Development of National Technology Framework in-line with Global Cybersecurity Framework

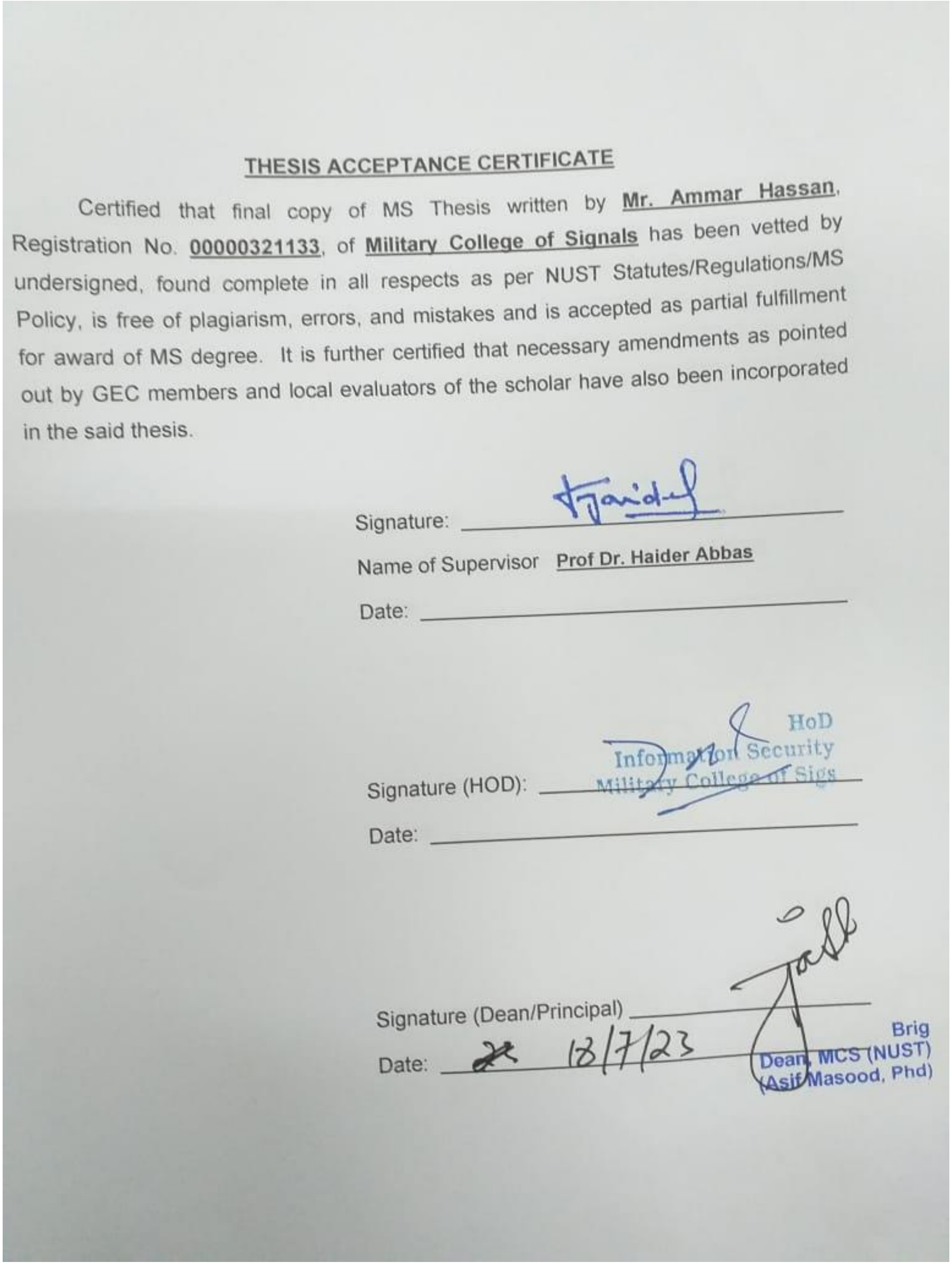
By

Ammar Hassan

00000321133

Submitted to the Faculty of the Department of Information Security Military College of Signals, National University of Sciences and Technology, Islamabad, in partial fulfillment of the requirements for the degree of MS in Information Security

JUNE 2023



THESIS ACCEPTANCE CERTIFICATE

Certified that final copy of MS Thesis written by **Mr. Ammar Hassan**, Registration No. **00000321133**, of **Military College of Signals** has been vetted by undersigned, found complete in all respects as per NUST Statutes/Regulations/MS Policy, is free of plagiarism, errors, and mistakes and is accepted as partial fulfillment for award of MS degree. It is further certified that necessary amendments as pointed out by GEC members and local evaluators of the scholar have also been incorporated in the said thesis.

Signature: ______________________

Name of Supervisor **Prof Dr. Haider Abbas**

Date: ______________________

HoD
Information Security
Military College of Sigs

Signature (HOD): ______________________

Date: ______________________

Signature (Dean/Principal) ______________________

Date: ~~2~~ 13/7/23

Brig
Dean, MCS (NUST)
(Asif Masood, Phd)

DECLARATION

I certify that this research work titled "Development of National Technology Framework in-line with Global Cybersecurity Framework" is my own work. No portion of the work presented in this dissertation has been submitted in support of another award or qualification either at this institution or elsewhere. The material used from other sources has been appropriately acknowledged/referred to.

Ammar Hassan

0000321133

DEDICATION

This thesis is dedicated to my Parents, teachers, and friends for their unconditional love, endless support, and continuous encouragement.

ACKNOWLEDGMENT

All worship and glory be to the All Magnificent and All-Merciful Allah Almighty. I am thankful to all my family, particularly my parents, who have always been my pillar of utmost strength and assistance.

I humbly thank my Thesis supervisor, Dr. Haider Abbas, who supervised my research and mentored me in a very polite yet considerate and helpful manner. As a supervisor, his facilitation and counseling have always been an irreplaceable resource of guidance for me and will continue to be so in the coming years. I am also grateful to my worthy co-supervisor Dr. Faisal Amjad for his constructive comments, which helped me refurbish my skills and bring a refined edge to this research, and to my esteemed committee members for their guidance, support, and suggestions.

I am grateful to the National University of Science and Technology (NUST) and my batchmates for giving me healthy competition and countless memories to cherish forever.

Abstract

The information security threat landscape is changing dramatically, and modern attacks are more sophisticated with highly targeted techniques. The rate at which adversaries change strategies to harm a system's resources is greater than those to defend the organization's system resources, making defense difficult. The National Technology Framework gives a direction to protect the entire nation from cyber threats and risks. This framework analyzes the existing cybersecurity measures and proposes the security framework under International Telecommunication (ITU) guidelines. The proposed framework is based on five pillars: legal, technical, organizational, capacity building, and cooperation measures, and this is also called the global cybersecurity agenda. The NTF aims to define and assign roles and responsibilities to the national stakeholders to protect national cyberspace. The NTF counts on prevailing coordinating structures and legislations to encourage resilience, integration, and synchronization across several areas of responsibility and jurisdictions. Such coordinating structures include the critical infrastructure sector, public-private organizations, law enforcement task forces, government, and governance boards. As a national doctrine, NTF presents a consolidated approach for aligning security tasks across the five domains' legal, technical, organizational, and capacity building and coordination structures. It encourages the mutual understanding of cybersecurity, eventually ensuring secure cyberspace and interoperability, efficient information sharing, and the efficacy of security-related activities nationwide to increase Pakistan's cybersecurity ranking.

Table of Contents

List of Figures x

List of Tables xi

Introduction 1

1.1 Overview 1

1.2 Background 1

1.3 Problem Statement 2

1.4 Objective 2

1.5 Relevance to National Needs 3

1.6 Scope of Study 3

Literature Review 5

2.1 Prevention of Electronic Crime Act, 2016 (PECA) 5

2.2 Personal Data Protection Bill 2020 6

2.3 Electronic Data Protection Act 2005 7

2.4 Cybersecurity Framework for Insurance Sector 2019 8

2.5 Electronic Transaction Ordinance 2002 (ETO) 9

2.6 Protection from SPAM, Unsolicited Fraudulent and Obnoxious Communication Regulations 2009 10

2.7 Critical Telecom Data and Infrastructure Security Regulations (CTDISR), 2020 10

2.8 National Cybersecurity Council Act, 2014 11

2.9 Information Security Auditors Registration Regulation 13

2.10 National Cybersecurity Policy 2021 13

2.11 Other Initiatives by the Government of Pakistan 16

2.11.1 National Center for Cyber Security (NCCS) 16

2.11.2 National Cybersecurity Academy (NCSA) 16

2.11.3 Higher Education Commission (HEC) Initiatives 16

2.11.4 National Initiative for Artificial Intelligence and Security (NIAIS) 17

2.11.5 National Response Center for Cyber Crime (NR3C) FIA 17

2.11.6 Pakistan Information Security Association (PISA) 17

GAP Analysis 18

3.1 Gap Assessment Methodology 18

3.2 Gap Assessment Tool 19

3.3 Gap Analysis Result 42

Research Methodology 43

4.1 NIST Cybersecurity Framework 44

4.2 Cybersecurity in Estonia 46

4.2.1 Legal Measures 47

4.2.2 Technical Measures 48

4.2.3 Organizational Measures 49

4.2.3.1 Cybersecurity Strategy of Estonia 49

4.2.4 Capacity Development 51

4.2.5 Cooperation Measures 52

4.3 Cybersecurity in Australia 53

4.3.1 Legal Measures 53

4.3.2 Technical Measures 54

4.3.3 Organizational Measures 55

4.3.4 Capacity Development 57

4.3.5 Cooperation Measures 58

4.4 Cybersecurity in India 58

4.4.1 Cybersecurity Strategy of India 59

4.4.2 Cybersecurity Profile of Pakistan 60

4.4.3 Cybersecurity Infrastructure Comparison India vs Pakistan Under GCI Requirements 61

National Technology Framework In line with Global Cybersecurity Framework 64

5.1 Legal Measures 66

5.1.1 National Cybersecurity Regulatory Authority (NCRA) 66

5.1.2 Cybersecurity Policies 68

5.1.3 Cybersecurity Strategy 68

5.2 Technical Measures 71

5.2.1 Cyber Emergency Response Team Pakistan (CERT-Pak) 71

5.2.2 Sectoral CERT 72

5.2.3 National Framework for Implementation of Cybersecurity Standards 72

5.2.4 Child Online Protection 74

5.3 Organizational Measures 75

5.3.1 Cybersecurity Planning & Legislative Infrastructure 75

5.3.2 Cybersecurity Operation Center and National CERT 76

5.3.3 Cyber Threat Intelligence 76

5.3.4 National Critical Infrastructure Protection 77

5.3.5 Cybersecurity Cooperation 77

5.3.6 Cybersecurity Audit & Evaluation 77

5.3.7 Information Security Governance, Risk, and Compliance 78

5.3.8 Child Online Protection 78

5.3.9 Cybersecurity Education Training & Awareness 79

5.4 Capacity Development 79

5.5 Cooperation Measures 80

Conclusion and Future Work 81

6.1 Conclusion 81

6.2 Future Work 81

6.3 Action Plan 82

References 83

List of Figures

Figure 3- 1 Gap Analysis 42

Figure 4- 2 Research Methodology 44

Figure 4- 3 NIST Cybersecurity Framework 45

Figure 4- 4 Cybersecurity Profile of Estonia 46

Figure 4- 5 Linkage between CS Strategy and National State Bodies 49

Figure 4- 6 Cybersecurity Profile of Australia 53

Figure 4- 7 Cybersecurity Profile of India 59

Figure 4- 8 Parts of Cybersecurity Strategy India 60

Figure 4- 9 Cybersecurity Profile of Pakistan 61

Figure 5- 1 Parameters of NTF 65

Figure 5- 2 Broader view of NTF 65

Figure 5- 3 Structure of NCRA 67

Figure 5- 4 National Cybersecurity Strategy Lifecycle 70

Figure 5- 5 National Framework for Implementation of Cybersecurity Standards 73

List of Tables

Table 4- 1 Legal Measures of Estonia 48

Table 4- 2 Technical Measures of Estonia 48

Table 4- 3 Organizational Measures of Estonia 51

Table 4- 4 Capacity Development Measures of Estonia 52

Table 4- 5 Cooperative Measures of Estonia 52

Table 4- 6 Legal Measures of Australia 54

Table 4- 7 Technical Measures of Australia 55

Table 4- 8 Organizational Measures of Australia 56

Table 4- 9 Capacity Development Measures of Australia 57

Table 4- 10 Cooperative Measures of Australia 58

Table 4- 11 Cybersecurity Infrastructure Pak vs India 63

Chapter 1

Introduction

1.1 Overview

A cybersecurity frame combines documents defining global best practices for a state to manage potential cybersecurity risks. Such frameworks include but are not limited to policies, procedures, guidelines, strategies, standards, and cybersecurity requirements related to legal, technical, organizational capacity building, and cooperation measures. The primary purpose of this National Technology Framework is to promote and encourage the adoption of best cybersecurity practices under the guidelines of the Global Cybersecurity Index (GCI), a specialized body of the International Telecommunication Union (ITU) Development area. After every two years, ITU GCI publishes the ranking of its 194 member states concerning cybersecurity commitment at the national level. This ranking mainly includes some security measures of the country regarding the five pillars of GCI [49]. This framework is developed after analyzing the top-ranked countries' top cybersecurity practices and frameworks by ITUs like Estonia, Italy, India, the United States of America (NIST), and Australia. The primary goal of this framework is to improve Pakistan's cybersecurity ranking and secure national cyberspace.

1.2 Background

In 2021, Pakistan launched its first-ever national cybersecurity policy, and several other national-level cybersecurity legislations are discussed in the analysis of the national legislation section. But unfortunately, Pakistan does not have a cybersecurity framework, and a framework is required to address the latest cyber threats, risks, and information security governance. If a country doesn't have a national cybersecurity strategy or framework, then that country is not seriously dealing with cybersecurity. That is why Pakistan is in the 79th position among 194 member states in the cybersecurity ranking.

1.3 Problem Statement

In the age of digitization, Pakistan does not yet have a national cybersecurity framework followed by other national-level documentation like national cybersecurity strategy, legal measures for child online protection, national and sectoral CERT, national framework for implementing cybersecurity standards, capacity development and measures related to cooperation at national and international level and much more which are highlighted in the gap analysis section. All these factors punch Pakistan to the bottom in the cybersecurity ranking, according to the GCI Report 2020. Furthermore, Pakistan has a population of 227 million [48]. Eighty-seven percent of the population has access to the internet [47], then we have the industrial 4.0 revolution. If we compare pre and during COVID-19 tenures, a 19 percent increase in data usage is observed. Moreover, we have the initiative of E-Government, the digital Pakistan vision of Prime Minister Pakistan. Then we have safe cities, smart cities, security of critical national infrastructure, cloud computing, and IoT.

COVID-19 and excessive digitization have changed the threat landscape globally. Securing national cyberspace is the biggest challenge, but National Technology Framework (NTF), in-line with Global Cybersecurity Framework, is developed to address the aforementioned issues.

1.4 Objective

The main objectives of this framework or study are the following:

a) The primary aim is to increase the cybersecurity ranking of Pakistan among ITU GCI member states

b) Analyze the already existing cybersecurity infrastructure of Pakistan and find the gaps

c) Analyze the globally best cybersecurity practices and frameworks of top-ranked countries and propose an aligned cybersecurity framework with ITU GCI requirements

d) The outcome is the development of safe and secure cyberspace for national and international stakeholders

1.5 Relevance to National Needs

Pakistan's threat landscape is exponentially increasing daily, and digitization is directly proportional to cyber threats. Most recently, the following are some significant breaches of history:

a) According to the ITU GCI cybersecurity ranking 2020, Pakistan is 79th among 194 member states and in 14th position among Asian Pacific region member states which is not good.

b) The Federal Board of Revenue (FBR) tax collection authority suffered from a cybersecurity breach in 2021 [46].

c) K-Electric, a company that manages electric power generation, distribution, and transmission to the city, was hit by a data breach in 2020 (Ransomware attack) [45].

d) In 2018-19, almost all central banks, Careem, and some hospitals became victims of cyberattacks/data beach [44].

e) According to Edward Snowden, Pakistan is the 2nd most spied over by the NSA [43].

Increased cyber threats and all these situations reveal that critical national information infrastructure is vulnerable, and we must take concrete steps to secure national critical information infrastructure. The National Technology Framework aims to rescue and suit national needs, as discussed above and in the problem statement section. Pakistan has no official approved national cybersecurity framework, strategy, or related legislation. However, this research work proposes a high-level perspective of the framework after gap analysis, and this framework will completely align Pakistan's cybersecurity measures with ITU GCI requirements.

1.6 Scope of Study

This proposed framework can be applied to national cyberspace, expressly but not limited to the public-private sector, where ICT infrastructure is the backbone. Furthermore, the framework applies to all departments but is not limited to those mentioned below:

a) Government sector

b) IT and Telecom Sector

c) Banking Sector

d) Education Sector

e) Health Industry

Chapter 2

Literature Review

A comprehensive analysis of existing national cybersecurity infrastructure concerning the Global Cybersecurity index is provided in this document. Currently, the following national-level legislations are existing in Pakistan to secure national cyberspace, which is in accordance with ITU Global Cybersecurity Framework.

2.1 Prevention of Electronic Crime Act, 2016 (PECA)

With increasing digitization, information, and communication technologies in Pakistan, information security is the biggest challenge. At the same time, the Prevention of Electronic Crime Act (PECA) is the only body to deal with cybercrimes [1]. According to Chapter 1, PECA Law is uniformly applicable to the whole state but is not implemented in the true sense. Chapter II is about offenses and punishments. However, some modern crimes are not defined in this section, like social engineering, Denial of Service to legitimate users, and Malicious ICT Equipment, nor are punishments related to these offenses. Chapter III is about establishing an investigation agency's mandate, working procedure, and powers. Chapter IV is about cooperation with international cybercrime investigation agencies. In Chapter V, the prosecution and trial of offences are described. Computer Emergency Response teams are introduced, which are crucial for an organization to rescue in case of a cyber emergency.

Due to increasing digitization and cybercrime laws, maximum states have tried to fit them within national cybersecurity frameworks. PECA, in comparison with GCI measures then it needs to be revamped [2], so it has the following ambiguities:

a) No Mechanism defined for periodic policy revision

b) Neither availability offenses nor punishment defined

c) There is no specific time frame specified for offense investigation

d) There is no offense no punishment defined against child online protection

e) Lack of practical implementation on the ground

f) Lack of awareness/training about PECA law among stakeholders and Jurisdiction.

In the awake of growing cybercrimes, the Prevention of Electronic Crime Act (PECA) needs to be amended with a solid implementation base, needs to enhance the capacity and power of investigation agencies, enhancement in cybercrime courts, and special training of judicial staff, involvement of intelligence agencies in cybercrime investigation. Government should need to ensure implementation, transparency, and accountability.

