned Enterprise (SOE) or a private company, the general practice is to report to their ISP and not BtCIRT.

iv. There is limited coverage of the consequences including legal and financial consequences.

v. There were no studies undertaken and metrics established to understand the cybersecurity behavioural aspects which could guide awareness-raising activities.

vi. The effectiveness of cybersecurity awareness is not measured and evaluated.

The delay in finalising the NCS has resulted in the non-implementation and execution of cybersecurity awareness activities assigned to agencies. Moreover, the lack of qualitative data on cybersecurity behaviour, cyber incidents and cyber-crime has also ensued in inefficiency in identifying the target audience, key areas to cover, and coverage and frequency of the awareness programs.

With a lack of effective cybersecurity awareness programs, adapting to 'digital by default' would be a challenge. A well-designed and standardised awareness and sensitisation program would not only lead to behavioural change but drive awareness, address threats, and ensure compliance with basic security measures thereby contributing to improving the cybersecurity posture of the country.

The BtCIRT explained that most of the activities, such as observation of National Cybersecurity Week, National Cyber Drill, Child Online Protection, production of timely advocacy videos and digital literacy have been initiated and the works are under progress even without the implementation of the NCS.

The BtCIRT informed that it is necessary and beneficial to conduct awareness programs time and again and that it is not a duplication of effort. Further, some sectors like the banking sector need to provide specific awareness related to securing mobile payment apps, being aware of prevalent financial scams, etc. Where coordinated efforts are required like in the case of Cybersecurity Week, the awareness programs have been conducted with the involvement of all the stakeholders.

Regarding the visibility and report of cyber incidents to ISPs, the BtCIRT stated that for immediate containment and support it is required to report to ISPs or agencies concerned and then report to BtCIRT. BtCIRT has been working closely with ISPs and they do share the incidents with BtCIRT.

The BtCIRT justified that due to the resource constraint, it was not feasible to conduct specific programs on cybersecurity behavioural aspects and likewise effectiveness of cybersecurity awareness is not measured and evaluated.

The justification provided is duly noted. However, the BtCIRT has not collected and analysed data on cybersecurity behaviour, cyber incidents, and cybercrime to identify the target audience, key areas to cover, and coverage and frequency of the awareness programs.

3.4.1.2 Employee Training for Awareness and Cyber Hygiene

Given the fact that the majority of attacks occur as a result of negligence and oblivion, employee training for awareness and cyber hygiene plays an important part in shoring up an organisation's cyber defence. Employee training for cyber hygiene and awareness will strengthen the dissemination, implementation, and enforcement of cybersecurity measures within the organisation. Such programs enhance behavioural changes by increasing employees' knowledge of their accountability and penalties associated with errors and omissions. Therefore, employees should receive appropriate cybersecurity awareness training tailored according to their roles. There should be periodic and mandatory training for current employees and new employees.

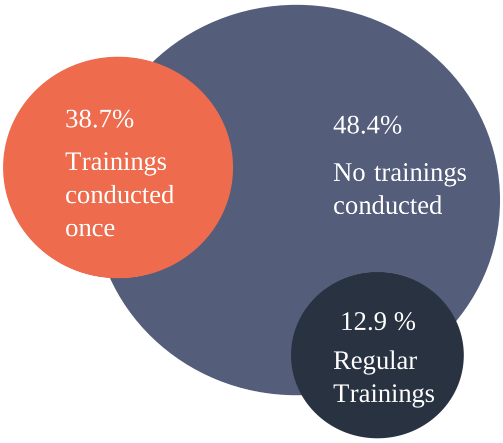
The RAA noted through the focus group discussion that financial institutions are required to conduct regular cybersecurity awareness as part of ISO certification. Therefore, ISO-certified financial institutions conduct awareness programs for their employees including phishing simulations every quarter. Moreover, it was learned that the BoBL has plans to institute accountability mechanisms for human errors resulting in cyber incidents.

Further, the BtCIRT provided awareness training to senior leadership and officials in February 2022 on cybersecurity trends and risks, implications of cyberattacks and data breaches, and security management in a public agency.

While the employees are provided with regular cybersecurity awareness training in financial institutions, the RAA observed it is not a regular activity in government agencies as per the survey administered by the RAA to assess and validate the existence of baseline security controls in the government agencies.

In the category of 'Security Awareness' of the questionnaire, the RAA asked the respondents (a total of 60 respondents) whether their organisation had provided employee training to raise cybersecurity awareness. The results of the survey depicted in figure 25 revealed that almost half (48.4%) of the respondents' organisations did not provide employee training to raise cybersecurity awareness, while 38.7 % of organisations had conducted such training only once.

Figure 25: Training provided to employees to raise awareness



Source: As per the survey administered by the RAA

Nonetheless, 12.9% of organisations are conducting training more than two times annually as part of general training, workshops, or conferences. Yet, the RAA found that most of the cybersecurity awareness training is based on presentations covering several topics at a time, making it challenging for employees to retain and implement security good practices.

Additionally, the majority of the workforce employees including those from the government, SoEs, and private sectors are not provided with cybersecurity awareness training. The majority of untrained employees may be vulnerable to cybersecurity threats and pose a potential gateway for cyber threat actors to gain access to the organisation's sensitive information.

Further, the remote workers may inadvertently act in ways that would expose the organisations to cyber threats and cause damage such as financial loss, remediation cost, loss of intellectual property, physical risk, reputational risk, and loss of trust.

The GovTech Agency has implemented the Digital Literacy program under the Digital Drukyul Flagship Program which also included a module on security and cyber-hygiene. It was first targeted at all civil servants and then at the general public.

3.4.2. The capacity of the BtCIRT

National Cyber Incident Response Team (CIRT) plays a critical role in providing its constituents with services and support in the assessment, management, and prevention of cyber-related incidents. The main responsibility of CIRT is to respond to computer security incidents effectively and quickly to regain control and minimise damage and impact in coordination with relevant stakeholders at the national level. Therefore, CIRTs should be an organised entity with a defined mission, structure, roles and responsibilities.

Technical skills required of a CIRT team member include (insert reference):

- Baseline skills such as understanding security principles, network protocols, vulnerabilities, and programming;
- Techniques and tactics to identify intruders;
- Knowledge of encryption to secure CIRTs communication; and
- Analytical skills to diagnose incidents to determine effective response mechanisms.

Moreover, CIRT is a service-based work and non-technical skills such as negotiation and communication competency in interaction with constituents are essential.