2.2 Personal Data Protection Bill 2020

The Personal Data Protection Bill (PDPB) has a broader scope, and data security is part of this bill. The primary purpose of this bill is to have control of the individual on his data, and the second purpose is to set certain processes, procedures, and guidelines for those commercial or governmental organizations who want to use this data for their purpose. It seems that definitions for this bill are derived from General Data Protection Regularity (GDPR), like data subject, data controller, and data processor. Specific mechanisms are defined to show the relationship between all these three, like guidelines on how personal data is to be processed and for what purpose data should be processed; for that purpose data controller and processor has to follow some necessary measures for individual data protection.

In developed countries, special cybersecurity courts are responsible for cybersecurity and data privacy/protection cases. However, here in Pakistan, there are no such courts, so this is the biggest challenge. This act is incompatible with existing IT infrastructure, like all data of Android users first came abroad, and there is no local copy retained for the host country. Several other challenges are mentioned below:

a) No guidelines regarding critical data Classification

b) No public awareness about individual data misuse and protection rights

c) Data localization and Cross border transmission rules not defined

d) Certain baselines are missing, like the role of authority, governance rules

e) No clarity about the data protection of public and strategic organizations

f) No compliance mechanism described for data protection

g) No capacity-building mechanism

h) No private stakeholder consultation on data protection

i) Initially, penalties are un-realistic and too high

Apart from these challenges, the rest of the things are very well defined in this personal data protection bill, which is currently presented as a bill for criticism by different public-private stakeholders; after that, it will become part of Pakistan's national legislation. The country is in real need of such a data protection act because, as we know that digitization is directly proportional to cyber threats, more specifically, data breaches. These digital devices produce bulk data, which is an alarming situation for state-sponsored cybersecurity analysts. The state is going to protect user's data along with five key parameters, which are data collection should be transparent and lawfully, the purpose of data collection should be the same as initially claimed by the company, the amount of data collected should be the same as initially defined in the agreement between user and company. Accurate data should be deleted at the user's demand. Lastly, the company should not be authorized to disclose the personnel or any other information to third parties; instead, they must make some necessary data confidentiality arrangements [3].

2.3 Electronic Data Protection Act 2005

The electronic data protection act applies to all electronic data processing within Pakistan and outside Pakistan. The first chapter is related to definitions of entities dealing with user data. This act does not apply to the personal or corporate data of federal, provincial, or local governments. Chapter Two is related to foreign and local data processing, data subject rights are discussed in chapter three, and chapter four is related to electronic data security, the security against accidental data loss, data confidentiality, unauthorized data access, and rules for data destruction. Chapter Five is about data operators and data disclosure. In chapter six, the powers and functions of the federal government are defined. Offenses and punishments are explained in chapter seven [4], although some ambiguities in this act are mentioned below:

a) There is no specific authority defined for the implementation of this act

b) Definitions in chapter one need to be updated according to the latest technologies

c) Not defined, what is sensitive data

d) No periodic review of this act founded

e) Rights on individuals Data are vaguely defined

f) No acceptable security level of data is described in this act

g) The most crucial data integrity aspect is not founded

The electronic data protection act needs to be reconstructed from the initial stage according to modern data collection, storage, and processing techniques, and baseline security should be enforced through this act across the public-private sector. Concerns of private stakeholders should also be addressed in this act. The cybersecurity audit requirements are partially defined from a global cybersecurity perspective.

2.4 Cybersecurity Framework for Insurance Sector 2019

The Security and Exchange Commission of Pakistan (SECP) was established under the Security and Exchange Commission of Pakistan Act 1997. Its mandate is supervision and regulation of the insurance sector, and information security regulation is part of its mandate.

SECP refers world’s best organizations' standers and practices for the development of cybersecurity frameworks for the insurance sector like the National Institute of Standards and Technology (NIST), Information Systems Audit and Control Association (ISACA), Control Objectives for Information and Related Technologies (COBIT) and Internation Organization for Standardization (ISO) 27000 series. In light of these standardizing entities, an accountable authority like Chief Information Security Officer (CISO) should be responsible for information security governance, risk, and compliance management. The Proposed Cybersecurity framework will cover all necessary controls to achieve compliance with all legislation and regulations nationally and internationally. The cybersecurity framework for the insurance sector covers some questionnaires of GCI under legal measures [5].

There are some flaws in the Cybersecurity Framework, like Information security governance mechanism, Compliance checking, lack of staff training and awareness, no proper reporting structure, and not the existence of a Cyber Emergency Response Team (CERT) at the organizational level and iteratively updating of all security policies, procedures, strategies, guidelines, and SOP.

2.5 Electronic Transaction Ordinance 2002 (ETO)

Electronic Transaction Ordinance (ETO) 2002 is to recognize and facilitate electronic documents, records, information, communication, and electronic transactions to provide for accreditation with electronic certification service providers. According to the first chapter of ETO, an "Electronic certification accreditation council" was established under section 18. This council is responsible for electronic certification for its cryptography services like digital signature, authentication, and integrity of documents. Furthermore, several other definitions of a certificate, cryptography services, electronic document and signature, information and information system, originator, etc. are defined in this chapter. The second chapter is about legal recognition and presumption, like proof of electronic signature, a mechanism for signing an electronic file, and attestation and notarization.

Chapter three concerns communication attributes like electronic file/ message originator, electronic communication's authenticity, receipt acknowledgment, clock synchronization, etc. Chapter Four is about certification service providers, and Chapter Five is about the certification council. In Pakistan, Electronic Certification Accreditation Council is working to regularize the country's certificate authority and electronic certification process. Chapter Eight is about offenses like violating the privacy of information and damage to the information system. Eventually, this ordinance some questionnaire of GCI under legal measure, which is "use of digital signatures in government and applications" [6].

2.6 Protection from SPAM, Unsolicited Fraudulent and Obnoxious Communication Regulations 2009

This act is working under the Pakistan Telecommunication Authority (PTA), which covers the questionnaires of GCI related to curbing spam which means that there is any national level legislation or regulation which restricts spamming activities. Part one is related to definitions of spamming activities, part two is about the procedures to control spamming, and part three and four are related to controlling fraudulent communication and unsolicited calls, respectively. Part five is about the Standard Operating Procedure (SOP) to control obnoxious communication, and part six defines the complaint handling procedure [7]. However, following some deficiencies found in this regulation:

a) Definitions of spamming activities are limited in scope
b) Not all spamming offenses are enlisted/defined
c) Old and vague procedures are described for spam controlling
d) Lack of technological controls founded in mechanism defined for controlling fraudulent communication and unsolicited calls
e) The poor mechanism defined for complaint handling
f) Penalties/punishments are not defined in this regulation
g) Lack of implementation

This policy needs to be revised, which incorporate the latest threats and their remediation according to the latest technologies

2.7 Critical Telecom Data and Infrastructure Security Regulations (CTDISR), 2020

This regulation came into existence under the authority of the Pakistan Telecommunication Authority. The first part of the regulation is about the definitions of technical terms like CERT, Critical telecom data, critical telecom infrastructure, cybersecurity incident, etc. These definitions are of a good scope and right according to modern technicalities. The second part of the legislation is related to license obligations, cybersecurity framework, physical and environmental security, security monitoring, user and event log information, guidelines against malware protection and data protection, cybersecurity incident and infrastructure management, etc. Part three is related to guidelines for periodic improvements in cybersecurity measures to carry out license affiliation with authorities, technical compliance is also discussed in this section [8]. The last part of the legislation is about miscellaneous matters.

From GCI technical measures point of view, this legislation covers several requirements, which include:

a) Identification and protection of nationally critical information infrastructure
b) National/Governmental CERT
c) Sectoral CERT in Pakistan
d) Guidelines for the Protection of critical telecom infrastructure
e) This legislation is good in terms of local legal compliance. Still, nothing is mentioned about compliance with internationally recognized standards which would further strengthen the overall governance of this legislation.

2.8 National Cybersecurity Council Act, 2014

The first-ever national cybersecurity bill was proposed by Senator Mushahid Hussain Sayed in 2014. This bill seeks the establishment of a national cybersecurity council. It defines its functions and powers and provides guidelines to develop policies, procedures, and strategies to formulate a cyber defense against potential cybersecurity threats. In this Act, the initial discussion is about the introduction of the act followed by the definition of terms like CERT, (PASHA) Pakistan Software Houses Association, (PISA) Pakistan Information Security Association, (ISPAK) Internet Service Providers Association of Pakistan, etc. National Cybersecurity Council comprises members from public, private, academic, and specialized groups. Section five is about the powers and functions of the council, where the establishment of national and international cybersecurity strategies is discussed [9].

Advisory groups are defined in section ten; the operational advisory group consists of members from public sectors and autonomous bodies, and the technical advisory group mainly consists of information security professionals, researchers, cryptologists, and professionals from academia. Policy and industry advisory groups comprised members from the public-private sector, stakeholders, auditors, and agencies. Apart from all these groups National Cybersecurity Council Act fulfills many Organizational requirements of GCI, which are the following:

a) National cybersecurity strategy/Policy
b) Protection of nationally critical information infrastructure and telecommunication sector
c) National cybersecurity strategy revised and updated continuously
d) Cybersecurity strategy is open for consultation by all relevant stakeholders, including the operation of critical infrastructure, ISP, and academia.
e) National Cybersecurity Council Act partially addresses the requirements of GCI related to action plans for implementing cybersecurity governance.
f) Special interest groups are defined, which are responsible for protecting national critical information infrastructure.
g) This act partially covers the national cybersecurity capacity development.
h) Instructions regarding cybersecurity audits at the national are defined in this act.
i) Some national-level organizations exist with the mandate of assessment of cybersecurity development at the national level.
j) Public-private and inter-agency partnership for cybersecurity resilience is also defined in this act.

Although this act is defined in a very comprehensive way, there are several limitations of this, act like there are no guidelines for child online protection, no internationally bilateral agreement on cybersecurity, no clear instruction for securing national cyberspace, no national/international collaboration with standardizing agencies for the development of secure cyberspace.

2.9 Information Security Auditors Registration Regulation

Electronic Certification Accreditation Council (ECAC) came into existence under the Electronic Transaction Ordinance 2002. This Regulation is called Information Security Auditors Registration Regulation. It regulates the information security auditors within Pakistan, and auditors must meet the specific academic and professional experience criteria for regularization. The first part of this regulation is about the definitions of auditors, applicants, certificate of registration, etc. Part two is about an authorized auditor's qualification and professional experience. The third part concerns the Registration process for auditors, the validity and effect of registration, the expiry of auditor registration which is five years, and renewal of the auditor’s registration; suspension and revocation of auditor registration are also discussed in part four [10].

From the GCI point of view, this regulation fulfills the requirement of audit at the national level and depicts the national level infrastructure of information security auditors. Despite all these things, there are several deficiencies in this regulation; there is no policy revision tenure defined, the education of auditors needs to be specific rather than generic, and there should need to introduce some internationally recognized auditor's certification to improve the audit quality at the national level, ECAC should ensure the implementation of this regulation across the country.

2.10 National Cybersecurity Policy 2021

Pakistan’s first National cybersecurity policy – 2021, was developed by the Ministry of Information Technology and Telecommunication (MoIT). This policy conforms with the national cybersecurity vision, and the objective is to have a safe and secure cyber ecosystem that ensures confidentiality, integrity, availability, and accountability for information exchange between all stakeholders. There are three challenges, fourteen fundamental policy objectives, and seventeen policy deliverables. According to the policy, the main challenge is ownership of the national information asset; the second challenge is vague enforcement/implementation of existing national cybersecurity legislations; one reason for the same is the non-existence of a national cybersecurity framework. The third challenge is poor cybersecurity structure and processes for governance and several other factors like poor quality of human resources, the gap between demand and supply of skilled cybersecurity professionals, and lack of data governance whereby national data is managed, controlled, and processed out of the jurisdiction of the country, dependencies on external resources like hardware and software, the lack of coordination at National and Internation level between response teams of public-private sectors.

Objectives of the national cybersecurity framework address fundamental issues like better information security governance and institutional framework, security of the national critical information infrastructure, implementation of a framework for information assurance, audit, and compliance, a national international and public-private partnership for information security-related matters, capacity development of professionals, research and development mechanisms are included in the objective.

Section Three is related to policy deliverables, and the first deliverable is about cybersecurity governance for which a Cyber Governance Policy Committee (CGPC) has been constituted to deal with national-level cybersecurity issues and to make sure the implementation of cybersecurity policy and act; the second task of CGPC is to make better institutional cybersecurity infrastructure at the national, sectoral and organizational level. The second deliverable emphasizes active defense for internet service providers and the telecom sector, protection against malware across the domain, blocking of malicious web sources, preventing email phishing and spoofing on public networks, and adopting global security best practices through internet governance as part of this deliverable. The third deliverable is about protecting internet-based services; it emphasizes online protection, data privacy, and securing national domains beyond baseline security. The fourth deliverable is related to securing national critical information infrastructure, including telecom, energy, finance, water, and healthcare. To achieve this critical objective, stakeholders are advised to adopt and promote the culture of accountability and information security self-governance in the public-private sector, develop and adopt the world’s best standards and practices for securing national critical information infrastructure and management of cybersecurity risk along with the appointment of the head of the department or Chief Information Security Officer (CISO) at the organizational level. According to the fifth deliverable, there should be an authentication and data protection framework, a vulnerability and patch management system for national critical infrastructure, and a dedicated budget for cybersecurity assurance and risk management. The sixth deliverable is about attaining cybersecurity assurance by adopting security by design in ICT products and services, upgradation of national-level cybersecurity forensic setups, cybersecurity audits, and compliance at public-private organizations. It also instructed to comply with best cybersecurity practices and standards like ISO/IEC 27001 and PCI DSS. The seventh and eighth deliverables are related to public-private partnership and cybersecurity research and development, respectively. All stakeholders are instructed to develop a framework for share/exchange of information about their cyber activities and actions; Ninth deliverable is about capacity building with the help of the establishment of centers of excellence for human resource training and development, the establishment of special courts related to proceedings of cybersecurity matters and increase in cybersecurity research and development budget is part of this deliverable. The tenth deliverable is about the awareness of the national culture of cybersecurity with the help of the national education curriculum at the middle and secondary levels. Other policy deliverables include global cooperation and collaboration through designated ministries, cyber response mechanism, implementation of existing national cybersecurity regulation, establishing of trust in digital transactions, improving Pakistan's ICT ranking, and last one is risk management and risk-based approach for all sectors [11].

Besides this good initiative, there are some deficiencies and recommendations for improvements in national cybersecurity policy:

a) To whom does CGPC report not defined in this national cybersecurity policy?

b) What powers and authorities are given to CGPC is not clear.

c) Who are the members of the CGPC policy committee are not yet defined.

d) No research and development governing body is defined to make sure world-class modern research and development.

e) Cybersecurity awareness programs should not be restricted to government systems but should be equally applicable to private systems.

f) No guidelines for child online protection

2.11 Other Initiatives by the Government of Pakistan

The following are some other initiatives taken by the Pakistani Government for cybersecurity:

2.11.1 National Center for Cyber Security (NCCS)

National Center for Cybersecurity is a joint project of the Higher Education Commission (HEC) and the Planning Commission of Pakistan, founded in June 2018. This center comprises eleven Research and Development (R&D) Labs across different country universities. The Center is a bridge between academic research and industrial research. NCCS is doing research with the mandate of developing secure systems, crime investigation, information security system design and evaluation and auditing, critical infrastructure security, IoT security, blockchain security, and other secure system development [12].

2.11.2 National Cybersecurity Academy (NCSA)

On November 2021, Pakistan introduced its first-ever National Cyber Security Academy (NCSA) with a joint venture of the Pakistan Air Force, Air University, and Higher Education Commission inaugurated by President Arif Alvi. The primary purpose of this academy is to produce cybersecurity experts and enhance the skills of existing professionals up to the level to secure national cyberspace and critical infrastructure [13].

2.11.3 Higher Education Commission (HEC) Initiatives

The Higher Education Commission of Pakistan introduced master's and Doctoral degrees in Cybersecurity; during the inauguration ceremony of the NCSA, the Director of HEC announced that HEC is going to make Cybersecurity a compulsory subject for all degrees (BS, MS, Ph.D.) applicable to all universities [14].

2.11.4 National Initiative for Artificial Intelligence and Security (NIAIS)

The demand for the technical workforce is increased with new technological innovations, the Industrial 4.0 Revolution, Safe, and Smart Cities. The National Initiative for Artificial Intelligence and Security (NIAIS) [15] and Presidential Initiative for Artificial Intelligence & Computing (PIAIC) [16] are national-level initiatives of the Government of Pakistan to overcome the technical workforce shortage and to enhance the capacity development in the field of AI and Cybersecurity.

2.11.5 National Response Center for Cyber Crime (NR3C) FIA

Federal Investigation Agency (FIA), established under the 1974 Act with the mandate of Investigation of all crimes, Cyber Crime Wing (CCW) and Nation Response Center for Cyber Crime are sections of FIA which deal explicitly with cybercrimes and investigation of cybercrimes under Prevention of Electronic Crime Act 2016, NR3C is also acting as national CERT with 1991 cyber rescue helpline to help in cyber emergency [17].

2.11.6 Pakistan Information Security Association (PISA)

Pakistan Information Security Association is an Internation organization for cybersecurity professionals and panel discussions about the cybersecurity threats landscape, potential risks, and information exchange with other countries about the latest technological trends. The thematic area of work is to initiate information security awareness campaigns, enhance skills and share knowledge [18].

Chapter 3

GAP Analysis

3.1 Gap Assessment Methodology

Gap Assessment is a systematic technique for identifying/finding gaps between the existing state of cybersecurity infrastructure and desired state. The main goal of gap assessment is to understand the flaws for improvement and plan to bridge those gaps. The adopted gap assessment strategy is under the guidelines of ITU GCI. The following steps are being followed to design, develop, and conduct a gap assessment of the National Cybersecurity Infrastructure of Pakistan:

a) Information gathering about the ITU GCI measures for its member states

b) Finding out the objective of each ITU GCI's measure

c) Finding out the weightage of each cybersecurity measures for its member states

d) Analysis of the cybersecurity infrastructure of Pakistan concerning legal, technical, organizational, capacity development, and cooperation measures

e) Setting the status of each cybersecurity measures against every ITU GCI requirement in the form of yes or no

f) Then we referred the policy evidence to each corresponding cybersecurity measure of ITU GCI

By comparing all these points, we have evaluated the gaps between ITU GCI requirements and the current cybersecurity measures of Pakistan. The gap assessment results will help us point out the actual problems and their solution to fill out these gaps.