Having understood that officials in BtCIRT should have both technical and managerial skills to implement and deal with all cybersecurity matters in the country, there should be a review of skills gap analyses regularly and accordingly, prepare capacity-building plans. Skills and knowledge gap analysis compare the current skills to the required skills and knowledge. There should be a competency-based framework and capacity assessment framework to determine the gap and enhance and build cybersecurity capabilities. These have the following benefits:

- Guide an organisation to identify required skills;
- Identify knowledge gaps in current cybersecurity policies and procedures;
- Assist continuous professional development;
- Ensure training and development efforts are effective, goal-oriented and meaningful;
- Enhance recruitment and performance evaluation (as performance indicators that you are expected to perform);
- Bring added value to strategic planning and implementation;
- Evaluate current cybersecurity practices against applicable international or local standards and best practices;
- Develop mitigation plans and implement new procedures; and
- Identify vulnerabilities in cybersecurity practices and procedures.

The RAA noted that knowledge and skill gap analysis was not conducted to identify the need to secure digital public services and secure government organisations and GDC. Nevertheless, the BtCIRT has carried out a human resource gap analysis (quantitative) against the entrusted mandates, roles and responsibilities of BtCIRT with the available human resource.

Besides the core function of incident response management, BtCIRT is also entrusted with the overarching mandate to oversee and implement all cybersecurity matters in the country (as reported earlier in the audit finding 3.2.2). In addition, CIRT services require the team to provide risk assessment and penetration testing services but the risk assessment and security assessments (Ethical hacking or Penetration testing) have not been provided due to a lack of capacity.

The DITT has a competency-based framework for all ICT officials to guide continuous professional development and performance evaluation, and to ensure that training and development efforts are effective, goal-oriented, and meaningful. Table 10 shows various cybersecurity-related training provided to ICT officials under MoIC since 2016.

Table 10: List of Cybersecurity related training/certification courses attended by ICT personnel under MoIC

Course	Number of Participants	STT Type/Level
30th Forum of Incident Response and Security Team	3	Certificate Course
7th Annual Meeting of Cybersecurity Alliance for Mutual Progress (CAMP)	1	Conference/Symposium
APISC Security Training Course	1	Certificate Course
APT Online Training Course on Future Network Technologies/Cyber Network defence and cybersecurity technologies	4	Certificate Course
BTNOG Training	10	Certificate Course
CCNA course/training with certificate Exam/Training on CCNA-S and CCSP/Training on CCNP	13	Certificate Course
CCSA & CCSE Training	2	Certificate Course
Certificate in Networking & Internetworking Technologies, Design & Implementation.	4	Certificate Course
Cyber Security Policies & Technologies Broadband C	1	Certificate Course
Cyber Security Sequence Training	1	Certificate Course
Cyber-Tech Global TelAviv 2022 Conference	3	Conference/Symposium
Ethical Hacking Training	2	Certificate Course
Executive Cybersecurity Workshop from USA	2	Seminar/Workshop
Integrated Cybersecurity for a safer Digital World	1	Certificate Course
Network Administration Using Window2000 Server	1	Seminar/Workshop
Network Design, development, Management and Maintenance/Networking & Internetworking Technologies	3	Certificate Course
Network Visualization & Optimization	1	Certificate Course
Penetration Testing course	2	Certificate Course
Red Hat System Administration and Red Hat System Administration with Red Hat Certification	3	Training/Certificate Course
SANOG Workshop/VI Workshop at banquet Hall	4	Seminar/Certificate Course
SASEC ICT Working	2	Certificate Course
Singapore Cooperation programme offer on "Integrated Cybersecurity for Safer Digital Worlds"	1	Certificate Course
Security Measures for the Era of Artificial Intel	4	Seminar/Certificate Course
Telecommunications Policy Course	2	Certificate Course
Training in Securing Linux	1	Certificate Course
Training on Campus Networking and security/Network and Security	5	Certificate Course
Training on Cyber Security Policies & Technologies	2	Certificate Course
Training on Cybersecurity and CERT/CIRT	4	Certificate Course
Training on Juniper Networking	2	Certificate Course
Training on system administration and Network Monitoring	3	Certificate Course/Seminar
Trends and Technology Broadband/Workshop on Networking	2	Seminar
Trends of ICT Network & Applications	2	Certificate Course
Cybersecurity Specialist Course on Practical Penetration Testing	15	Certificate Course
Total	107	

Source: RAA extraction of HR training data provided by HRD, MoIC.

Despite having a competency-based framework for ICT officials, and a series of cybersecurity-related training being provided over the years, the BtCIRT is still facing challenges in several areas including vulnerability and patch management, ineffective malware cleaning, and data privacy.

In absence of gap analysis, the maturity level for building cybersecurity capabilities both at strategic and operational levels could not be determined which has resulted in providing a range of training, some of which may not have been relevant. Furthermore, the delay in implementing the draft NCS defining the strategic objective of cybersecurity has resulted in a delay in the evaluation and development of cybersecurity capabilities (core competencies). Limited capacity and manpower shortages have also led to delaying the development of required policies and strategies.

Consequently, these will impact the identification of areas to improve and build cybersecurity capabilities, which would otherwise sustain the growth of the BtCIRT's capacity.

The BtCIRT responded that all the training listed is not attended by their staff and the current training received is not sufficient. The BtCIRT requires other capabilities such as digital forensics, log analysis, reverse engineering and malware analysis.

The RAA acknowledges the response provided by the BtCIRT. The training topics based on gap analysis would have been effective in building and sustaining the appropriate skills and competencies required of a cybersecurity professional.

3.4.3. National Educational Programmes

The *Building Cyber-Security Capacity in the Kingdom of Bhutan*, conducted by the World Bank in collaboration with the Global Cyber Security Capacity Centre in 2015, reports on the assessment of the cybersecurity capacity in Bhutan. The assessment was carried out in five dimensions and in the dimension, 'Cyber-security Education, Training and Skills', Bhutan's level of maturity was at the 'Start-up' stage. This means that in this dimension, there is no or little capacity. This level of maturity may also reflect that no concrete action has been initiated.