3.2 Gap Assessment Tool

Section	Cyber Security Measure/Parameter	ITU - GCI Objective (Details)	Average of Weightage Recs	Status	Policy Documents/URL	Remarks
L	**Legal Measures**					
L.1	**Cybercrime substantive law**	**Substantive law refers to all categories of public and private law, including the law of contracts, real property, torts, wills, and criminal law that essentially creates, defines, and regulates rights.**	6.22	Yes	Prevention of electronic crimes Act, 2016	
L.1.1	Do you have substantive law on illegal online behavior?		4.11	Yes	Prevention of electronic crimes Act, 2016	
L.1.1.1	Do you have substantive laws on illegal access on devices, computer systems and data?	Access - the ability and means to communicate with or otherwise interact with a system, to use system resources to handle information, to gain knowledge of the information the system contains, or to control system components and functions (NICCS); Computer system or system - any device or a group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of data (COE - Convention on Cybercrime); Computer data - any representation of facts, information or concepts in a form suitable for processing in a computer system, including a program suitable to cause a computer system to perform a function (COE - Convention on Cybercrime);	2.02	Yes	Prevention of electronic crimes Act, 2016	

Section	Cyber Security Measure/Parameter	ITU - GCI Objective (Details)	Average of Weightage Recs	Status	Policy Documents/URL	Remarks
L.1.1.2	Do you have substantive law on illegal interferences (through data input, alteration, and suppression) on devices, data, and computer systems?	Computer system interference - both intentional and unauthorized serious hindering of the functioning of a computer system. It may include inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data. Data interference - either intentional and unauthorized damaging, deletion, deterioration, alteration or suppression of computer data.	2.56	Yes	Prevention of electronic crimes Act, 2016	
L.1.1.3	Do you have substantive laws on the illegal interception of devices, computer systems, and data?	Illegal interception - both intentional and unauthorized, non-public transmission of computer data to, from or within a computer or another electronic system, made by technical means.	2.39	Yes	Prevention of electronic crimes Act, 2016	
L.1.1.4	Do you have substantive laws on online identity and data theft?	Online identity theft- stealing personal information such as names, addresses, date of birth, contact information or bank account. Can occur as a result of phishing, hacking online accounts, retrieving information from social media or illegal access to databases.	3.03	Yes	Prevention of electronic crimes Act, 2016	
L.1.2	**Do you have dispositions on computer-related forgery (piracy/copyright infringements)?**	**Unauthorized input, alteration, or deletion of computer data resulting to inauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic, to perpetuate a fraudulent or dishonest design.**	3.53	Yes	Prevention of electronic crimes Act, 2016	
L.1.3	**Do you have substantive laws on online safety?**	**Online Safety - refers to maximizing Internet safety-related to various security risks on private and personal or property associated information, as well as enhancing users' self-protection from cybercrimes.**	2.36	No		

Section	Cyber Security Measure/Parameter	ITU - GCI Objective (Details)	Average of Weightage Recs	Status	Policy Documents/URL	Remarks
L.1.3.1	Do you have dispositions/legal measures on offences related to racist and xenophobic online materials?	Measures to prevent different forms of online hate speech and other forms of intolerances because of race, color, religion, descent or national or ethnic origin, sexual orientation or gender identity, disability, social status or other characteristics.	2.99	Yes	Prevention of electronic crimes Act, 2016	
L.1.3.2	Do you have dispositions/legal measures on online harassment and abuse against personal dignity/integrity?	Cyber harassment or bullying - messages sent by email, direct messaging, or derogatory websites aimed to bully or otherwise harass an individual or a group of individuals via personalized attacks.	3.47	Yes	Prevention of electronic crimes Act, 2016	
L.1.3.3	Do you have dispositions/legal measures related to Child Online Protection?	Laws which makes it clear that any and every crime that can be committed against a child in the real world can also be committed on the internet or any other electronic network. It is necessary to develop new laws or adopt existing ones to outlaw certain types of behavior which can only take place on the internet, for example the remote enticement of children to perform or watch sexual acts or grooming children to meet in the real world for a sexual purpose (ITU Guidelines for policy makes on Child Online Protection).	3.54	No		
L.2	**Is there any cybersecurity regulation related to…**	**Regulation is rule based and meant to carry out a specific piece of legislation. Regulations are enforced usually by a regulatory agency formed or mandated to carry out the purpose or provisions of a legislation. Cybersecurity regulation designates the principles, to be abided by various stakeholders, emanating from and being part of the implementation of**	3.78	Partial	**Partially Existing**	

Section	Cyber Security Measure/Parameter	ITU - GCI Objective (Details)	Average of Weightage Recs	Status	Policy Documents/URL	Remarks
		laws dealing with data protection, breach notification, cybersecurity certification/standardization requirements, implementation of cybersecurity measures, cybersecurity audit requirements, privacy protection, child online protection, digital signatures and e-transactions, and the liability of Internet service providers.				
L.2.1	Personal data/privacy protection?	Regulations about protection personal data from unauthorized access, alteration, destruction, or use. Internet privacy is the privacy and security level of personal data published via the Internet. It is a broad term that refers to a variety of factors, techniques and technologies used to protect sensitive and private data, communications, and preferences; An example of such legislation may be in the Data Protection Act.	2.7	Yes	Prevention of electronic crimes Act, 2016 Personal Data Protection Bill 2020	
L.2.2	Data breach/incident notification?	Breach notification laws or regulations are ones that require an entity that has been subject to a breach to notify the authorities, their customers and other parties about the breach, and take other steps to remediate injuries caused by the breach. These laws are enacted in response to an escalating number of breaches of consumer databases containing personally identifiable information;	2.05	Yes	http://complaint.fia.gov.pk/	
L.2.3	Cybersecurity audit requirements?	A security audit means a systematic and periodic evaluation of the information system's security. Typical audit may include assessment of the security of the system's physical	1.41	Partial	Electronic Data Protection Act 2005 National Cyber Security Policy - 2021	Defined in National Cybersecurity Policy,

Section	Cyber Security Measure/Parameter	ITU - GCI Objective (Details)	Average of Weightage Recs	Status	Policy Documents/URL	Remarks
		configuration and environment, software, information handling processes, and user practices.		🟨		but there are no guidelines about the tenure of audit in any legislation.
L.2.4	Implementation of standards?	Existence of a government-approved (or endorsed) framework (or frameworks) for the implementation of internationally recognized cybersecurity standards within the public sector (government agencies) and within the critical infrastructure (even if operated by the private sector). These standards include, but are not limited to those developed by the following agencies: ISO, ITU, IETF, IEEE, ATIS, OASIS, 3GPP, 3GPP2, IAB, ISOC, ISG, ISI, ETSI, ISF, RFC, ISA, IEC, NERC, NIST, FIPS, PCI DSS, etc.;	0.82	Yes	Cybersecurity Framework for Insurance Sector 2019 SEC Directive (Draft)-08012019 National Cyber Security Policy - 2021	
L.2.5	Use of digital signatures in government services and applications (e-govt)?	A digital signature is a mathematical technique used to validate the authenticity and integrity of a message, software, or digital document. An electronic transaction is the sale or purchase of goods or services, whether between businesses, households, individuals, governments, and other public or private organizations, conducted over computer-mediated networks; examples of such legislative documents include the Electronic Commerce Act, Law on Electronic Signatures, E-Transaction Law, and other which	0.79	Yes	Electronic Transaction Ordinance (ETO) 2002 National Cyber Security Policy - 2021	

Section	Cyber Security Measure/Parameter	ITU - GCI Objective (Details)	Average of Weightage Recs	Status	Policy Documents/URL	Remarks
		may include regulations on the establishment of a controller of certificate authorities..				
L.2.6	Curbing of spam?	Information on any laws or regulations restricting SPAMMING activities.	0.67	Yes	Protection from SPAM, Unsolicited fraudulent and obnoxious communication Regulations 2009	
L.2.7	Identifying and protecting the national critical information infrastructures?	Critical infrastructure constitutes basic systems crucial for safety, security, economic security, and public health of a nation. Those systems may include, but are not limited to defense systems, banking and finance, telecommunications, energy, and other. Attach any links or documents that define critical infrastructures or documents/news that confirms definitions of those.	1.55	Yes	Critical Telecom Data and Infrastructure Security Regulations, 2020 National Cyber Security Policy - 2021	
T	**Technical Measures**					
T.1	**National/Government CIRT/CSIRT/CERT.**	**CIRT-CSIRT-CERT: computer incident response teams, staffed concrete organizational entities that are assigned the responsibility for coordinating and supporting the response to computer security events or incidents on national or government level.**	3.04	Partial	**Partially Existing**	**National CERT etc., defined in law but not existing on the ground**

Section	Cyber Security Measure/Parameter	ITU - GCI Objective (Details)	Average of Weightage Recs	Status	Policy Documents/URL	Remarks
T.1.1	Is there a National/Government CIRT/CSIRT/CERT?	Supported by a government's decision or is part of governmental or national structures.	2.41	Yes	Critical Telecom Data and Infrastructure Security Regulations, 2020, Prevention of electronic crimes Act, 2016 National Cyber Security Policy - 2021	Defined in several legislations but on the ground not existing
T.1.2	**Does your National or Government CIRT/CSIRT/CERT…**		2.31	No		
T.1.2.1	Develop and execute cybersecurity awareness activities?	Efforts to promote widespread publicity campaigns to reach the nation about safe cyber-behavior online.	2.63	Yes	https://www.pisa.org.pk/# , http://www.nr3c.gov.pk/cscouts.html national Cyber Security Policy - 2021	
T.1.2.2	Conduct regular cyber security exercises such as Cyber Drills?	A planned event during which an organization simulates a cyber disruption to develop or test capabilities such as preventing, detecting, mitigating, responding to, or recovering from the disruption. Are the exercises organized periodically or repeatedly?	2.61	No		
T.1.2.3	Provide publicly available Advisories?	CIRT Advisories: the sharing of information with the general public on emerging cyberthreats and the recommended actions to take.	2.44	Yes	http://www.nr3c.gov.pk/ctips.html	
T.1.2.4	Contribute to the issues of Child Online Protection?	The CIRT/CSIRT/CERT provides support such as awareness creation campaigns, reporting of incidents related to children, providing educational materials on Child Online Protection and others.	2.31	No		

Section	Cyber Security Measure/Parameter	ITU - GCI Objective (Details)	Average of Weightage Recs	Status	Policy Documents/URL	Remarks
T.1.3	**Is the above mentioned CIRTs (CSIRT or CERT) affiliated with FIRST?**	**A Full Member or Liaison Member of the Forum of Incident Response and Security Teams. www.first.org**	1.96	No		
T.1.4	**Is the above CIRT/s (CSIRT or CERT) affiliated with a regional CERT?**	**A formal or informal relation with any other CERT within, or outside the country, as a part of any regional CERT group. Examples of regional CERTS include APCERT, AFRICACERT, EGC, OIC, and OAS.**	1.8	No		
T.1.5	**Was the maturity level of above CIRT, CSIRT or CERT services certified by the TI certification scheme under TF-CSIRT –SIM3?**	**SIM3 is a basis for CIRT certification.**	1.51	No		
T.2	**Sectoral CIRT/CSIRT/CERT (ex: financial academia etc...)**	**A sectoral CIRT/CSIRT/CERT is an entity that responds to computer security or cybersecurity incidents which affect a specific sector. Sectoral CERTs are usually established for critical sectors such as healthcare, public utilities, academia, emergency services and the financial sector. The sectoral CERT provides its services to constituents from a single sector only.**	2.44	Partial	**Partially Existing**	Partial Sectoral CERT exists
T.2.1	Are there sectoral CIRTs/CSIRTs/CERTs in your country?		5.09	Partial	Critical Telecom Data and Infrastructure Security Regulations, 2020 National Cyber Security Policy - 2021	Only financial sectors have CERT, Not founded for Health, Academia, Public Sector

Section	Cyber Security Measure/Parameter	ITU - GCI Objective (Details)	Average of Weightage Recs	Status	Policy Documents/URL	Remarks
T.2.2	**Does your sectoral CIRT/s, CSIRT/s, CERT/s:**		4.91	No		
T.2.2.1	Develop and execute cybersecurity awareness activities for a sector?		3.4	No		
T.2.2.2	Actively participate in national Cyber Drills?		3.38	No		
T.2.2.3	Share sectoral related incidents within its constituency?	sharing of information on emerging cyberthreats and the recommended actions to take.	3.22	No		
T.3	**National framework for implementation of cybersecurity standards**	**Adopted a national framework (or frameworks) for the implementation of internationally recognized cybersecurity standards within the public sector (government agencies) and within the critical infrastructure (even if operated by the private sector). These standards include, but are not limited to, those developed by the following agencies: ISO, ITU, IETF, IEEE, ATIS, OASIS, 3GPP, 3GPP2, IAB, ISOC, ISG, ISI, ETSI, ISF, RFC, ISA, IEC, NERC, NIST, FIPS, PCI DSS, etc.**	2.46	No	**Not Existing**	
T.3.1	Is there a framework for implementation/adoption of cybersecurity standards?		5.15	Yes	National Cyber Security Policy - 2021	
T.3.2	Does the framework include international or other related standards?	ITU-T, ISO/IEC, NIST, ANSI/ISA and others.	4.85	Yes	National Cyber Security Policy - 201	

Section	Cyber Security Measure/Parameter	ITU - GCI Objective (Details)	Average of Weightage Recs	Status	Policy Documents/URL	Remarks
T.4	**Child Online Protection**	**This indicator measures the existence of a national agency dedicated to Child Online Protection, the availability of a national telephone number to report issues associated with children online, any technical mechanisms and capabilities deployed to help protect children online, and any activity by government or non-government institutions to provide knowledge and support to stakeholders on how to protect children online telephone number, email address, web forms and other, where the interested parties can report incidents or concerns related to Child Online Protection (COP).**	2.06	No	**Not Existing**	
T.4.1	Are there any reporting mechanisms and capabilities deployed to help protect children online?	Such as hotlines, helplines etc.		No		
O	**Organizational Measures**					
O.1	**National Cybersecurity Strategy**	**The development of policy to promote cybersecurity as one of national top priorities. A national cybersecurity strategy should define the maintaining of resilient and reliable national critical information infrastructures including the security and the safety of citizens; protect the material and intellectual assets of citizens, organizations and the nation; respond, prevent cyber-attacks against critical**	4.76	Yes	National cybersecurity council act	Sections 5, (b), and (c) instruct about establishing National and Internation Cybersecurity Strategy, but on the

Section	Cyber Security Measure/Parameter	ITU - GCI Objective (Details)	Average of Weightage Recs	Status	Policy Documents/URL	Remarks
		infrastructures; and minimize damage and recovery time from cyber-attacks.				ground, both do not exist until now.
O.1.1	**Does your country have a national cybersecurity strategy/policy?**		4.53	Yes	National cybersecurity council act National Cyber Security Policy - 2021	
O.1.1.1	Does it address the protection of national critical information infrastructures, including in the telecommunication sector?	Any physical or virtual information system that controls, processes, transmits, receives or stores electronic information in any from including data, voice, or video that is vital to the functioning of a critical infrastructure; so vital that the incapacity or destruction of such systems would have a debilitating impact on national security, national economic security, or national public health and safety.	2.49	Yes	National cybersecurity council act , Critical Telecom Data and Infrastructure Security Regulations, 2020 national Cyber Security Policy - 2021	The definition of critical infrastructure is not comprehensive, only limited to the public and telecom sectors.
O.1.1.2	Does it include reference to the national cybersecurity resilience?	A national cybersecurity resiliency plan ensures that the country has the ability to resist, absorb, accommodate to and recover from the effects of any hazard (including natural or human-made) in a timely and efficient manner, including through the preservation and restoration of its essential services and functions with reliance on external service.	2.86	Partial	Guidelines on cybersecurity framework for insurers 2020 (sec)	No Policy exists at the national level, although some organizations have resilience policies; **recommendation:** (CERT team can be responsible for this)

Section	Cyber Security Measure/Parameter	ITU - GCI Objective (Details)	Average of Weightage Recs	Status	Policy Documents/URL	Remarks
O.1.1.3	Is the national cybersecurity strategy revised and updated on a continuous basis?	The life cycle management of the strategy is defined, the strategy is updated according to national, technological, social, economic and political developments that may affect national cybersecurity situation.	2.41	Yes	National cybersecurity council act National Cyber Security Policy - 2021	
O.1.1.4	Is the cybersecurity strategy open to any form of consultation with national experts in cybersecurity?	The strategy is open for consultation by all relevant stakeholders, including operators of critical infrastructures, ISPs, academia and others.	2.23	Partial	National cybersecurity council act National Cyber Security Policy - 2021	
O.1.2	**Is there a defined action plan/roadmap for the implementation of cybersecurity governance?**	**A strategic plan that defines the national cybersecurity outcomes including steps and milestones needed to implement it.**	3.33	Partial	National cybersecurity council act National Cyber Security Policy - 2021	Defined in Section 5,b,c but not right according to CGI Requirements.
O.1.3	**Is there a national strategy for Child Online Protection?**		2.14	No		
O.2	**Responsible Agency**	**A responsible agency for implementing the national cybersecurity strategy/policy can include permanent committees, official working groups, advisory councils, or cross-disciplinary centers. Such a body may also be directly responsible for the national CIRT. The responsible agency may exist within the government and may have the authority to compel other agencies and national bodies to implement policies and adopt standards.**	3.09	Partial	National cybersecurity council act National Cyber Security Policy - 2021	Things are defined in this section, but there are no clear directives about the responsible agency.