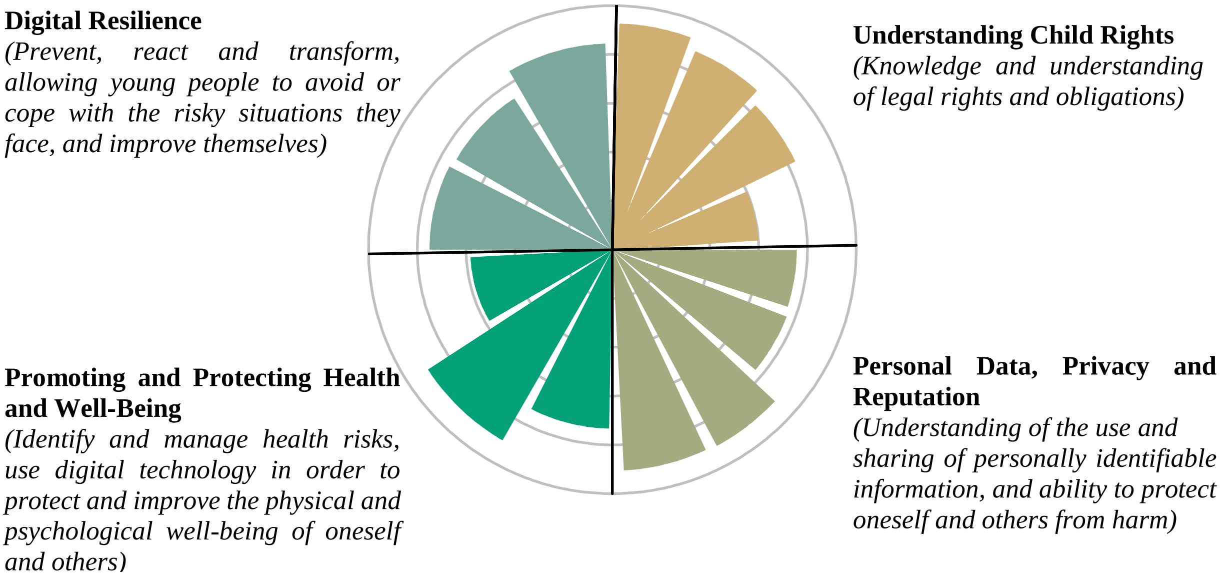
The report further found that cybersecurity in a formal education setting in Bhutan was yet to be developed and the mandate for developing cyber-security education was non-existent. Considering the findings of the report, the RAA reviewed the education programmes relating to cybersecurity at three levels, the school level (From Class PP-XII), the higher education level (Degree Programmes), and the professional level (Certification Programmes) and noted the following programmes.

a) Cybersecurity Education Programmes in Schools

The Country Report of Bhutan on the Digital Kids Asia Pacific (DKAP) was conducted in 2020 by the Ministry of Education (MoE) with the objective to examine children's attitude, behaviour, safety, competency level, and use of ICT when engaging with the Internet or digital technologies in the classroom and at home. The report sampled 1,191 students aged 15 years old from a total of 9,962 students across the country.

Overall, the study found that almost all the students have access to smartphones and other digital devices with internet connectivity both at home and at school. Students also spend from 1 to 2 hours a day on the internet and are mostly online at home. Having such access to digital devices and the Internet, the students showed a high level of understanding of Digital Safety and Resilience. The questions in this area of the study focused on gaining an understanding of the ability of children to protect themselves and others from harm in the digital space. Figure 26 depicts the representation of students' understanding and ability in the four sub-competencies in Digital Safety and Resilience.

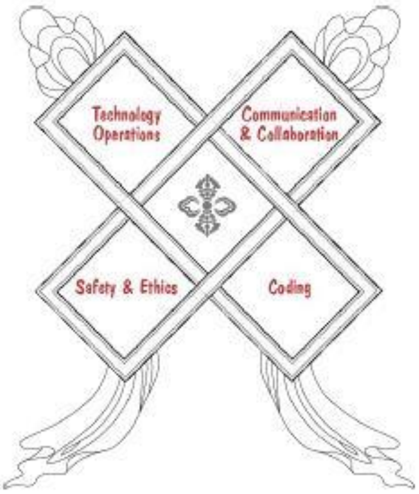
Figure 26: Students' understanding and ability in the four sub-competencies in Digital Safety and Resilience



Source: RAA's representation based on the Result of the Country Report on the Digital Kids Asia Pacific

The high level of understanding and ability of the four competencies under Digital Safety and Resilience can be attributed to the curriculum framework geared towards such developments. The ICT Curriculum Framework (Classes PP-XII) developed by the Department of Curriculum and Professional Development under the MoE, grouped the standards and competencies in all classes into broad thematic areas called strands as portrayed in figure 27.

Figure 27: Four strands identified in the ICT Curriculum Framework

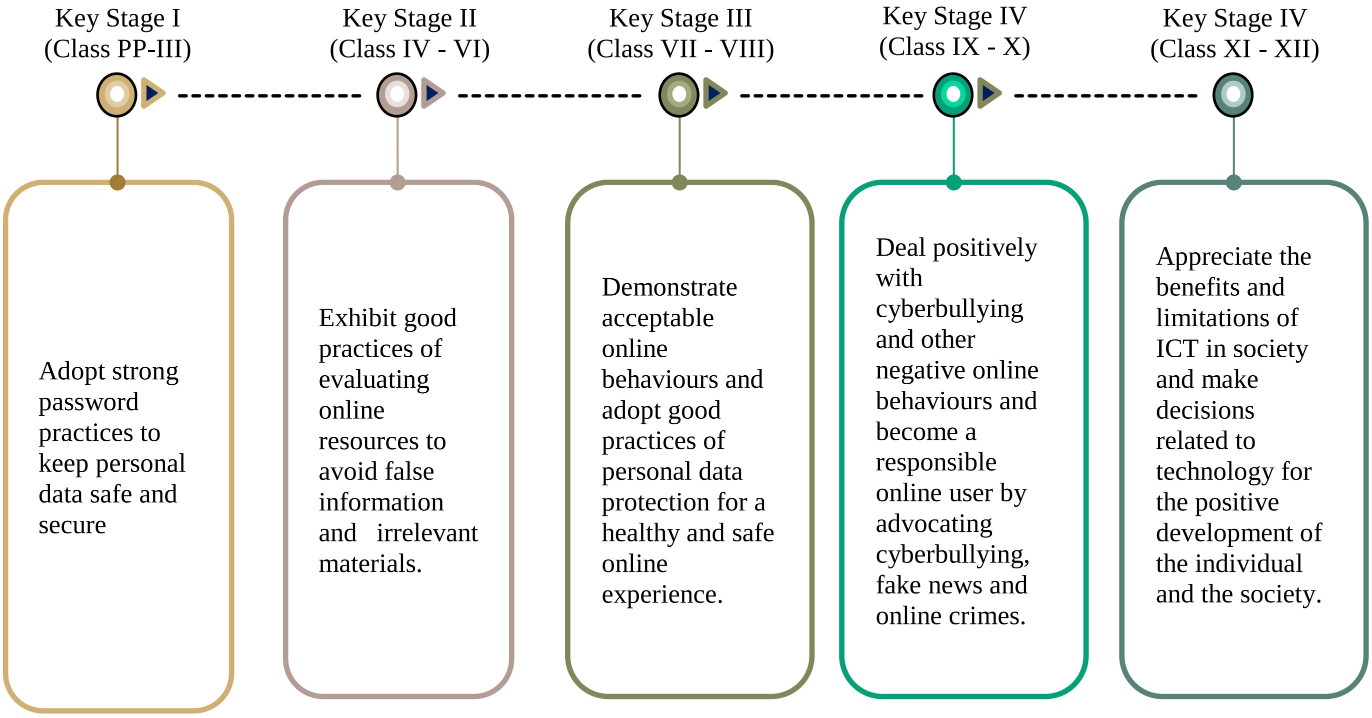


Source: ICT Curriculum Framework, 2021

The 'Safety and Ethics' strand prepares the students to evaluate the various positive and negative impacts of computers on society and demonstrate an understanding of ethical, cultural and societal issues related to technology. They practice responsible use of technology systems and information and develop positive attitudes towards technology that support lifelong learning.

The learning standards and competencies are further divided into five key stages with competency-based standards identified at each key stage as represented in figure 28. The competencies include the adoption of strong password practices to protect personal data, data backup and malware prevention strategies and demonstrating responsible behaviour online.

Figure 28: Competencies of each key stage



Key Stage I (Class PP-III)

Adopt strong password practices to keep personal data safe and secure

Key Stage II (Class IV - VI)

Exhibit good practices of evaluating online resources to avoid false information and irrelevant materials.

Key Stage III (Class VII - VIII)

Demonstrate acceptable online behaviours and adopt good practices of personal data protection for a healthy and safe online experience.

Key Stage IV (Class IX - X)

Deal positively with cyberbullying and other negative online behaviours and become a responsible online user by advocating cyberbullying, fake news and online crimes.

Key Stage IV (Class XI - XII)

Appreciate the benefits and limitations of ICT in society and make decisions related to technology for the positive development of the individual and the society.

Source: RAA's representation of the competencies at each Key Stage from the ICT Curriculum Framework (Class PP-XII), Department of Curriculum and Professional Development

b) Cybersecurity Education Programmes in Higher Education

The Gyalpozhing College of Information Technology (GCIT), under its School of Computing (SOC), offers two degrees; a Bachelor of Computer Science (Blockchain Development) and a Bachelor of Computer Science (Full Stack Development). Becoming a Cybersecurity Professional has been identified as a career prospect under both degree programmes.

The two elective units that are offered to the students under the SOC are Cybersecurity and Technopreneurship. The cybersecurity course offers three modules to the students comprising of the following:

i. Cyber Growth Conversation

This module aims to equip the students with a fundamental awareness of cybersecurity, which in turn enhances their preparedness and resilience to cybercrimes against themselves and beyond. Additionally, the module covers the basics of cybersecurity, tools and methods used in cybercrimes and vulnerabilities in information systems and organisations and exposes the students to the essentials of cyber forensics and security ramifications of emerging technologies.

ii. Secure Coding

The objective of the module is to equip students with the basic principles for producing secure software and applications, through a series of tutorial and practical exercises enabling students to write programs without security vulnerability for web, mobile and database applications.

iii. Ethical Hacking

The outcome of this module is enabling the students to develop an understanding of and practical experience in ethical hacking techniques. Performing detailed reconnaissance, exploiting target systems to gain access and measure real business risk and scanning target networks using best-of-breed tools in a virtual computer network which is set up as a training environment with the motivation to make systems and networks safer are the learning objectives.

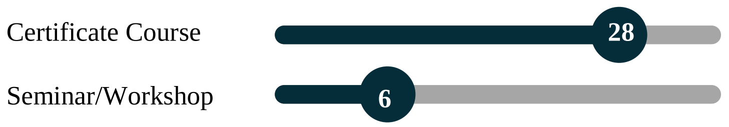
The RAA noted that the cybersecurity course unit is in line with the capacity gap strategy identified in the Building Cyber-Security Capacity in the Kingdom of Bhutan Report. The report stated that modules in information security or if possible, cybersecurity, should be promoted across all universities with computer science degrees.

c) Certification of ICT Professionals in Cybersecurity

The ICT landscape is always changing, this is especially true when it comes to cybersecurity. The emergence of new evolving threats requires organisations to continuously improve their security posture by continuously developing the knowledge and skills of their employees to combat such threats. Providing specialised cybersecurity training for those responsible for managing cybersecurity within the organisation will ensure that they will have the skills and competencies required to do their jobs.

The review of the training programmes attended by the MoIC staff from January 2016 to September 2022 shows that a majority of training on cybersecurity is for certificate courses as shown in figure 29. These trainings have been attended by ICT professionals at various levels (from P and SS levels).

Figure 29: Certificate courses and meetings/symposiums/workshops attended



Source: RAA representation of HR training data provided by HRD, MoIC.

Nonetheless, the training programmes attended by the ICT officials do not include certification programmes on cybersecurity.

The Readiness Assessment Report for Establishing a National CIRT 2012 by the ITU found that ICT personnel are aware of cybersecurity certification courses overseas, but are unable to access them due to a lack of financial resources.

Although there are IT courses offered by training institutes in the country, none of the training institutes offers cybersecurity certification courses. This has further added to the difficulty faced by ICT officials in gaining proper certification in cybersecurity.

The certification of ICT professionals in cybersecurity will ensure that the ICT officials that are responsible for cybersecurity in their organisation are equipped with the appropriate skills and knowledge to perform their duties and ensure that the organisations follow cybersecurity standards and reduce cyber threats to CIIs and other sensitive information. This in turn will improve the overall cybersecurity posture of the organisation.

The Cybersecurity Skills Development in the EU report by the ENISA identified the challenges in cybersecurity education and training. The main recommendation of the report highlighted the importance of major stakeholders engaging in discussion to clearly define the education and market requirements. These discussions will enable defining what cybersecurity students ought to know and be able to do upon graduation and before entering the labour market.

Although education programmes concerning cybersecurity have been initiated at all levels of the review, the RAA found no records of discussion between the various major stakeholders to define education and market requirements.

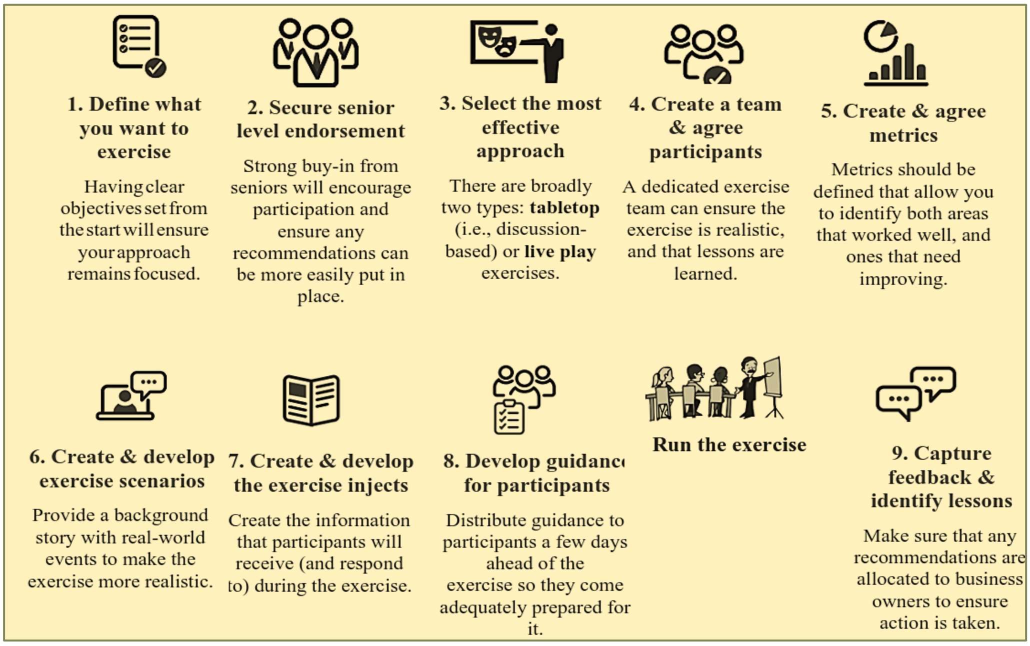
Lack of such discussion would result in the issues affecting cybersecurity education such as the lack of cybersecurity educators, poor interaction with the industry, little understanding of the labour market, outdated or unrealistic platforms in education environments and difficulties in keeping pace with the changing environment.