Section	Cyber Security Measure/Parameter	ITU - GCI Objective (Details)	Average of Weightage Recs	Status	Policy Documents/URL	Remarks
O.2.1	**Is there an agency responsible for cybersecurity coordination at a national level?**		2.73	Partial	National cybersecurity council act National Cyber Security Policy - 2021	not existing on the ground
O.2.1.1	Does this agency oversee National Critical Information Infrastructure Protection?		2.89	Yes	National cybersecurity council act National Cyber Security Policy - 2021	
O.2.2	**Is there a national agency overseeing national cybersecurity capacity development?**		2.34	Yes	National cybersecurity council act National Cyber Security Policy - 2021	
O.2.3	**Is there any agency overseeing the child online protection initiatives at the national level?**	**Existence of a national agency dedicated to oversee and promote Child Online Protection.**	2.04	No		
0.3	**Cybersecurity metrics**	**Existence of any officially recognized national or sector-specific benchmarking exercises or referential used to measure cybersecurity development, risk-assessment strategies, cybersecurity audits, and other tools and activities for a rating or evaluating resulting performance for future improvements. For example, based on ISO/IEC 27004, which is concerned with measurements relating to information security management.**	2.15	Partial	**Partially Existing**	

Section	Cyber Security Measure/Parameter	ITU - GCI Objective (Details)	Average of Weightage Recs	Status	Policy Documents/URL	Remarks
0.3.1	Are there any cybersecurity audits performed at a national level?	A security audit is a systematic evaluation of the security of an information system by measuring how well conforms to a set of established criteria. A thorough audit typically assesses the security of the system's physical configuration and environment, software, information handling processes, and user practices. Privately managed critical infrastructures may be requested by the regulatory bodies to perform security posture assessments periodically and report on findings.	3.4	Yes	National cybersecurity council act , Information Security Auditors Registration Regulations national Cyber Security Policy - 2021	
0.3.2	Are there metrics for assessing cyberspace associated risks at a national level?	It is a process comprising risk identification, risk analysis and risk evaluation.	3.16	Yes	National Cyber Security Policy - 2021	
0.3.3	Are there measures for assessing the level of cybersecurity development at a national level?	It is an approach to measure the development level of cybersecurity in a nation state.	3.44	Yes	National cybersecurity council act	
C	Capacity Development					
C.1	Public cybersecurity awareness campaigns	Public awareness includes efforts to promote campaigns to reach as many citizens as possible as well as making use of NGOs, institutions, organizations, ISPs, libraries, local trade organizations, community centers,	2.07	Partial	Partially Existing	

Section	Cyber Security Measure/Parameter	ITU - GCI Objective (Details)	Average of Weightage Recs	Status	Policy Documents/URL	Remarks
		community colleges and adult education programmes, schools and parent-teacher organizations to get the message across about safe cyber-behavior online. This includes actions such as setting up portals and websites to promote awareness, disseminating support materials and other relevant activities.				
C.1.1	Are there public awareness campaigns targeting specific sector such as SMEs, private sector companies, and government agencies?		2.27	Yes	https://www.niais.org/ https://www.pisa.org.pk/# http://www.nr3c.gov.pk/cscouts.html National Cyber Security Policy - 2021	
C.1.2	Are there public awareness campaigns targeting civil society?	NGOs, community-based organizations.	1.79	No	National Cyber Security Policy - 2021	
C.1.3	Are there public awareness campaigns targeting citizens?		1.87	Ye Partial s	http://www.nr3c.gov.pk/cscouts.html National Cyber Security Policy - 2021	
C.1.4	Are there public awareness campaigns targeting the elderly?		1.07	Partial	https://www.niais.org/	
C.1.5	Are there public awareness campaigns targeting persons with special needs?		1.25	Partial	https://www.pisa.org.pk/#	
C.1.6	Are there public awareness campaigns involving parents, educators and children (COP)?		1.75	Partial	http://www.nr3c.gov.pk/cscouts.html	

Section	Cyber Security Measure/Parameter	ITU - GCI Objective (Details)	Average of Weightage Recs	Status	Policy Documents/URL	Remarks
C.2	Training for Cybersecurity professionals	The existence of sector-specific professional training programs for raising awareness for the general public (i.e., national cybersecurity awareness day, week, or month), promoting cybersecurity education for the workforce of different profiles (technical, social sciences, etc.) and promoting certification of professionals in either the public or the private sector. It also includes cybersecurity training for law enforcement officers, judicial and other legal actors designate professional and technical training that can be recurring for police officers, enforcement agents, judges, solicitors, barristers, attorneys, lawyers, paralegals and other persons of the legal and law enforcement profession. This indicator also includes the existence of a government-approved (or endorsed) framework (or frameworks) for the certification and accreditation of professionals by internationally recognized cybersecurity standards. These certifications, accreditations, and standards include, but are not limited to, the following: Cloud Security knowledge (Cloud Security Alliance), CISSP, SSCP, CSSLP CBK, Cybersecurity Forensic Analyst (ISC^2), and other.	1.41	Partial	Partially Existing	
C.2.1	Does your government develop/support	Promoting cybersecurity courses in the workforce (technical, social sciences, etc. and promoting certifications for professionals in either the public or the private sector.	3.66	Yes	https://www.niais.org/cyber-security National Cyber Security Policy - 2021	

Section	Cyber Security Measure/Parameter	ITU - GCI Objective (Details)	Average of Weightage Recs	Status	Policy Documents/URL	Remarks
	professional training courses in cybersecurity?					
C.2.2	**Is there an accreditation program for cybersecurity professionals in your country?**	**Ex: Institutes accrediting cybersecurity professionals, or any other related mechanisms.**	3.21	Partial	https://pseb.org.pk/images/6_List_of_selected_training_firms1.pdf National Cyber Security Policy - 2021	PSEB + MoIT Started a certification program for IT/Cybersecurity professionals nationwide, but due to lack of funds lingers on
C.2.3	**Are there a national sector-specific educational programmes/trainings for professionals on cybersecurity courses?**		3.13	Yes	National Cyber Security Policy - 2021	HEC launches Cybersecurity programs for BS, MS, and PhD
C.2.3.1	For law enforcement (police officers and enforcement agents)?	Cybersecurity formal process for educating legal actors (police officers and enforcement agents) about computer security	2.45	No		Need to establish Cybersecurity courts for better governance and

Section	Cyber Security Measure/Parameter	ITU - GCI Objective (Details)	Average of Weightage Recs	Status	Policy Documents/URL	Remarks
						accountability
C.2.3.2	For judicial and other legal actors (judges, solicitors, barristers, attorneys, lawyers, paralegals etc.)?	Cybersecurity training or technical training that can be recurring for police officers, enforcement agents, judges, solicitors, barristers, attorneys, lawyers, paralegals and other persons of the legal and law enforcement profession.	2.3	No		
C.2.3.3	For SMEs/private companies?	Good practices trainings / capacity development on cybersecurity to guard their businesses, etc. by proper use of online services.	2.66	No		
C.2.3.4	For other public sector/government officials?		2.59	No		
C.3	**Does your government/organization develop or support any educational programmes or academic curricula in cybersecurity…**	**Existence and the promotion of national education courses and programmes to train the younger generation in cybersecurity-related skills and professions in schools, colleges, universities and other learning institutes. Cybersecurity-related professions include, but are not limited to, cryptanalysts, digital forensics experts, incident responders, security architects and penetration testers.**	1.51	Partial	https://www.niais.org/ https://www.nccs.pk/	HEC
C.3.1	In primary education?		2.91	No		
C.3.2	In secondary education?		3	No		

Section	Cyber Security Measure/Parameter	ITU - GCI Objective (Details)	Average of Weightage Recs	Status	Policy Documents/URL	Remarks
C.3.3	In higher education?		4.09	Yes	https://nust.edu.pk/academic/mastersprograms/ https://au.edu.pk/Pages/Faculties/IAA/Departments/Avionics/avi_programs_detail.aspx	HEC
C.4	**Cybersecurity research and development programs**		1.47	Yes	National Cyber Security Policy - 2021	
C.4.1	**Are there cybersecurity R&D activities at the national level?**			Yes	https://ncsael.mcs.nust.edu.pk/ https://www.nccs.pk/	
C.4.1.1	Are there private sector cybersecurity R&D programmes?		3.16	No		
C.4.1.2	Are there public sector cybersecurity R&D programmes?		3.09	Yes	https://www.nccs.pk/	
C.4.1.3	Are higher education institutions such as academia and universities engaged in R&D activities?		3.75	Yes	https://www.nccs.pk/	
C.5	**National Cybersecurity Industry**		1.81	Partial	HEC	
C.5.1	**Is there a national cybersecurity industry?**	**(service providers, system integrators, system developers etc.)?**		Partial	https://www.nccs.pk/	

Section	Cyber Security Measure/Parameter	ITU - GCI Objective (Details)	Average of Weightage Recs	Status	Policy Documents/URL	Remarks
C.6	Are there any government incentive mechanisms in place...	This indicator looks at any incentive efforts by the government to encourage capacity building in the field of cybersecurity, whether through tax breaks, grants, funding, loans, disposal of facilities, and other economic and financial motivators, including dedicated and nationally recognized institutional body overseeing cybersecurity capacity-building activities. Incentives increase the demand for cybersecurity-related services and products, which improves defenses against cyber threats.	1.73	No	Not Existing	
C.6.1	To encourage capacity development in the field of cybersecurity?		5.07	No		
C.6.2	For the development of a cybersecurity industry?	support to start-ups cybersecurity services in academia and other	4.93	Yes	https://www.nccs.pk/	
A	Cooperation Measures					
A.1	Bilateral agreements on cybersecurity cooperation with other countries		2.06	No	Not Existing	
A.1.1	Do you have bilateral agreements on			No		

Section	Cyber Security Measure/Parameter	ITU - GCI Objective (Details)	Average of Weightage Recs	Status	Policy Documents/URL	Remarks
	cybersecurity cooperation with other countries?					
A.1.1.1	Is information sharing part of the agreement(s)?	Information-sharing refers to the practices around sharing on non-sensitive information.	3.76	No		
A.1.1.2	Is capacity building part of the agreement(s)?	The ability to encourage trainings to strengthen the skills, competencies and abilities of National cybersecurity professionals through cooperation to ensure collective efforts against cyber threats.	3.35	No		
A.1.1.3	Is mutual legal assistance part of the agreement(s)?	Mutual assistance between two or more countries for the purpose of gathering and exchanging information in an effort to enforce public or criminal laws.	2.89	No		
A.2	**Government participation in international mechanisms related to cybersecurity activities**	**It may also include ratification of international agreements regarding cybersecurity, such as African Union Convention on Cyber Security and Personal Data Protection, Budapest Convention on Cybercrime and others.**	2.13	Partial	National Cybersecurity Policy	
A.2.1	**Does your government/organization participate in international mechanisms related to cybersecurity activities?**			Yes		

Section	Cyber Security Measure/Parameter	ITU - GCI Objective (Details)	Average of Weightage Recs	Status	Policy Documents/URL	Remarks
A.3	**Cybersecurity multilateral agreements**	**Multilateral agreements (one to multiparty agreements) refers to any officially recognized national or sector-specific programmes for sharing cybersecurity information or assets across borders by the government with multiple foreign governments or international organizations (i.e. the cooperation or exchange of information, expertise, technology and other resources).**	2.04	No	**Not Existing**	
A.3.1	**Does your government have multilateral agreements on cybersecurity cooperation?**			Partial	National cybersecurity policy	
A.3.1.1	Is information sharing part of the agreement(s)?	Information-sharing refers to the practices around sharing on non-sensitive information.	5.33	Partial	National cybersecurity policy	
A.3.1.2	Is capacity building part of the agreement(s)?	The ability to encourage trainings to strengthen the skills, competencies and abilities of National cybersecurity professionals through cooperation to ensure collective efforts against cyber threats.	4.67	Partial	National cybersecurity policy	
A.4	**Partnerships with the private sector (PPPs)**	**Public-private partnerships (PPP) refer to ventures between the public and private sector. This performance indicator measures the number of officially recognized national or sector-specific PPPs for sharing cybersecurity information and assets (people, processes, tools) between the public and private sector (i.e. official partnerships for the cooperation or exchange of information, expertise, technology**	1.89	Yes	National cybersecurity council act National cybersecurity policy	

Section	Cyber Security Measure/Parameter	ITU - GCI Objective (Details)	Average of Weightage Recs	Status	Policy Documents/URL	Remarks
		and/or resources), whether nationally or internationally.				
A.4.1	Does your government engage in PPPs with locally established companies?		5.47	Yes	National cybersecurity council act National cybersecurity policy	
A.4.2	Does your government engage in PPPs with foreign owned companies in your country?		4.53	No		
A.5	**Inter-agency partnerships**	**This performance indicator refers to any official partnerships between the various government agencies within the nation state (does not refer to international partnerships). This can designate partnerships for information- or asset-sharing between ministries, departments, programmes and other public sector institutions.**	1.89	Partial	National cybersecurity council act	
A.5.1	**Are there inter-agency partnerships/agreements among different governmental bodies in relation to cybersecurity?**	**Cooperation between ministries or specialized agencies**		Partial	National cybersecurity council act National cybersecurity policy	

3.3 Gap Analysis Result

According to the gap analysis tool, Pakistan is 41% compliant with ITU GCI measures and 26% compliant by fulfilling ITU's partial requirements. These measures are needed to mature further to make them up to the required/desired level of ITU. Pakistan is 33% non-compliant with the measures of ITU GCI, which needs serious attention to make them according to the requirements of ITU. Furthermore, the below-mentioned chart depicts the complaint status and gap analysis results.

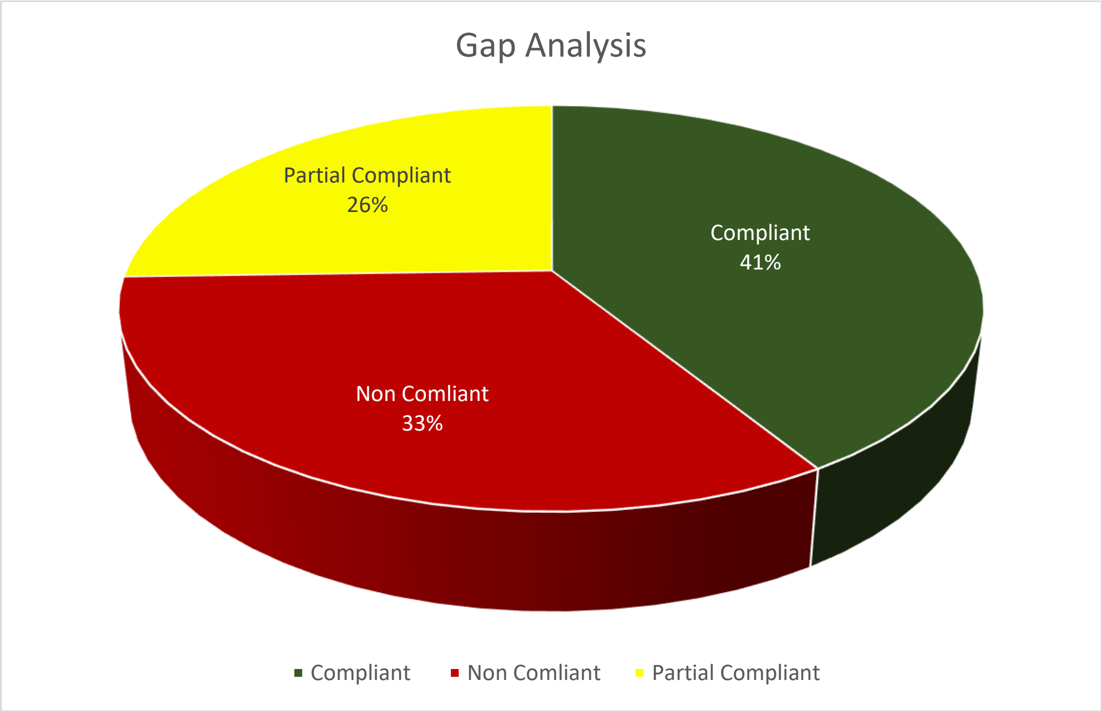


Figure 3- 1 Gap Analysis

Chapter 4

Research Methodology

Keeping in view all the factors like the cybersecurity threat landscape of Pakistan and current measures to address potential security risks. Choosing a research methodology that analyses and incorporates all the existing national security legislation/measures and proposes a suitable framework was challenging, but this research work solved this problem in a very systematic way, followed by below mentioned steps:

a) The first step is analyzing all national-level legislation and trying to understand what they intend to achieve along with their pros and cons.

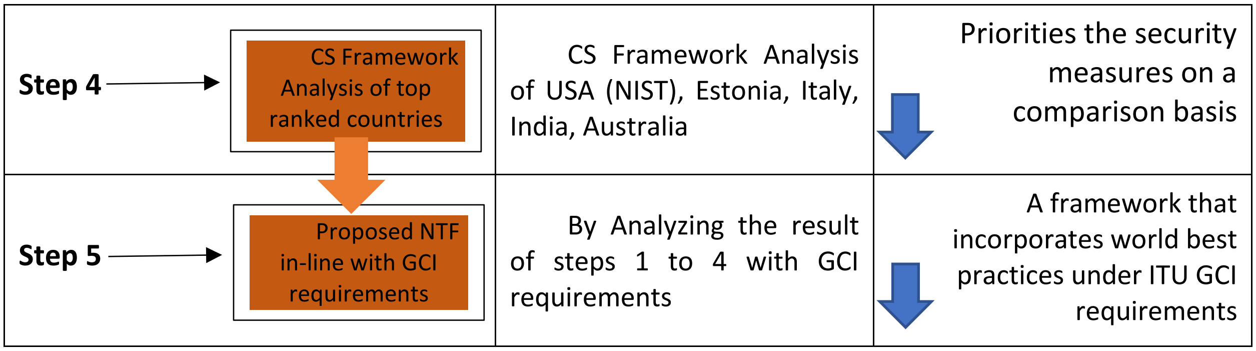
b) Second step – Requirement gathering about ITU GCI measures for its member states.

c) Third step – Gap Analysis, finding the gap between existing national cybersecurity infrastructure and GCI requirements.

d) The Fourth step – Analysing the already implemented cybersecurity framework of top-ranked countries like the United States of America (NIST), Estonia, India, and Australia.

e) Fifth step – Propose a high-level perspective of the National Cybersecurity Framework in-line with the Global Cybersecurity Framework.

Phases	Activity	Output/Delivery
Step 1 → Analysis of National Legislations	Understanding the high-level objectives	Analyzing Existing Cybersecurity Infrastructure
Step 2 → ITU GCI Requirement Gathering	ITU GCI requirement gathering and analysis	82 questions across 20 indicators and five pillars
Step 3 → GAP Analysis	Map existing cybersecurity measures with GCI requirements	Finding the Gap between Existing CS Infrastructure and GCI Requirements



Step 4	CS Framework Analysis of top ranked countries	CS Framework Analysis of USA (NIST), Estonia, Italy, India, Australia	Priorities the security measures on a comparison basis
Step 5	Proposed NTF in-line with GCI requirements	By Analyzing the result of steps 1 to 4 with GCI requirements	A framework that incorporates world best practices under ITU GCI requirements

Figure 4- 2 Research Methodology

4.1 NIST Cybersecurity Framework

The first version of the National Institute of Standards and Technology was introduced in February 2014, and version 1.1 was launched in April 2018. In the latest version, NIST improves clarity about compliance, provides a detailed explanation of cyber supply chain risk management, and provides more clarity on authorization, authentication, and identity proofing. NIST also introduces new sections like self-assessing cybersecurity risks. NIST Cybersecurity Framework (CSF) consists of three main areas:

a) The Framework Core
b) The Implementation Tier
c) The Framework Profile.

The framework Core section is about cyber risk management, and a high-level perspective is defined with five concurrent interrelated functions Identity, Protect, Detect, Respond, and Recover. These functions provide a high-level strategic and continuous process overview. The core functions are depicted in Figure 4.2

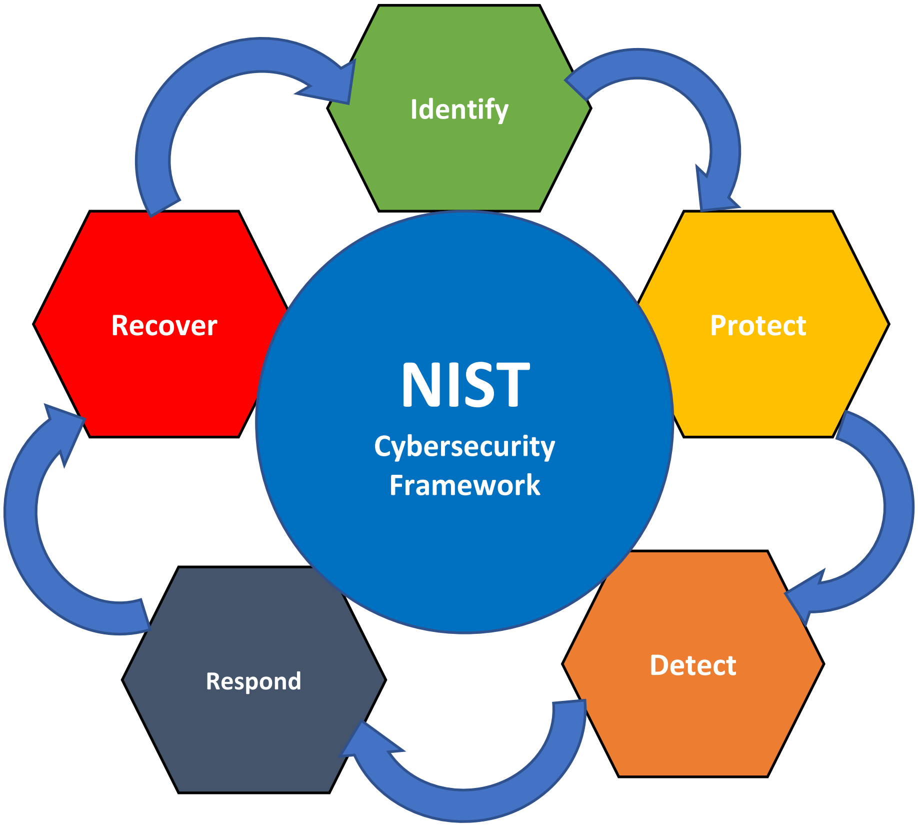


Figure 4- 3 NIST Cybersecurity Framework

Identify: - The Basic step is to identify cybersecurity risks associated with all organization assets like people, procedures, tangible and intangible assets. Assets criticality, prioritization, potential risk assessment, risk treatment strategies, and governance are the primary outcomes of this step.

Protect: - The main objective of this step is to develop and implement respective controls to ensure the protection of critical information assets. The protection mechanism could be but is not limited to Training and Awareness, Access Control, and data privacy and integrity measures.

Detect: - This step enables and develops a mechanism to detect anomalies, identify security events, and monitor security.

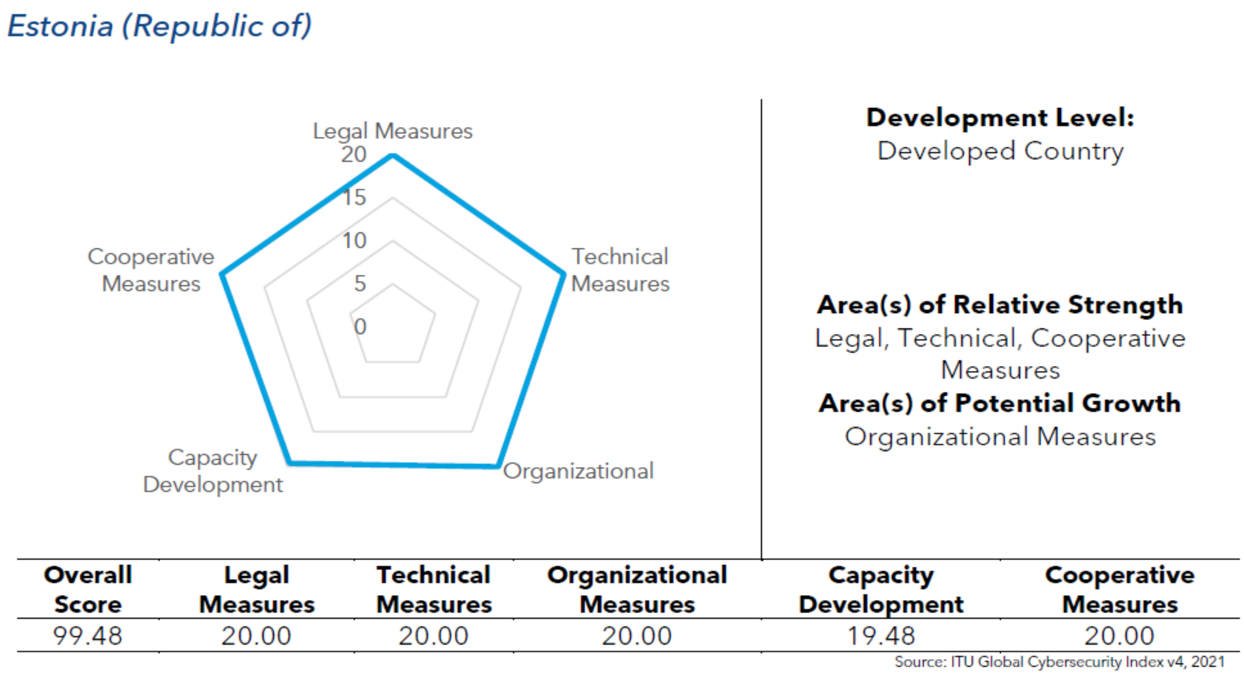
Respond*:* - Refers to a response plan against anomaly detection, which includes the response planning, analysis, conclusion/results, and improvements.

Recover: - The recovery function will develop and implement appropriate processes to reduce the impact of business loss during a cybersecurity incident and ensure business continuity.

The second section of the NIST cybersecurity framework consists of four tiers related to the risk management process. The process started with risk assessment and was followed by risk treatment. The third section is the framework profile which deals with aligning all organizational functions with the help of gap analysis and issues prioritization [20].

4.2 Cybersecurity in Estonia

Estonia is a small northern European country with a 1.33 million population [21]. According to the latest GCI report, Estonia is in 3rd and 2nd position in cybersecurity ranking globally and in the European region, respectively [49]. The Cybersecurity framework of Estonia is majorly based on five legal pillars legal, technical, organizational, cooperative measures, and capacity measures. The Cyber security profile of Estonia is shown in the figure below:



Estonia (Republic of)

Development Level:
Developed Country

Area(s) of Relative Strength
Legal, Technical, Cooperative Measures
Area(s) of Potential Growth
Organizational Measures

Overall Score	Legal Measures	Technical Measures	Organizational Measures	Capacity Development	Cooperative Measures
99.48	20.00	20.00	20.00	19.48	20.00

Source: ITU Global Cybersecurity Index v4, 2021

Figure 4- 4 Cybersecurity Profile of Estonia

4.2.1 Legal Measures

The existing legal legislation of Estonia almost a hundred percent fulfills ITU GCI's requirements. These legislations include the Estonian Cybersecurity Strategy, data protection computer system security criminal legislation, Emergency Act 2009, Critical Infrastructure Protection, The State Secret and Classified Information of Foreign States Act 2009, and the Estonian Information System Authority. Other legal measures of Estonia are shown in the table below [23]:

Legal Measure	Status	Detail
Cybersecurity Policy or Strategy	✓	"Cybersecurity Strategy" Developed by the Estonian government in 2008 incorporated operational and capacity-building relevant frameworks.
Critical Infrastructure Protection Strategy/ Plan	✓	The "Emergency Act 2009" subsection 40 (2) refers to the identification of critical infrastructure identification and protection.
Legislation that requires Information Security Plan	✓	The "Emergency Act 2009", Subsection 40, paragraph two, Security Measures for the Protection of Information Systems
Legislation related to Systems and the classification of data	✓	"The State Secrets and Classified Information of Foreign States Act 2007" deals with state secret and information classification levels.
Legislation that requires security practices to be mapped to risk levels	✓	"The State Secrets and Classified Information of Foreign States Act 2007" align security requirements with information security risk levels.
Annual Cybersecurity Audit	✓	"The State Secrets and Classified Information of Foreign States Act 2007" and "The Electronic Communication Act 2004" refer to periodic inspection and surveillance audits.
The Legislative requirement for the Appointing of a CIO/CSO	✗	No related legislation is found which requires the appointment of a Chief Information Security Officer or Chief Security Officer in public or private organizations.
Legislative measure for Cybersecurity Incident reporting	✓	According to the Regulation on "Security Measures for Information System of Vital Services and Related Information Assets 2013," Information Security Incidents should be reported to the Estonian Information System Authority.
Definition of Critical Infrastructure Protection in Legislation	✓	Estonian Information System Authority defines "Critical Infrastructure" and "Critical Infrastructure Protection."

Table 4- 1 Legal Measures of Estonia

4.2.2 Technical Measures

According to the GCI Report 2020, the technical measures of Estonia are almost completed. Technical measures include but are not limited to National CERT, maturity and affiliation of CERT or Incident response team with international bodies like FIRST, sectoral CERT, and framework for implementing cybersecurity best practices and standards and measures for child online protection.

The summary of all technical or operational measures of Estonia is mentioned below table [24]:

Technical Measures	Status	Detail
National Computer Emergency Response Team (CERT) or Computer Security Incident Response Team (CSIRT)	✓	Computer Emergency Response Team (CERT-EE) was established in 2006 to manage and respond to cybersecurity incidents across the country.
Competent Authority to deal with Network and Information Security (NIS)	✓	2011 Estonian Informatics Center became the Republic of Estonian Information System Authority (RIA). The Authority deals with Network and Information Security matters across the country in all sectors.
A platform for cyber incident reporting and collection of data	✓	The CERT Estonia is responsible for that and provides an email-based incident reporting mechanism. Furthermore, Estonia doesn't have an emergency helpline for the same.
National-level Cybersecurity Drills/Exercises	✓	The Republic of Estonia periodically conducts cybersecurity drills with the joint venture of European Union member states and NATO's Cooperative Cyber Defence Center of Excellence (CCDCOE)
Child Online Protection	✗	No related legislation or authorities have been found that works on child protection, specifically in an online environment.
National-level framework for implementation of cybersecurity standards	✓	Estonian Information System Authority (RIA) is responsible for implementing world best practices and standards across the country.

Table 4- 2 Technical Measures of Estonia

4.2.3 Organizational Measures

Estonia almost fulfills all requirements of ITU GCI under the organizational measures category. National cybersecurity strategy has a major role in this category, followed by the national strategy for child online protection, a responsible agency for implementing national cybersecurity policy or strategy, cybersecurity audits, and cybersecurity risk assessment and analysis.

4.2.3.1 Cybersecurity Strategy of Estonia

The National Cybersecurity Strategy defines a baseline of security and state commitment toward securing national cyberspace. Estonia developed its first cybersecurity strategy in 2008; its latest cybersecurity strategy is for 2019 – 2022. The Cybersecurity Strategy of Estonia is designed to be equally suitable and applicable for the whole state stakeholders, as shown in the figure below.

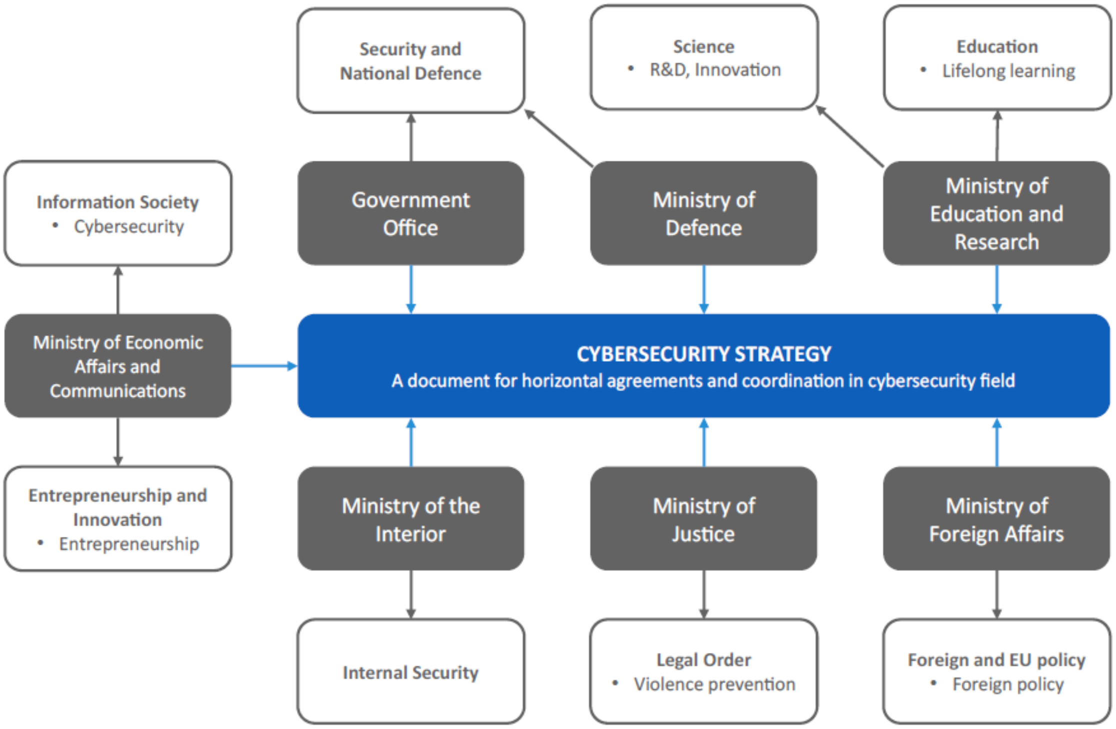


Figure 4- 5 Linkage between CS Strategy and National State Bodies

Majorly there are four objectives of the Estonian cybersecurity strategy, which are the following:

a) *A Sustainable digital society:* Main aim is to develop a reliable digital ecosystem with rapid technological adaptation and cyber resilience. The main areas under this objective are resilience from a technical perspective, preparedness for crises, attacks, and cyber incidents, and the development of competitive leadership, governance, and community.

b) *Cybersecurity Industry, Research, and Development:* The purpose is to develop cybersecurity competencies and strengthen the cybersecurity workforce with the help of innovation research and development. Modern tools like Cyber Range platforms can support innovative research and cyber defense.

c) *Leading International Contributor:* Estonia knows that its stability in the cybersecurity field is associated with its cooperation with other international stakeholders of the cyber industry. The primary purpose of this objective is to fulfill the requirements of cooperative measures of the global cybersecurity index.

d) *A Cyber-literate Society:* Cybersecurity awareness and training are the main objectives as developing cybersecurity talent for in-demand security roles. It is beneficial to find resources with best-fit competencies and mitigate the risk of cybersecurity workforce supply chain security [22].

Other Organizational measures of Estonia are mentioned below in the table:

Organizational Measures	Status	Detail
Cybersecurity Strategy	✓	"Cybersecurity Strategy" Developed by the Estonian government in 2008 incorporated operational and capacity-building relevant frameworks.
Responsible Agency for Implementing Cybersecurity Policies	✓	The Information System Authority (RIA) is responsible for implementing national cybersecurity policies.
Agency overseeing child online protection matters	✗	No such agency existed to oversee the matters of child online protection at the national level.

Organizational Measures	Status	Detail
Action plan/roadmap for the implementation of cybersecurity governance	✓	The first objective of the Estonian cybersecurity strategy 2019-2022 refers to a sustainable digital society through better cybersecurity governance and a cohesive cybersecurity community.
Cybersecurity Audits at National Level	✓	Cybersecurity strategy has the directive and guidelines for conducting cybersecurity audits at the national level.

Table 4- 3 Organizational Measures of Estonia

4.2.4 Capacity Development

Estonia is not completely compliant with ITU GCI Capacity Development measures, and cybersecurity workforce development has a major role in this section. Other measures include public cybersecurity awareness programs, specific cybersecurity education and training, and special cybersecurity research centers.

Other Capacity Development measures of Estonia are listed below in the table:

Capacity Development Measures	Status	Detail
Public Cybersecurity awareness campaigns	✓	Estonian Foreign Policy Development Plan 2030 deals with cybersecurity awareness at the national and international levels. CERT-EE also has the mandate to raise public cybersecurity awareness [25]
Training of cybersecurity professionals	✓	Training of new cybersecurity professionals is part of the Estonian cybersecurity strategy 2019-2022,
Training of cybersecurity professionals of SME/Private Companies	✗	No significant measures were found for the training guide for professionals of private SMEs.
Educational strategy to enhance or support cybersecurity education	✓	The Cybersecurity Strategy of Estonia aims to support and fund the education sector, specifically in the cybersecurity domain.
Cybersecurity Research and Development	✓	The Cybersecurity Strategy of Estonia 2019-2022 has a specific focus on cybersecurity research and development.

Capacity Development Measures	Status	Detail
National Industry for Cybersecurity Capacity Development	✓	The Cybersecurity Strategy and Estonian Information System Authority join hands to gather for the same purpose.

Table 4- 4 Capacity Development Measures of Estonia

4.2.5 Cooperation Measures

Estonia's Cooperative measures almost fulfill GCI's requirements; however, some sections need to be improved. Cooperation mainly includes but is not limited to the bilateral agreement with other countries for cybersecurity and public-private partnerships.

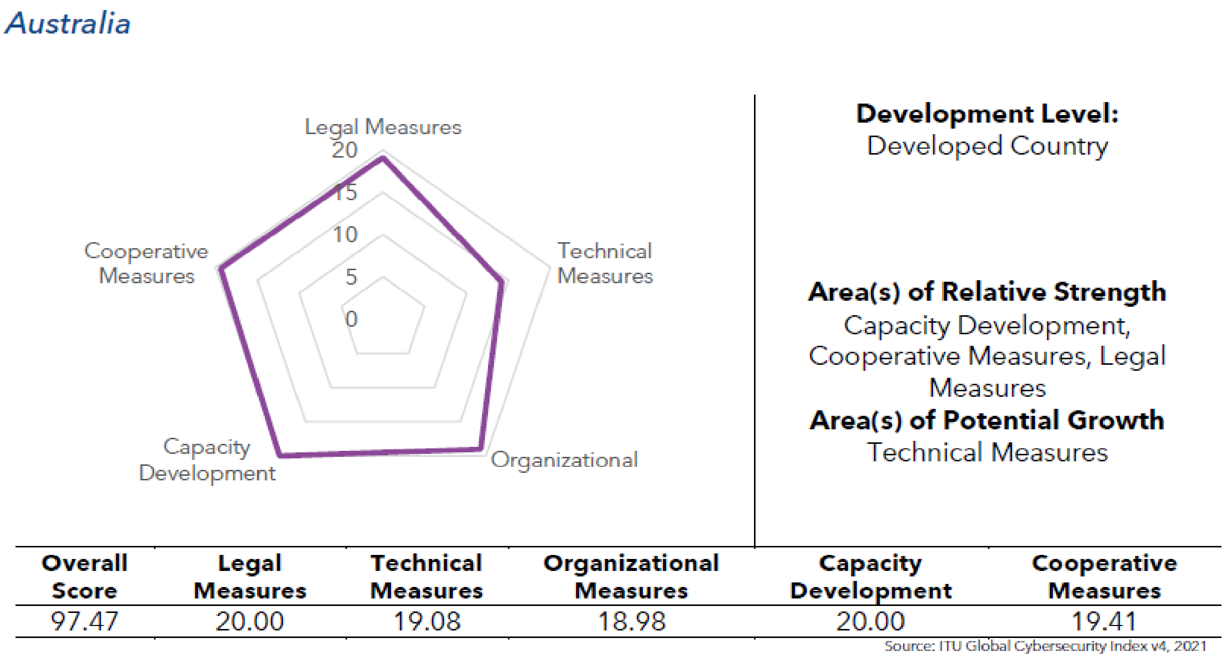
Other measures of cooperation section are mentioned below in the table:

Cooperation Measures	Status	Detail
Bilateral Agreements on Cybersecurity with Other Countries	✓	Estonia is a member of NATO's Cooperative Cyber Defence Center of Excellence (CCDCOE); they share information related to new emerging cyber threats mutually.
Government participation in International mechanisms related to cybersecurity	✓	Since 2020, Estonia has been a member of the World Bank-associated cybersecurity trust fund.
Cybersecurity Mutual Agreement	✓	The cybersecurity alliance for mutual progress (CAMP) and Estonian Informatics Center is a joint cybersecurity agreement [26]
Partnership with the Private Sector	✓	There are no significant measures found for private sector partnership; however, RIA and the Estonian Ministry of Defense have signed MoU with some private sectors [27]
Inter-agency partnership	✓	Estonia is a member state of the European Union and the joint venture of European Union member states and NATO's Cooperative Cyber Defence Center of Excellence (CCDCOE)

Table 4- 5 Cooperative Measures of Estonia

4.3 Cybersecurity in Australia

Australia is an important country in the Asian Pacific region, with a population of 25 million people and 55th in the world population ranking [28]. From a cybersecurity perspective, according to the ITU GCI report 2020, Australia is number 12th and 5th in the global cybersecurity ranking and Asian Pacific Region, respectively. Australia almost fulfilled all requirements of GCI. The cybersecurity profile of Australia is shown below in the figure:



Australia

Development Level:
Developed Country

Area(s) of Relative Strength
Capacity Development, Cooperative Measures, Legal Measures
Area(s) of Potential Growth
Technical Measures

Overall Score	Legal Measures	Technical Measures	Organizational Measures	Capacity Development	Cooperative Measures
97.47	20.00	19.08	18.98	20.00	19.41

Source: ITU Global Cybersecurity Index v4, 2021

Figure 4- 6 Cybersecurity Profile of Australia

Australia is good in cybersecurity legal measures capacity development and lacks technical, organizational, and cooperative measures. To improve its global cybersecurity ranking, they need to advance its Technical, Organizational, and Cooperative measures to stand among top-ranked countries.