3.4.4. Cyber Drill Exercises

A cyber drill exercise is a planned event where organisations simulate cyberattacks, information security incidents, and other types of disruption. It exposes the realistic situations that can occur in day-to-day operations. Cyber drill exercise tests whether the organisation can detect and respond quickly and effectively to a cyber incident and helps organisations to build resilience to cyber-attacks, and practice their responses in a safe environment.

Figure 30 depicts the process of conducting a cyber exercise developed by the NCSC, UK.

Figure 30: Process to conduct cyber drill exercise



1. Define what you want to exercise

Having clear objectives set from the start will ensure your approach remains focused.

2. Secure senior level endorsement

Strong buy-in from seniors will encourage participation and ensure any recommendations can be more easily put in place.

3. Select the most effective approach

There are broadly two types: **tabletop** (i.e., discussion-based) or **live play** exercises.

4. Create a team & agree participants

A dedicated exercise team can ensure the exercise is realistic, and that lessons are learned.

5. Create & agree metrics

Metrics should be defined that allow you to identify both areas that worked well, and ones that need improving.

6. Create & develop exercise scenarios

Provide a background story with real-world events to make the exercise more realistic.

7. Create & develop the exercise injects

Create the information that participants will receive (and respond to) during the exercise.

8. Develop guidanc for participants

Distribute guidance to participants a few days ahead of the exercise so they come adequately prepared for it.

Run the exercise

9. Capture feedback & identify lessons

Make sure that any recommendations are allocated to business owners to ensure action is taken.

Source: NCSC, UK

Conducting cybersecurity exercises provides but is not limited to the following benefits:

- ✓ Organisations can identify what is working well and such strategies can be emulated by other organisations, and employees can further train others.
- ✓ It helps the organisation to improve its response to future attacks.
- ✓ The response team can include management to have support and fast decision-making during the incident response.
- ✓ The employees will gain practical experience in dealing with an attack.
- ✓ Cybersecurity exercises can provide accurate cost estimates and timescales involved, which will help to build greater resilience or use for any financial justification that

might be required. Further, it will help in figuring out where to invest budgets in training or new technology.

- ✓ It will also help in determining if external expertise is required to respond to cyber-attack and in understanding the actual versus perceived capabilities of the employees and technology used.
- ✓ The exercise will help to expose technical vulnerabilities on the network or weaknesses in security controls. This will in turn help to prepare remediation plans and act immediately to improve on the weaknesses identified.

It is thus imperative for the organisation to conduct cyber drill exercises to be able to detect and respond quickly and effectively to a cyber incident to reduce impact on the organisation. The ITU also improves cybersecurity readiness, protection and incident capabilities by conducting cyber drill exercises at regional and as well as international levels.

As per the annual report 2018, 2020-2021 and 2021-2022 of the BtCIRT and subsequent discussion with the officials from the BtCIRT, the following activities have been carried out on cyber drills as detailed in table 11.

Table 11: Cyber drills conducted

Sl. No.	Date of Drill conducted	Drill Name	Specific exercises conducted	Duration	Participants	Conducted by
1	12-16/11/2018	Security Incident Mock Drill	Plausible cybersecurity cases and commonly occurred incidents	1 Day	(DITT-INFRA, APP, BtCIRT) JDWNRH, NLC, RAA, MoF, RBP, ACC, MoAF, BIL	Asia Pacific Network Information Centre & BtCIRT
2	27/11/2018	Cyber Security Incident Simulation Exercise	Tabletop Exercise (Incidents generated Dynamically)	1 Day	Heads of government, policymakers and other high-ranking figures	Prof. Marco Gercke from Cybercrime Research Institute
3	27/10-5/11/2020	ITU Global Cyber Drill 2020	-Web server compromise -Data exfiltration -Lateral movement in the network -Operational Technology Attack -Cyber Anon Advanced Persistent Threat (APT) attack scenario -Ransomware attack	6 Days (3hrs each)	CIRT/CERTs of ITU member countries including BtCIRT	ITU experts
4	2-11/11/2021	ITU Global Cyber Drill 2021	-Botnet attack -Memory Forensics -Operational Technology attack -Analyzing malicious exploits caused by a spear phishing email	6 Days (3hrs each)	CIRT/CERTs of ITU member countries including BtCIRT	ITU experts

Sl. No.	Date of Drill conducted	Drill Name	Specific exercises conducted	Duration	Participants	Conducted by
			-Opensource Intelligence (OSINT)			
5	25/08/ 2021	Annual APCERT drill	Supply Chain Attack Through Spear-Phishing	1 Day	BtCIRT	Asia Pacific Computer Emergency Response Team
6	11-14/07/ 2022	ITU-Bhutan Cyber Drill 2022	1. General (Sector-neutral) "**Reviewing a Cyber Threat Intelligence Report**" 2. Finance/Banking Sector Specific "Someone got phished" 3. Threat Hunting 4. Operational Technology Specific	2 Days	Bhutan Telecom, Tashi Cell, RMA, BNB, BOB, T-Bank, DrukPNB, NPPF, RICB, BDBL, BIL, MoF, MoH, MoE, MoEA, MoWHS, Nano, BtCIRT, Tech Park Ltd, BPC, DGPC, Bhutan Automation	ITU and BtCIRT Joint Cyber Drill

As shown in table 11, the cyber drills are mostly conducted through international collaborations or solely by international experts. Until now, the BtCIRT has not conducted any cyber drills independently. Further, the RAA noted that cyber drills are performed on a cyber range platform and no hands-on cyber drill has been conducted on agencies' systems. Similarly, through the focus group discussion, the RAA also found out that CII agencies from the energy sector, financial sector, and telcos have not conducted cyber drills in their agencies.

Cyber drills not being conducted in the CII agencies and the BtCIRT not hosting cyber drills can be attributed to the limited resources. If the CII agencies and government agencies or the private agencies do not conduct the cyber drill, cybersecurity readiness and their response capabilities cannot be evaluated. If a cyber incident occurs, the response team will not be in a position to handle incidents that could cause serious threats to the provision of essential services, data security, and public safety.

BtCIRT justified that to prepare drill scenarios, resources such as separate labs with sufficient hardware servers are required but BtCIRT does not have a lab nor the space, time, and finance. Moreover, Cyber Drills are supposed to be conducted in a simulated environment as they cannot be conducted on an organisation's live systems.

While acknowledging the challenges and the constraints faced by BtCIRT in conducting independent cyber drills, cyber drill exercises are essential to assess the capabilities and ensure readiness in responding to cyber incidents.

3.5 Incident Handling Mechanism

Incident handling is crucial for organisations to manage and enhance cybersecurity, and achieve security maturity. An incident handling mechanism is a system that constitutes plans, procedures, tools and resources to prevent, protect, mitigate, detect, respond to, and recover from incidents. Recognising the importance of incident handling mechanisms, even the draft NCS has identified robust incident handling as one of the strategic goals. The RAA evaluated and assessed the adequacy of the incident handling mechanism and observed deficiencies which are discussed hereunder.

3.5.1 Cyber Incident Handling

A cyber incident is any event that has an impact on any of the components of cyberspace or the functioning of cyberspace. It may be natural or human-made; malicious or non-malicious intent; deliberate or inadvertent, due to incompetence; due to development, or due to operational interactions.

An unattended cyber incident can have serious ramifications in terms of disruption to normal business operations, unavailability of systems and services, financial loss, data loss, reputational damage, and attacks resulting in the exploitation of the organisation's interconnected systems. Therefore, it is important to have a proper incident response plan including preparation for incident detection, incident handling and analysis of security incidents, containment, eradication and recovery, post-analysis and learning procedures. More so, preparedness is a critical aspect of cyber incident management to enhance proactive, efficient and systematic response to minimise the impact.

To properly detect and analyse cyber events, there should be defined processes, appropriate technology, and sufficient baseline information to monitor, detect and alert anomalous and suspicious activities. Additionally, there should be cybersecurity strategies and action plans to identify vulnerabilities and provide the required framework to respond to risk.

Further, responding to cyber incidents and ensuring immediate restoration of critical services and reviving a disastrous interruption to activities after the incident requires a Disaster Recovery Plan (DRP). The DRP should define resources, actions, tasks, and data required to manage the recovery process in the event of disruption thereby, minimising damages and disruption to daily operations.

Moreover, an incident response plan should be a continuously evolving document that can be updated based on lessons learnt during an actual incident and changes in the risk landscape. Security weaknesses should be analysed to prioritise post-incident actions, the impact measured with proper documentation, impacted parties notified, and the incident reported to appropriate agencies including regulatory bodies and law enforcement.

The RAA observed the following after the assessment:

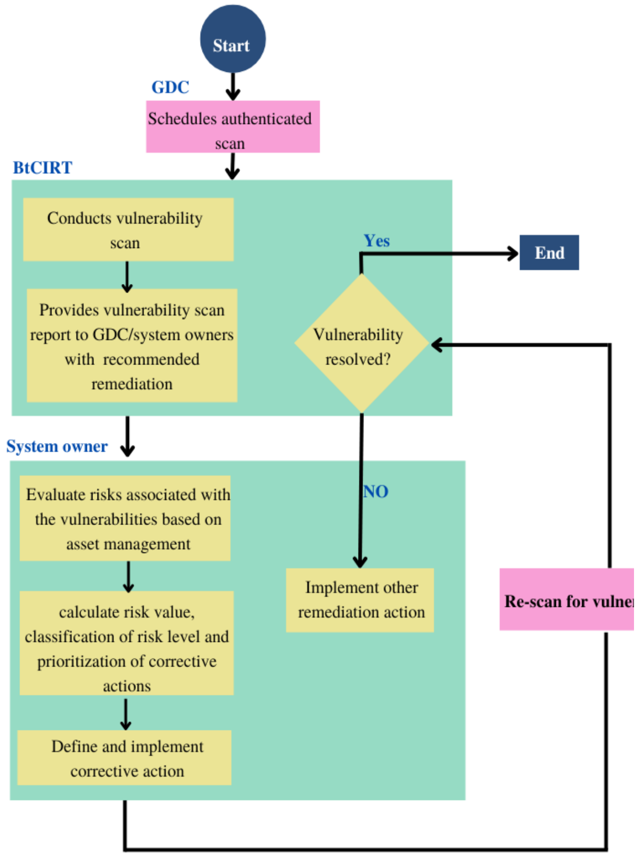
a) Detection of vulnerabilities

BtCIRT developed a Vulnerability Management Process for GDC, on 15 July 2017. The document aims to provide a high-level overview of the vulnerability management workflow for the GDC with standards and procedures for managing vulnerability. The Vulnerability Management Process flow is illustrated in figure 31.

Nonetheless, BtCIRT conducts vulnerability scans of IT systems hosted only in GDC but does not provide vulnerability assessment of known CIIs.

In addition, the RAA-administered security control survey revealed that 66% of government agencies do not have intrusion detection and prevention system, which are necessary for detecting external intruders. Even the BtCIRT does not have the required tools to detect the abnormalities at the national level.

Figure 31: Vulnerability Management Process Flowchart


Start
GDC
Schedules authenticated scan
BtCIRT
Conducts vulnerability scan
Provides vulnerability scan report to GDC/system owners with recommended remediation
Yes
End
Vulnerability resolved?
System owner
Evaluate risks associated with the vulnerabilities based on asset management
NO
Implement other remediation action
Re-scan for vulne
calculate risk value, classification of risk level and prioritization of corrective actions
Define and implement corrective action

Source: RAA analysis of Vulnerability Management Process Flowchart based on Vulnerability Management Process for GDC

b) Remediation of Identified Vulnerabilities

The BtCIRT issues a vulnerability assessment report to GDC and system owners along with the recommended remediation. The system owner and GDC need to evaluate risk and implement remediation. The GDC Incident Management Procedure [Version 1.0] (12 June 2017) provides standards and procedures to ensure immediate restoration of service operations and minimise adverse impact on business.

However, there is no follow-up mechanism instituted to ensure remediations are implemented by the system owners. The absence of such mechanism will result in having the same vulnerabilities that are left unmanaged. Further, there is no strong system/mechanism in place requiring the system owners to mandatorily implement the remedies provided for weak vulnerabilities in the assessment reports. Additionally, there are no actions or sanctions imposed if the system owners fail to implement those security measures.

Moreover, the RAA-administered survey results also show that 35.5% of government agencies do not update and apply patches to mitigate vulnerabilities.