4.3.1 Legal Measures

Australia is hundred percent compliant with ITU legal requirements. These requirements include but are not limited to national legislation under ITU GCI guidelines. A summary of the legal measures of Australia is mentioned below in the table [29]:

Legal Measures	Status	Detail
Cybersecurity Strategy / Policy	✓	Australian Government Department of Home Affairs in the year 2016 released a cybersecurity strategy, which was later on, replaced with the Australian Cybersecurity Strategy 2020
Critical Infrastructure Protection Strategy/ Plan	✓	Guidelines for the protection of critical infrastructure are mentioned in the cybersecurity strategy 2020
Legislation that requires Information Security Plan	✓	Ten years plan for cybersecurity resilience, and an action plan to protect critical infrastructure is defined in the Australian Cybersecurity Strategy 2020
Legislation related to Systems and the classification of data	✓	Guidelines related to information and system classification are defined in the Australian Privacy Act. Further categories of system resources are mentioned in the national classification scheme
Cybercrime Substantive Law	✓	Australian Cybercrime Act 2001
Annual Cybersecurity Audit	✓	Australian National Audit Office is responsible for cybersecurity audits at the national level.
Legislation for personal data and privacy protection	✓	The Privacy Act 1988
Legislation for implementation of cybersecurity standards	✓	Australia's Cybersecurity Strategy 2020

Table 4- 6 Legal Measures of Australia

4.3.2 Technical Measures

Australia is lacking behind in technical measures. ITU's major technical measures consist of National and sectoral CERTs, the maturity of CERT, the framework for Implementing different cybersecurity standards, and child online protection. Furthermore, the summary of technical measures of Australia is mentioned below in the table [30]:

Technical Measures	Status	Detail
National Computer Emergency Response Team (CERT) or Computer Security Incident Response Team (CSIRT)	✓	CERT Australia is the national-level computer emergency response team. CERT Australia provides an advisory to concern national critical infrastructure stakeholders about lasted threats and vulnerabilities
Is national CERT affiliated with FIRST?	✓	CERT Australia is mature and affiliated with FIRST
Hotline for reporting Cybersecurity incidents	✓	CERT Australia has a hotline to report cyber incidents; Australian Cybersecurity Hotline: 1300 (1300 292 371)
National-level Cybersecurity Drills/Exercises	✓	Cyber exercises are conducted under the observation of CERT Australia and the Australian Cybersecurity Center (ASCS) [31]
Child Online Protection	✓	Australia's Online Safety Act 2021 incorporates instructions for a child's online environment [32]
National-level framework for implementation of cybersecurity standards	✓	Australian Cybersecurity Strategy 2020

Table 4- 7 Technical Measures of Australia

4.3.3 Organizational Measures

Australia partially fulfills the organizational measures of ITU with a score of 19.98 out of 20. The organizational measures include the National Cybersecurity Strategy, a centralized responsible agency for implementing cybersecurity policies and strategies, and cyber resilience. Furthermore, the summary of the organizational measures of Australia is mentioned in the table below:

Organizational Measures	Status	Detail
Cybersecurity Strategy	✓	Australian Cybersecurity Strategy 2020
Responsible Agency for Implementing Cybersecurity Policies	✓	Australian Cybersecurity Center (ASCS), under the supervision of the Australian Signals Directorate

Organizational Measures	Status	Detail
The agency overseeing child online protection matters	✗	Statutory child protection Australia partially looks into the matters of child online protection
Action plan/roadmap for the implementation of cybersecurity governance	✓	Australian Cybersecurity Strategy 2020
Cybersecurity Audits at National Level	✗	Australian Cybersecurity Center is responsible for doing so, but they are not performing audits at the national level.

Table 4- 8 Organizational Measures of Australia

Cybersecurity Strategy of Australia

The first cybersecurity strategy in Australia was released in 2009, the second in 2016, and the third cybersecurity strategy was released in 2020. According to the latest cyber strategy, their vision and mission are to create a more secure cyberspace for Australia. Australian government invested $230 million in the 2016 strategy for cybersecurity programs, and they allocated a budget of $1.67 billion for ten years to achieve the secure cyberspace goal. The objectives of the cybersecurity strategy are mentioned below:

a) Active defense of Australian critical infrastructure; With the help of adopting new incident investigation techniques and cyber resilience.

b) There should be a strong protection mechanism for government data and network infrastructure and stakeholder collaboration to fill the cyber skills gap.

c) Public-private solid partnership for the latest threat information exchange. Cybersecurity awareness and training about the latest security threats.

d) Establishing the Joint Cybersecurity Center and Australian Cybersecurity Center is the main foundation for cooperation between national and international stakeholders and cyber resilience.

Cyber attacks are growing exponentially, and countering these attacks requires a skilled cyber workforce. Australia is seriously dealing with this issue to secure its digital economy. Australian cybersecurity strategy emphasizes this important issue. An action plan for each stakeholder is also defined as Immediate actions required by the government, actions required by Small and Medium Enterprises, and actions needed by the community because security is not the responsibility of any person or organization. It is the responsibility of everyone in the community [34].

4.3.4 Capacity Development

Australia has almost fulfilled all requirements of GCI under the capacity development pillar. These requirements include cybersecurity awareness campaigns for the public-private sector and civil society. Training of cybersecurity professionals, government support to the education sector for cybersecurity subjects, further measures, and their status is mentioned in the table below:

Capacity Development Measure	Status	Detail
Public Cybersecurity awareness campaigns	✓	Cybersecurity Strategy Australia 2020, Australia will invest billions of $ in cybersecurity awareness for all national stakeholders and civil society.
Training of cybersecurity professionals	✓	Australian Cybersecurity Center is responsible for providing training to cybersecurity professionals.
Training of cybersecurity professionals of SME/Private Companies	✓	Cybersecurity Strategy Australia 2020 and the Australian Cybersecurity Center under the Australian Signals Directorate provide pieces of training to the professionals of private SMEs
Educational strategy to enhance or support cybersecurity education	✓	In the Cybersecurity National Workforce Growth Program, partnerships innovation funds are mandated to support academia for higher education in the cybersecurity field.
Cybersecurity Research and Development	✓	According to Cybersecurity Strategy 2020, Australia will support several technologies and innovation centers like cutting-edge research laboratories, Cybersecurity cooperative research centers, Emerging technology research labs, and Australia's Academic Research Network (AARNet).
National Industry for Cybersecurity Capacity Development	✓	Cybersecurity Strategy Australia 2020 has a directive for the development of cybersecurity capacity.

Table 4- 9 Capacity Development Measures of Australia

4.3.5 Cooperation Measures

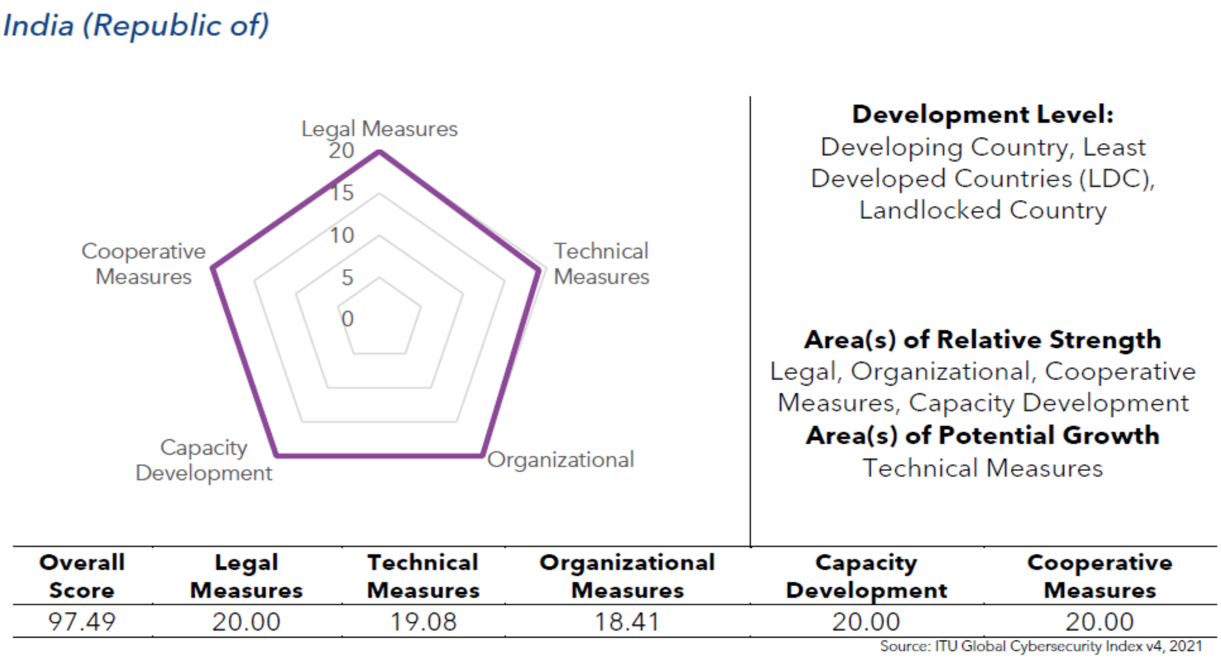
According to the GCI, the Cooperative measure includes the bilateral agreement on cybersecurity cooperation with other countries, government participation in international cybersecurity mechanisms, public-private partnerships, inter-agency partnerships, and multilateral cybersecurity agreements. Australia almost fulfills all requirements of GCI under this pillar. Further detail is mentioned in the table below:

Cooperation Measures	Status	Detail
Bilateral Agreements on Cybersecurity with Other Countries	✓	Cybersecurity Strategy Australia 2020 emphasizes cybersecurity cooperation with its neighbor and other countries, although bilateral cybersecurity information sharing is not part of it
Government participation in International mechanisms related to cybersecurity	✓	Cooperation and participation in international mechanisms related to cybersecurity is the objective of the cybersecurity strategy of Australia.
Cybersecurity Mutual Agreement	✓	Cybersecurity Strategy of Australia and Australian Cybersecurity Centre
Partnership with the Private Sector	✓	Public-private partnership for cybersecurity activities is part of the Australian national cybersecurity infrastructure.

Table 4- 10 Cooperative Measures of Australia

4.4 Cybersecurity in India

The Republic of India is South Asia's seventh and second-largest country by area and population [34]. According to the ITU GCI cybersecurity ranking, India ranks 10th in the global order and 4th in Asia-Pacific Region, with an overall score of 95.5. Indian cybersecurity infrastructure almost covers all requirements of GCI, and further details are shown in the figure below:



India (Republic of)

Development Level:
Developing Country, Least
Developed Countries (LDC),
Landlocked Country

Area(s) of Relative Strength
Legal, Organizational, Cooperative
Measures, Capacity Development
Area(s) of Potential Growth
Technical Measures

Overall Score	Legal Measures	Technical Measures	Organizational Measures	Capacity Development	Cooperative Measures
97.49	20.00	19.08	18.41	20.00	20.00

Source: ITU Global Cybersecurity Index v4, 2021

Figure 4- 7 Cybersecurity Profile of India

According to the GCI Report 2018, India was in 47th position in the global cybersecurity ranking [35]. In two years, India has strengthened its national cybersecurity posture by taking solid initiatives like developing a national cybersecurity strategy, an initiative for child online protection, a national cybersecurity policy of India, and other initiatives for ICT education at school and higher education levels. These measures uplift Indian cybersecurity, ranking almost 37 positions and currently at 10th position in the global cybersecurity ranking. Indian cybersecurity infrastructure fulfills all measures of legal, capacity development, and cooperative pillars, while it lacks technical and organizational measures.

4.4.1 Cybersecurity Strategy of India

The Data Security Council of India (DSCI) presented the first-ever cybersecurity strategy for India in 2020. DSCI is a non-profit organization set up by the National Association of Software and Services Company (NASSCOM), dedicated to making secure, safe cyberspace by adopting the best cybersecurity practices and standards. The Cybersecurity Strategy of India is based on three principles, as shown in the figure below:

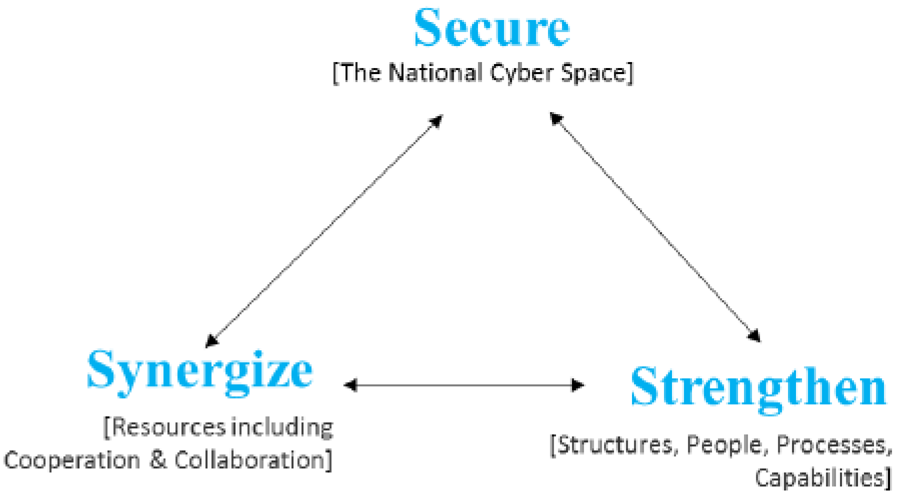

Secure
[The National Cyber Space]
Synergize
[Resources including Cooperation & Collaboration]
Strengthen
[Structures, People, Processes, Capabilities]

Figure 4- 8 Parts of Cybersecurity Strategy India

a) Secure the national cyberspace

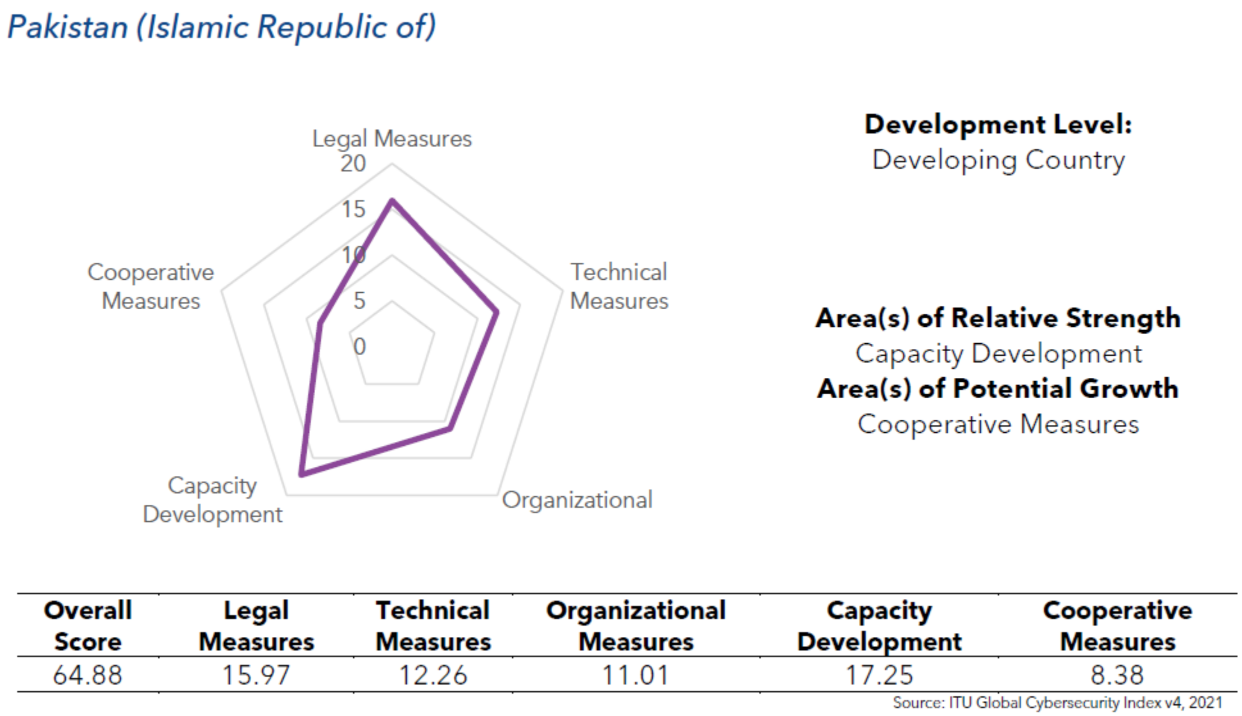
b) Strengthen infrastructure, including people, processes, and capabilities

c) Synergize resources, including collaboration, cooperation, and public-private partnership

The vision and mission of this strategy are to secure the large-scale digitization of public infrastructure, the security of the supply chain by mitigating potential risks, protection of critical infrastructures like the SCADA system, digital payment, Telecommunication services, and power generation and distribution system. The second part of the strategy is to strengthen ICT infrastructure and information security governance, allocate a budget for research development and innovation, auditing, and skill development are the main points. Internet infrastructure security, standards development, cyber insurance, cybercrime investigation, and cyber diplomacy are points of the third part of the strategy [36].