The RAA was also informed by the BtCIRT in having challenges in vulnerability and patch management and ineffective malware clean-up.

c) Documentation of Lessons Learnt

Likewise, the RAA also noted that after an incident response and recovery, there is no system of documenting lessons learnt.

The aforementioned issues can be attributed to the human resource constraints of the BtCIRT. Consequently, the inadequate capacity and mechanism to handle and respond to cyber incidents would result in inefficient planning, detection, and response to malicious activities in cyberspace. This would ultimately result in prolonged service disruption, financial loss, reputational damage, and costly recovery after the incident.

BtCIRT explained that Vulnerability Assessment (VA) scan is recorded in the ticketing system and followed up with the VA requester if they have carried out required remediation actions. However, if the VA requester is not accessible even after a month, we close the ticket. For incidents such as malware infections, defacements, and ransomware attacks among others we document our analysis as incident reports. For incidents such as viral scams or social media-related incidents, we provide advisories, and for zero-day vulnerabilities which are globally applicable we provide alerts.

While acknowledging the responses, the fact is that there is no proper monitoring mechanism instituted to ensure appropriate security measures are implemented to remedy the security vulnerabilities identified in the GDC.

Chapter 4: Recommendations

The RAA conducted a root cause analysis to identify the root causes to correct the deficiencies and issues reflected under audit findings in Chapter 3. Based on the root cause analysis, the RAA has developed three recommendations to address the issues and guide the management to implement corrective actions. The RAA hopes that the corrective actions would contribute towards ensuring a safe, secure, and resilient cyberspace in the country.

The GovTech Agency may review the relevancy and appropriateness of these recommendations for implementation and also note that there may be better alternatives to address the shortcomings. As such, the recommendations are not intended to restrict the ability of policy and decision-makers in their decision-making but to select better alternatives to address the findings in this report. The recommendations are divided into two categories; Strategic and Operational.

4.1. Strategic

Recommendations of strategic nature would require actions at the policy and strategic levels and may be considered for discussion at the national level.

4.1.1. The GovTech Agency should review and improve the regulatory framework for Cybersecurity

The RAA, while assessing the existence and adequacy of the legal and regulatory framework, noted that one of the main causes for some audit findings is poor enforcement of legal provisions. Weak enforcement exists due to the non-identification of regulators for cybersecurity in most of the critical sectors or lack of clarity on the role of the regulators for cybersecurity.

For this reason, the GovTech Agency should review and improve the regulatory framework. More specifically:

i. There is a need for a national regulatory body for cybersecurity or to expand the role of existing regulators to regulate cybersecurity for an effective regulatory framework.

ii. The regulators need to have adequate personnel with cybersecurity know-how to handle matters related to national cybersecurity.

iii. Moreover, the regulators need to enhance enforcement and compliance mechanisms through various means such as rules and regulations, license contract agreements, monitoring and reporting mechanisms, and accountability mechanisms.

Having an effective regulatory framework would ensure that the security controls are implemented and compliance requirements are met. This would result in driving the national agenda for the protection and regulation of the identified CIIs leading to contributing towards the enhancement of the cybersecurity posture of the country.

4.1.2. The GovTech Agency should strengthen the institutional framework for Cybersecurity

Of several factors, robust cybersecurity is dependent on an effective and well-coordinated institutional framework. Presently, there is a disconnect between the various agencies involved in the cybersecurity system in the country leading to a diffusion of responsibilities. Thus, the

GovTech Agency should take the lead to strengthen the institutional framework for cybersecurity in collaboration with all other agencies involved in contributing towards the safe and secure cyberspace of Bhutan. In particular, the GovTech Agency may start with the following:

i. Establish a coordinating leadership for cybersecurity to provide strategic direction.

ii. Empower the nodal agency for cybersecurity, in terms of institutional and manpower capacity and capability.

iii. Form institutional linkages amongst the policymakers, regulators, and implementors including SoEs and government agencies. Moreover, the institutional linkages can be reinforced through the following.

   a) Identification of focal points in agencies with critical information systems;

   b) Formation of sectoral CIRT for CIIs; and

   c) Strengthening the information-sharing platform and expertise through working groups and/or forums to collaborate on threat monitoring, detection, and response.

With an effective institutional framework, the country would be in a better position to identify, protect, and detect cybersecurity threats to adequately respond to and recover from cybersecurity incidents.

4.2. Operational

Recommendations of operational nature would require direct actions by the specific audited entities.

4.2.1. The GovTech Agency should endorse and implement the draft National Cybersecurity Strategy

The RAA observed that almost all the audit issues could be resolved by implementing the draft NCS. The NCS is one of the main documents that express the vision, high-level objectives, principles and priorities that guide a country in enhancing its cybersecurity.

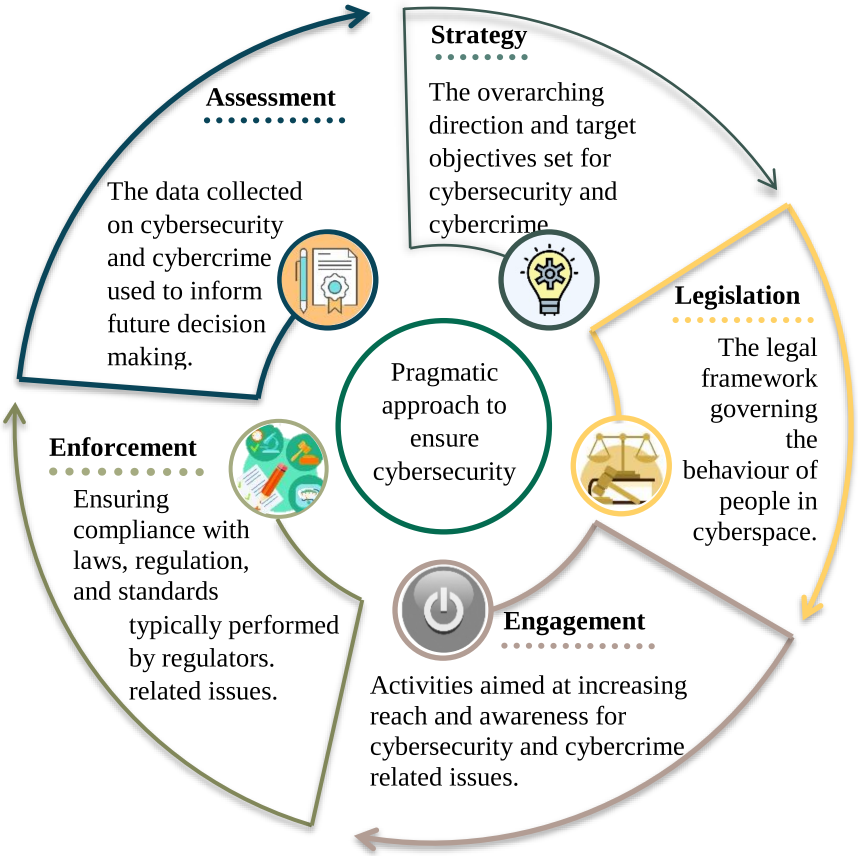
Therefore, the GovTech Agency should endorse and implement the draft NCS to achieve the seven goals identified in the strategy. More importantly, the GovTech should:

i. Review the strategy along with the action/implementation plan to identify appropriate sub-goals and activities, accord required resources and budget, identify lead and responsible agencies, and facilitate coordination.

ii. Institute a monitoring framework with appropriate KPIs, targets and deadlines to track progress, and reporting and accountability mechanisms.

iii. Institute an evaluation Framework with evaluation timing, accountability, and revision of NCS based on the evaluation.