4.4.2 Cybersecurity Profile of Pakistan

According to the ITU GCI report 2020, Pakistan is in the 79th position in the global cybersecurity ranking, regional ranking of Pakistan is 14th position in the Asia-Pacific region with a 64.88 score. Pakistan is behind in almost every measuring field of ITU, including legal, technical, organizational, capacity development, and cooperative measures. Further details and categories score is shown in the figure below:



Pakistan (Islamic Republic of)

Development Level:
Developing Country

Area(s) of Relative Strength
Capacity Development
Area(s) of Potential Growth
Cooperative Measures

Overall Score	Legal Measures	Technical Measures	Organizational Measures	Capacity Development	Cooperative Measures
64.88	15.97	12.26	11.01	17.25	8.38

Source: ITU Global Cybersecurity Index v4, 2021

Figure 4- 9 Cybersecurity Profile of Pakistan

This cybersecurity ranking of countries is based on the questionnaires submitted by respective countries till 2020. At the end of 2021, Pakistan released its first-ever National Cybersecurity Policy, which will be added in the next ranking cycle.

4.4.3 Cybersecurity Infrastructure Comparison India vs Pakistan Under GCI Requirements

Sr #	Description of Cybersecurity Measure	Status in India	Status in Pakistan
1	**The score of Legal Measures**	**20/20**	**15.97/20**
1.1	Legal measures related to child online protection	Yes	Not Existing
1.2	National Level Cybersecurity Audit	Yes	Partially Existing
3	**The Score of Technical Measures**	**19.08/20**	**12.26/20**
3.1	National Governmental CERT	CERT India	Not Existing

Sr #	Description of Cybersecurity Measure	Status in India	Status in Pakistan
3.2	Conduct regular cybersecurity exercises like cyber drills	National Cybersecurity Strategy, India	Not Existing
3.3	CERT contribution to child online protection	CERT India	Partially, FIA Cyber Crime Wing
3.4	National CERT Affiliated with FIRST	Yes	No
3.5	Participation of sectoral CERT in National Cyber Drills	Yes	No
3.6	National Framework for implementation of cybersecurity standards	Yes, in National CS Strategy	Yes, in National CS Policy
3.7	Child Online Protection	Yes	No
4	**The Score of Organizational Measures**	**18.41/20**	**11.01/20**
4.1	National Cybersecurity Strategy	Yes, National CS Strategy 2020	No
4.2	National Strategy for Child Online Protection	Partially	No
4.3	Responsible Agency for Cybersecurity Coordination	Yes	No
5	**The Score of Capacity Development Measures**	**20/20**	**17.25/20**
5.1	Initiative of cybersecurity awareness campaigns targeting civil society	Yes	No
5.2	Training for Cybersecurity Professionals	Yes	Partial
5.3	National Sector-specific Cybersecurity Training programs/courses for law enforcement	Yes	No
5.4	National Sector-specific Cybersecurity Training programs/courses for judicial and other legal actors	Yes	No

Sr #	Description of Cybersecurity Measure	Status in India	Status in Pakistan
5.5	Governmental support for cybersecurity education programs at the primary level	Yes	No
6	**The Score of Cooperation Measures**	**20/20**	**8.38/20**
6.1	Bilateral Agreements on cybersecurity with other countries	Yes, CERT India	No
6.2	Government participation in international activities related to cybersecurity	Yes	Partial
6.3	Public-Private Partnership for cybersecurity	Yes	Partial

Table 4- 11 Cybersecurity Infrastructure Pak vs India

Chapter 5

National Technology Framework In line with Global Cybersecurity Framework

Keeping in view the cybersecurity ranking of Pakistan at the global and regional levels, the National Technology Framework (NTF) is the primary need of the country. The main objective of NTF is to increase Pakistan's cybersecurity ranking and propose a high-level perspective of the cybersecurity framework for Pakistan under the guidelines of ITU and GCI. It is resultantly the development of safe and secure cyberspace by adopting best security practices and standards for national critical infrastructure security.

The proposed technology framework is based on the cybersecurity infrastructure of the top-ranked member states of ITU, Gap analysis of the existing cybersecurity infrastructure of Pakistan with ITU GCI requirements, and analysis of existing local cybersecurity legislation policies with other top-ranked countries; all of these are explained in detail in other chapters. Furthermore, the effectiveness of already cybersecurity policies and the implementation of corresponding security controls have been evaluated to get an insight into the real cybersecurity posture of Pakistan. In light of all these, the proposed framework is based on five parameters which are legal, technical, organizational, cooperation measures, and capacity development, as shown in the figure below:

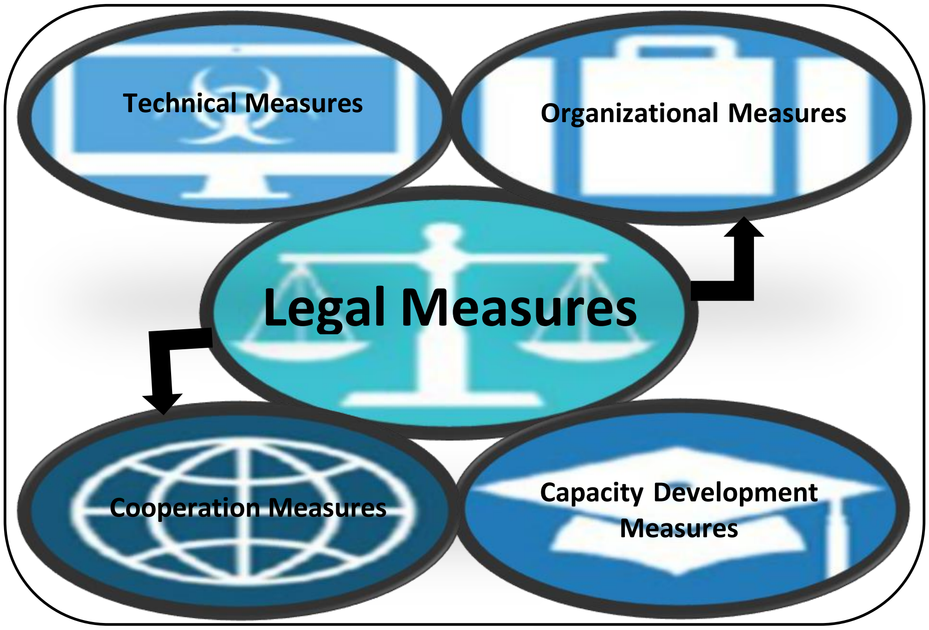


Figure 5- 1 Parameters of NTF

National Technology Framework is based on the requirement of five parameters: capacity building, technical, organizational, legal, and cooperation. These five pillars are also called Global Cybersecurity Agenda (GCA), as shown below in the figure.

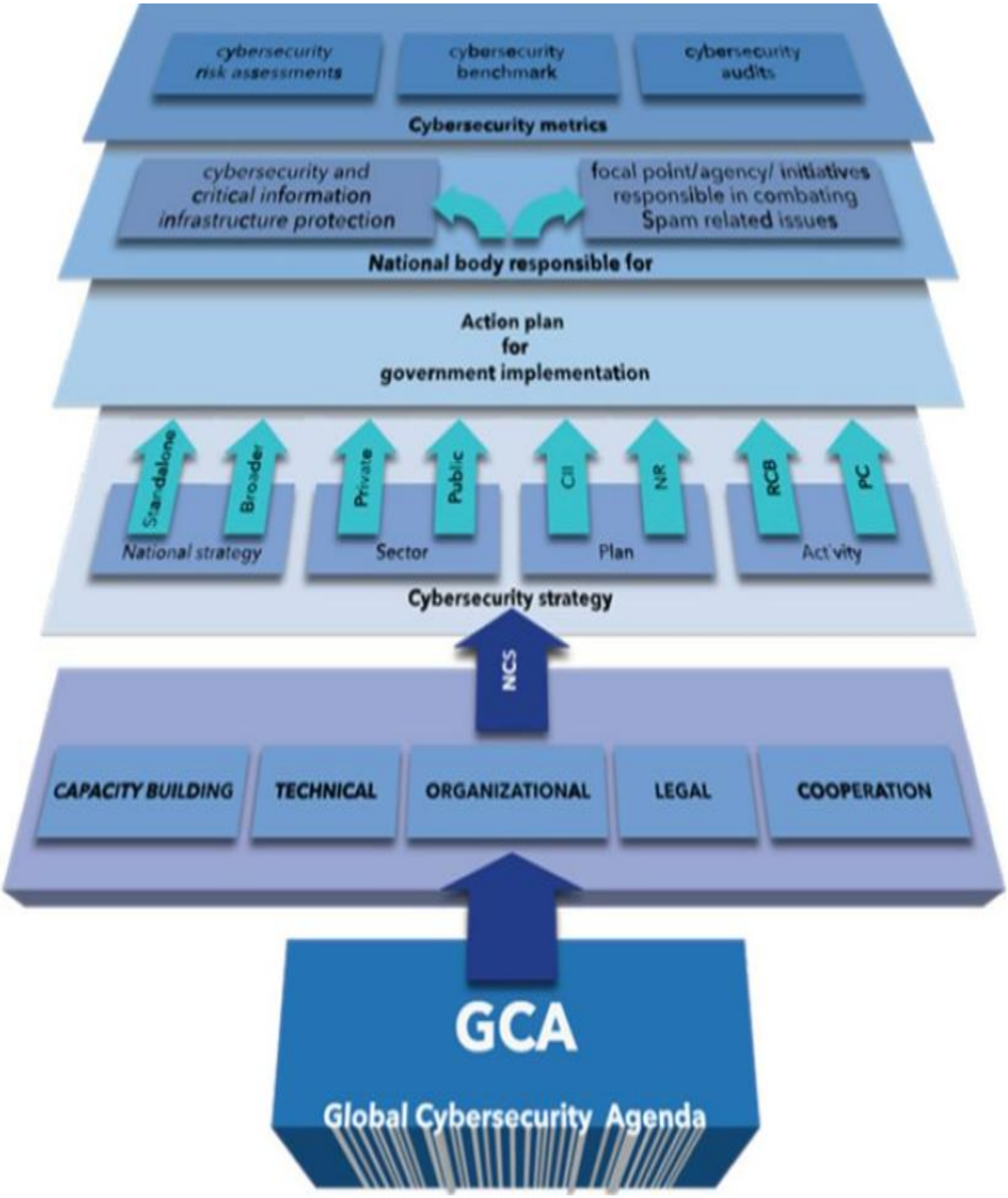

cybersecurity risk assessments
cybersecurity benchmark
cybersecurity audits
Cybersecurity metrics
cybersecurity and critical information infrastructure protection
focal point/agency/ initiatives responsible in combating Spam related issues
National body responsible for
Action plan for government implementation
Standalone
Broader
Private
Public
CII
NR
RCB
PC
National strategy
Sector
Plan
Activity
Cybersecurity strategy
NCS
CAPACITY BUILDING
TECHNICAL
ORGANIZATIONAL
LEGAL
COOPERATION
GCA
Global Cybersecurity Agenda

Figure 5- 2 Broader view of NTF

5.1 Legal Measures

Legal measures are based on the country's legal infrastructure, like legislation, institutions, and frameworks, to deal with cybercrimes and cybersecurity at the national level. The legal measures are the foundation for authorizing a state to act against cybercrimes, investigations, and penalties against non-compliance with local cybersecurity legislation. A legislation framework like policies, strategies, procedures, and guidelines is the foundation for cyber resilience and capabilities. The main objective of the legislation is to have sufficient guidelines to fulfill legal measures for the safety and security of national cyberspace by adopting best practices and standards. The strength of the legal parameters of a country depends upon the number of legislations, cybersecurity frameworks, and legal institutions. Considering Pakistan's existing legislative infrastructure, apart from those discussed below, legislation is highly recommended for Pakistan.

5.1.1 National Cybersecurity Regulatory Authority (NCRA)

Currently, no such governmental authority exists that regulates public/private organizations/institutions concerning cybersecurity at the national level. The National Cybersecurity Authority (NCRA) will be responsible for developing and complying with federal cybersecurity legislation incorporating the latest tools, technologies, maintenance, and implementation of the National Technology Framework. It is also accountable for collaboration and coordination on cybersecurity-related national and international matters. The members of this regulatory Authority should be from the public and private sectors. Furthermore, the structure is shown below in the figure:

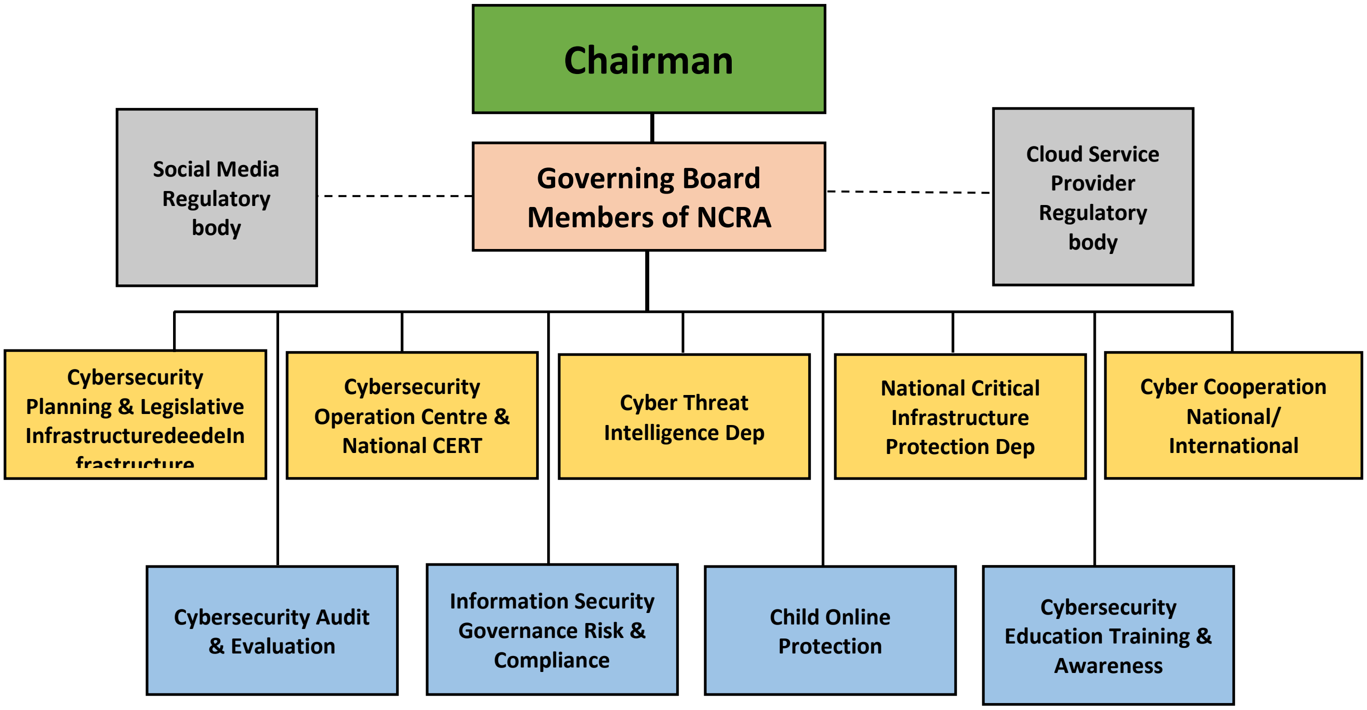

Chairman
Governing Board Members of NCRA
Social Media Regulatory body
Cloud Service Provider Regulatory body
Cybersecurity Planning & Legislative InfrastructuredeedeIn frastructure
Cybersecurity Operation Centre & National CERT
Cyber Threat Intelligence Dep
National Critical Infrastructure Protection Dep
Cyber Cooperation National/ International
Cybersecurity Audit & Evaluation
Information Security Governance Risk & Compliance
Child Online Protection
Cybersecurity Education Training & Awareness

Figure 5- 3 Structure of NCRA

The governing board members should be from academia, public and private sector, and there should be a separate head of department for each branch of the national cybersecurity regulatory. This body is responsible for the cybersecurity matters of the state at the strategic, tactical, and operational levels. The functions of NCRA include but are not limited to the following:

a) Develop national cybersecurity legislation like Policies, strategies, procedures, and guidelines.

b) Improvement of cybersecurity ranking of Pakistan, developing secure and safe cyberspace for stakeholders.

c) From a broader perspective, it is responsible for cybersecurity measures under legal, technical, organizational, capacity development, and cooperation measures.

d) The regulatory body of social media and cloud computing platforms is also a thematic area of its functions.

5.1.2 Cybersecurity Policies

What is policy, and why should a country have a national cybersecurity policy?

A policy is a document that defines a high level of objective or management directives, what a country intends to do, and what they want to achieve; policy is also the description of a high-level futuristic goal. National Cybersecurity policy refers to a plan that defines what a country intends to do or achieve soon in cybersecurity at the national level. Pakistan developed its first-ever cybersecurity policy in 2021; further detail is discussed in the literature review section.

The cybersecurity planning and legislative infrastructure development department in NCRA should be responsible for all cybersecurity legislation at the national level. The cyber threat landscape is changing very quickly. New technologies are evolving with novel threats and vulnerabilities. In this situation, the legislative infrastructure department is responsible for the development and revision/review of all policies incorporating the latest tools and technologies. The legislation related to the following should be developed immediately:

a) Policy related to personal data protection, privacy, and protection of personal data
b) Legislation for systematic and periodic audit/evaluation of federal organizations
c) Development of legislation for the implementation of cybersecurity standards within the governmental organizations
d) Legislation related to the use of digital signatures for E-Government or other document authentication mechanism
e) National critical infrastructure protection policy
f) Cybersecurity workforce development, education, awareness, R&D Policy

5.1.3 Cybersecurity Strategy

Why should the country adopt a cybersecurity strategy?

Strategy is not a piece of national-level document that describes a high-level objective. Infect the strategy is a real detailed strategy that means being a country, what you intend to do practically to protect the country's national interest by securing national cyberspace, socioeconomic development, public and private sector protection, critical infrastructure, and protecting citizens online. According to the ITU cybersecurity experts' panel, if a country doesn't have a national cybersecurity strategy, they are not dealing seriously with security at the national level [19]. Cybersecurity strategy helps the country improve and maintain secure cyberspace and cyber resilience. In cybersecurity, the security strategy is defined as a systematic path for cyber incidents to CERT, law enforcement agencies, intelligence services, or other civil services. Still, a sound cybersecurity strategy brings it all together quite simply for a state.