The RAA understands that the BtCIRT has initiated some activities from the strategy but having it endorsed would ensure that appropriate resources are made available to implement such an important strategy in the cybersecurity domain. The endorsement and implementation of the NCS would lead to a pragmatic approach to cybersecurity as shown below.


Strategy
The overarching direction and target objectives set for cybersecurity and cybercrime
Assessment
The data collected on cybersecurity and cybercrime used to inform future decision making.
Legislation
The legal framework governing the behaviour of people in cyberspace.
Pragmatic approach to ensure cybersecurity
Enforcement
Ensuring compliance with laws, regulation, and standards typically performed by regulators. related issues.
Engagement
Activities aimed at increasing reach and awareness for cybersecurity and cybercrime related issues.

4.2.2. The GovTech Agency should expedite the protection of Critical Information Infrastructures (CIIs) in the country

Critical Information Infrastructures (CIIs) are digitised components of essential services provided by critical sectors and the incapacitation or destruction of CIIs would have a debilitating impact on national security, economy, public health, social welfare, or safety. The RAA found that the CIIs have not been identified. Therefore, the GovTech should declare and identify the CIIs to protect the same. In particular, the GovTech should:

i. Develop the identification framework for CIIs.

ii. Identify the CIIs and CIIs owners.

iii. Declare the CIIs.

iv. Inform the CIIs owners on the duties and responsibilities and on the measures to be taken by the CIIs owners including reporting cyber incidents to ensure the cybersecurity of CIIs.

v. Ensure protection through CII regulations including risk assessment of CIIs by CIIs owners.

These actions would ensure adequate protection mechanisms for CIIs in the country.

4.2.3. The GovTech Agency should take the lead to strengthen the legal framework for cybersecurity

An integral component of robust cybersecurity is appropriate legislation which is harmonised with national, regional, and international policies and practices. The RAA noted inadequacies in the legal framework for cybersecurity which would require the review and gap analysis of the existing legislation. Hence, the GovTech Agency should strengthen the legal framework through the following:

i. Review the existing Acts, Rules and Regulations on cybersecurity.

ii. Identify and address legal gaps.

iii. Harmonise the laws.

Strengthening the legal framework for cybersecurity would result in creating a robust legal ecosystem inclusive of cybersecurity and data protection.

4.2.4. The GovTech Agency should strengthen the enforcement mechanism for data privacy and data protection

The RAA observed that weak enforcement mechanisms for data privacy and protection which would expose personally identifiable information (PII) to data breaches, identity theft, and scams.

Therefore, the GovTech Agency should ensure adequate mechanisms for the enforcement of legal provisions and government executive orders for data privacy and data protection to protect against unauthorised disclosure and unauthorised processing of personal data.

Further, the RAA observed that government agencies are using Google Workspace for communication and storing all official information. In order to ensure data protection and security, the GovTech Agency should develop protocols to classify data to ensure that sensitive and confidential information is not uploaded to Google Workspace.

Chapter 5: Conclusion

Recognising the importance of cybersecurity in digital transformation and in securing our cyberspace, the RAA carried out the performance audit of “Preparedness for Cybersecurity”. The audit was conducted to ascertain the Government's efforts towards ensuring safe, secure, and resilient cyberspace in Bhutan. The sub-objectives are to determine the appropriateness of the cybersecurity program/system in the country and to examine whether the CII systems are identified and protected.

During the audit, the RAA noted the inadequacies of the regulatory framework resulting in the non-enforcement of some legal provisions for cybersecurity and a lack of coordinating leadership resulting in the non-implementation of national cybersecurity strategy and a disconnect between the various agencies involved in the cybersecurity system in the country. Moreover, the RAA observed non-identification of critical CIIs in the country exposing the CIIs to potential cyber threats. Additionally, the RAA noted a lack of adequate legal framework and mechanisms to address cybercrime.

Due to cybersecurity being multi-sectoral, the current scenario is characterised by fragmented approaches to ensuring safe, secure, and resilient cyberspace intensified by non-implementation of the national strategy to provide vision and high-level objectives, and a weak regulatory and institutional framework delineating responsibilities and accountability amongst agencies.

The RAA deduces that the cybersecurity program/system is weak and the CIIs are yet to be identified. Thus, the RAA concludes that the Government’s efforts towards ensuring safe, secure, and resilient cyberspace in Bhutan are not adequate and need to prioritise enhancing the country’s cybersecurity posture.

The Government’s role in cybersecurity will only grow as the global demand and dependency on the Internet and Internet-connected devices continue to increase. With increasing cyber threats and risks, the Government must be prepared to protect our computer systems and networks from cyber-attacks. The RAA recommends addressing the shortcomings and implementing corrective actions. To address the range of issues confronting cybersecurity and implement corrective actions, the RAA provided six recommendations.

The RAA hopes that the Government and the GovTech Agency in particular will use this audit report and implement the recommendations to enhance the cybersecurity posture of the country.

Appendix A – MANAGEMENT ACTION PLAN AND ACCOUNTABILITY STATEMENT

Recommendation No.	Audit Recommendation in brief	Action Plans: Action taken or to be taken	Estimated implementation date	Estimated completion date	Direct Accountability			Supervisory Accountability		
					Name & Design	CID & EID No.	Signature	Name & Design	CID & EID No.	Signature
4.1.1	The GovTech Agency should review and improve the regulatory framework for Cybersecurity									
4.1.2	The GovTech Agency should review and improve the regulatory framework for Cybersecurity									
4.2.1	The GovTech Agency should endorse and implement the draft National Cybersecurity Strategy									
4.2.2	The GovTech Agency should expedite the protection of Critical Information Infrastructures (CIIs) in the country									

Recommendation No.	Audit Recommendation in brief	Action Plans: Action taken or to be taken	Estimated implementation date	Estimated completion date	Direct Accountability			Supervisory Accountability		
					Name & Design	CID & EID No.	Signature	Name & Design	CID & EID No.	Signature
4.2.3	The GovTech Agency should take the lead to strengthen the legal framework for cybersecurity									
4.2.4	The GovTech Agency should strengthen the enforcement mechanism for data privacy and data protection									

AIN: TAD-2022-436

www.bhutanaudit.gov.bt