The biggest cybersecurity strategy challenges are priorities, the national issues to address, and finding the gaps and funding. Other problems include capacity development, bilateral agreements on information exchange, incident response, accountability, and cyber resilience. An excellent national cybersecurity policy and national cybersecurity strategy help overcome all the issues mentioned above. Currently, Pakistan has no cybersecurity strategy at the national level, and there is a need to develop the strategy urgently. A cybersecurity strategy lifecycle should have five phases:

a) Initiation
b) Analysis
c) Production
d) Implementation
e) Monitoring and evaluation

The initiation phase starts with developing a project authority and a top leadership selection. Establishing a steering committee, identifying stakeholders, and planning and evolving strategy is the function of this phase. Stage two's tasks are measuring the cybersecurity threat landscape and assessing cyber risks. In phase three, a draft cybersecurity strategy is developed to review stakeholders, and a formally approved strategy is published after consultation. The authorized strategy is implemented with the help of an action plan; allotment of funds, resources, and time frame are the functions of the fourth phase. The fifth step is monitoring with the help of key performance indicators (KPIs) and governance [37]. Further details of cybersecurity strategy development are shown in the figure below:

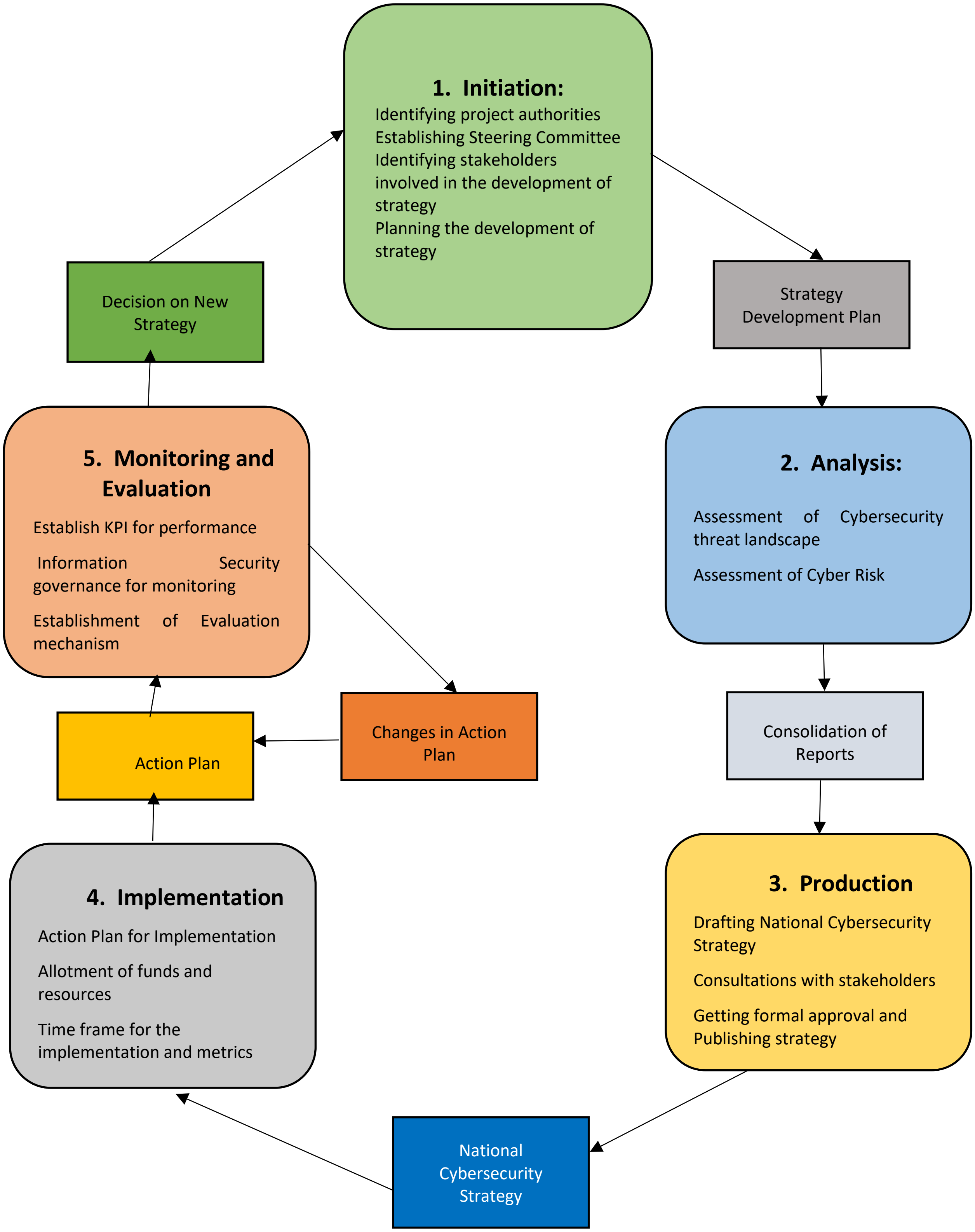

1. Initiation:
Identifying project authorities
Establishing Steering Committee
Identifying stakeholders involved in the development of strategy
Planning the development of strategy
Strategy Development Plan
2. Analysis:
Assessment of Cybersecurity threat landscape
Assessment of Cyber Risk
Consolidation of Reports
3. Production
Drafting National Cybersecurity Strategy
Consultations with stakeholders
Getting formal approval and Publishing strategy
National Cybersecurity Strategy
4. Implementation
Action Plan for Implementation
Allotment of funds and resources
Time frame for the implementation and metrics
Action Plan
Changes in Action Plan
5. Monitoring and Evaluation
Establish KPI for performance
Information Security governance for monitoring
Establishment of Evaluation mechanism
Decision on New Strategy

Figure 5- 4 National Cybersecurity Strategy Lifecycle

5.2 Technical Measures

Technical measures are the first line of defense against cyber threats, and the existence of specialized institutions, mechanisms, and frameworks are prerequisites for technical measures. Developing secure national cyberspace is impossible without deploying technical controls like incident detection and prevention mechanism, vulnerability assessment, and cyber emergency response team. Therefore, Pakistan needs to implement baseline security controls by adopting best security practices and standards with the help of the National Cybersecurity Regulatory Authority (NCRA).

5.2.1 Cyber Emergency Response Team Pakistan (CERT-Pak)

The dynamic change in the cyber threat landscape puts national ICT critical infrastructure of governments and the private sector at risk of attacks and breaches. To mitigate and counter these novel attacks, the state needs a coordinated and centralized response from the state [38]. Due to its strategic location and prevailing cyber terrorism, Pakistan desperately needs a Cyber Emergency Response Team (CERT). The proposed CERT operates under the National Cybersecurity Regulatory Authority (NCRA) directive and directions. The following should be the functions of CERT:

a) One window solution for contacting and reporting cyber incidents
b) Assist the public-private sector in handling cybersecurity incidents
c) Incident response according to the situation
d) 24 x 7 security services, monitoring, and response
e) Production of cyber threat intelligence for national stakeholders
f) Issue security awareness training, guidelines, and advisories to national stakeholders
g) Issue reports and statics biannually about threats to SMEs and the public-private sector
h) Conduct cybersecurity exercises such as cyber drills

The proposed CERT should proactively participate in cyber security offensive and defensive activities, and drills at the national and international levels should contribute to child online protection. CERT-Pak should be a member of any global cyber incident response forum like FIRS.

Management should focus on the maturity of CERT and take steps to get affiliated with national CERT with other regional CERTs like OIC CERT, APCERT, etc.

5.2.2 Sectoral CERT

Sectoral CERT is a cyber or computer emergency response team dedicated explicitly to the national critical sectors like Health care, Finance, Telecommunication, and Education. These CERTs provide services within the specific industry/sector under the cooperation of national CERT. The function of these CERTS are the same (cybersecurity drills, security awareness training, maintaining statistics of threats and vulnerabilities) as the national CERT, but their scope is limited to a specific sector.

5.2.3 National Framework for Implementation of Cybersecurity Standards

At the strategic level, dealing with National information security risks and local and international policy compliance is the biggest challenge. There should be a National framework for the implementation of cybersecurity standards. The NCRA uses this national framework for risk assessment and compliance enforcement, and it will make it easy to watch, warn, and respond to security incidents. The following should be the component of this framework, an overview of the framework is shown in Figure 5.5.

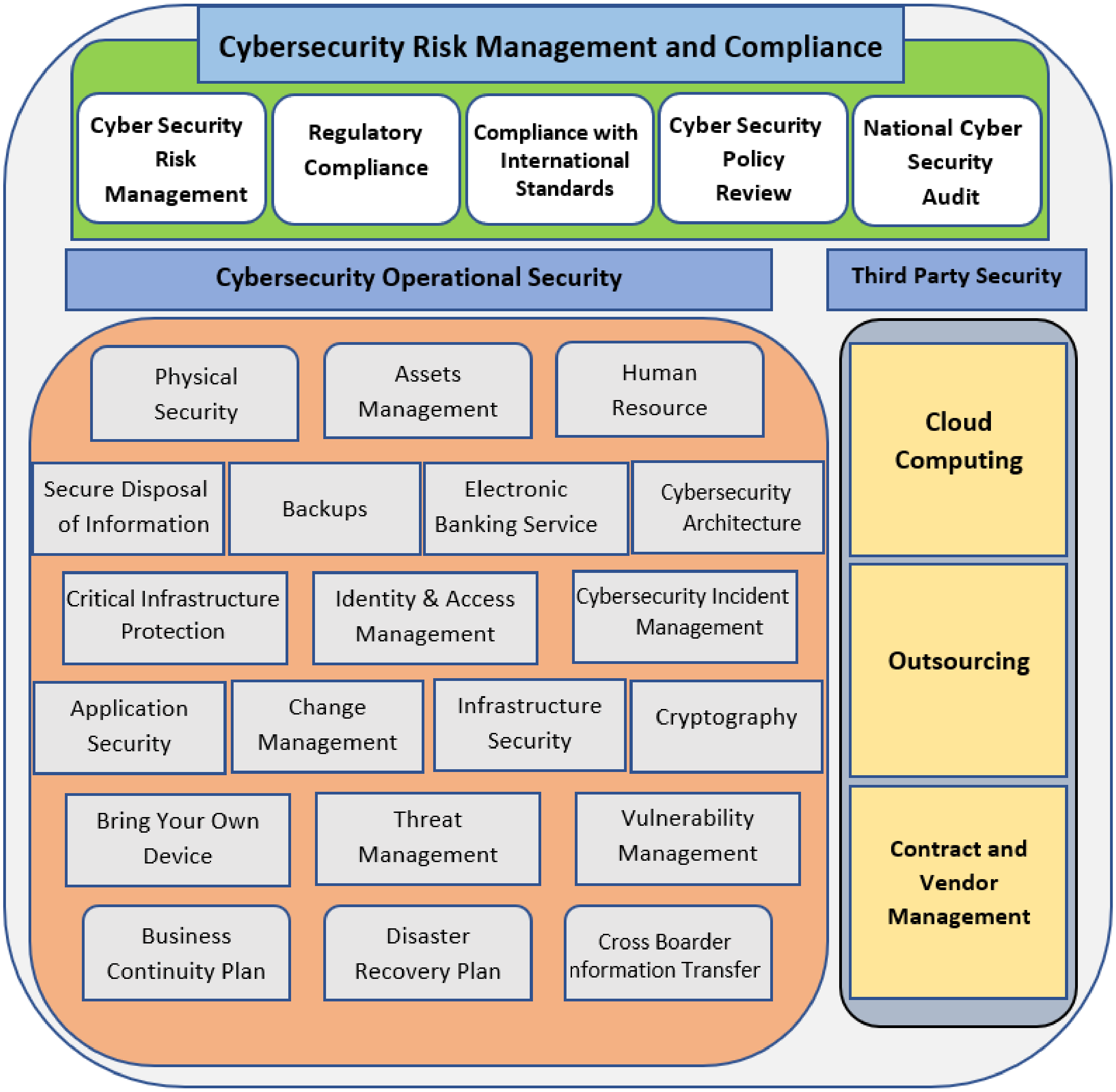

Cybersecurity Risk Management and Compliance
Cyber Security Risk Management
Regulatory Compliance
Compliance with International Standards
Cyber Security Policy Review
National Cyber Security Audit
Cybersecurity Operational Security
Third Party Security
Physical Security
Assets Management
Human Resource
Secure Disposal of Information
Backups
Electronic Banking Service
Cybersecurity Architecture
Critical Infrastructure Protection
Identity & Access Management
Cybersecurity Incident Management
Application Security
Change Management
Infrastructure Security
Cryptography
Bring Your Own Device
Threat Management
Vulnerability Management
Business Continuity Plan
Disaster Recovery Plan
Cross Boarder nformation Transfer
Cloud Computing
Outsourcing
Contract and Vendor Management

Figure 5- 5 National Framework for Implementation of Cybersecurity Standards

Figure 5.5 depicts a high-level overview of the cybersecurity framework for implementing world best practices and standards. The NCRA should use this framework for risk assessment and compliance review at the national level and enforcement of international standards but not limited to ISO, ITU, NIST, PCI DSS, IEEE, FIPS, etc.

5.2.4 Child Online Protection

An abrupt information and communication technology development made internet access easy for children—this easy access lure-in more children connected to the internet on personal or shared devices. However, COVID-19 and this wider and more familiar access to the internet puts children’s rights and safety at risk. Today, children are more vulnerable to harassment, cyberbullying, harmful online content, sexual abuse, and exploitation. All these factors make child online protection a global challenge.

The International Telecommunication Union gives considerable weightage to its member state's child online protection (COP) mechanism and measurements. Although some measures exist in Pakistan to protect users in the online environment, there is no dedicated legal framework and measures for child online protection at the national level. The children in Pakistan are more vulnerable to cyberbullying and harassment, grooming for sexual purposes, luring in for sexual abuse, and kidnapping.

Pakistan needs to take serious action for child online protection and should develop a comprehensive policy with the following policy action items:

Child Rights: National authorities should define child rights by collaborating with international bodies working on child rights, like the United Nations (UN). Child rights should protect children online through a proper mechanism for monitoring, investigation, education, training, and awareness session with the child's participation of children.

Legislations: Pakistan needs to develop more legislation specifically for child protection in the online environment. This legislative framework should address illegal acts against children with the help of the internationally best-implemented framework for child online protection.

Regulation and Law Enforcement: should develop regulations in line with child protection in the online environment, and enforcement of these policies should be made sure with specialized law enforcement agencies dedicated to child protection.

Reporting and Monitoring: The state should establish a mechanism for reporting illegal content online and a hold line to facilitate reporting of children's online safety issues. Authority should be developed to monitor the gauge online activities of children and relevant stakeholders.

ICT Sector: Encourage the ICT industry to adopt a mechanism for the safety of children in the online environment. The industry should ensure a friendly report protocol against child abuse online.

Education, Awareness, and Capacity: The education sector should introduce some courses for child online protection. National-level awareness programs should also be part of this national strategy for child online protection.

5.3 Organizational Measures

International Telecommunication Union gives considerable value to organizational measures of its member states in evaluating cybersecurity ranking. According to Global Cybersecurity Index 2020, Pakistan can only obtain eleven points out of twenty, which means Pakistan only fulfills fifty percent of requirements from an organizational measure’s perspective.

Organizational measures consist of national strategic planning, objectives, and defining roles and responsibilities of cybersecurity institutions in achieving strategic goals. Organizational measures are necessary to implement controls and maintain secure cyberspace effectively. Organizational strategic goals should be aligned with the national cybersecurity strategy because achieving these goals without a national cybersecurity strategy is difficult.

The proposed National Cybersecurity Regulatory Authority (NCRA) will play a vital role in organizational measures. The bodies and functions/departments under NCRA are responsible for the following respective roles:

5.3.1 Cybersecurity Planning & Legislative Infrastructure

The cybersecurity planning and legislative infrastructure section's role is crucial under the panel of this department, which will be reporting to the board of directors of NCRA. This section is responsible for the national legislative framework, which includes policy, procedures, and strategy development for the relevant stakeholders. The following are some responsibilities of this section include:

a) Development of National Cybersecurity Strategy
b) Development of cybersecurity policies, procedures, and regulations
c) Development of cybersecurity privacy laws
d) Critical infrastructure protection legislations development
e) Development of cybersecurity regulatory framework for all ICT infrastructure organizations
f) Updation of relevant cybersecurity regulation with change in the threat landscape
g) Monitor and analyze cybersecurity threats

5.3.2 Cybersecurity Operation Center and National CERT

The function of the national security operation center is to provide a framework for operational security monitoring and incident management. The National Cyber Emergency Response Team (CERT) provides the services of preventing, detecting, responding, and recovering against cyber threats. They also protect national critical infrastructure by maintaining situational awareness and coordinating with relevant stakeholders. The following are the primary functions of this section under NCRA:

a) Regulate Sectoral and Organizational CERT within Pakistan.
b) Identify the incidents, respond, and make a strategy to recover at the national level.
c) Responsible for the identification of threats and vulnerabilities for the state.
d) Incident coordination with other national and international stakeholders
e) Arrangements of cybersecurity awareness and training sessions across the country.

5.3.3 Cyber Threat Intelligence

Cyber Threat Intelligence (CTI) operated closely with the national CERT and defense security intelligence agencies. This intelligence department aims to gather cyber threat intelligence information with the cooperation of international stakeholders. The primary focus of this department is to provide threat intelligence deriving from global cyberspace, political extremism, cyber terrorism, and sabotage. It also helps in conducting the cyber crime investigation with the cooperation of national and international stakeholders.

5.3.4 National Critical Infrastructure Protection

National Critical Infrastructure Protection Department is vital to National Cybersecurity Regulatory Authority. This department is responsible for the protection of national critical assets and infrastructure. Following should be the functions of this department under NCRA:

a) Development of cybersecurity policies for critical infrastructure organizations/sector
b) Make sure the implementation of these policies and take necessary actions for continual improvement.
c) Risk assessment and making strategies to mitigate/treat those potential risks
d) Arrangement of training and awareness sessions on the protection of critical infrastructure and resilience
e) To do research and development on protecting critical infrastructure with the collaboration of international research institutions and academia.

5.3.5 Cybersecurity Cooperation

The proposed cybersecurity cooperation department will work under the guidelines of ITU GCI’s cooperation measures. This department cooperates with national and international stakeholders to secure their respective cyberspace. This department's functions, roles, and responsibilities are mentioned in the next section of the chapter.

5.3.6 Cybersecurity Audit & Evaluation

The main role of this department is to take action for the continual improvement of the cybersecurity posture of national critical infrastructure organizations. The continual improvement can only be gauged through periodic audits. The following should be the role and responsibilities of this department:

a) Cybersecurity audits of the public-private sector, critical infrastructure organizations, and other entities.
b) Checking the compliance level of national and international best standards/practices within government agencies.
c) Evaluation of cybersecurity measures and technical controls deployed for the protection of critical infrastructure.
d) Development of strategies for the improvement of the overall security of the national cyberspace
e) Regularise the auditors and audit process within the countries, and coordinate among other stakeholders.

5.3.7 Information Security Governance, Risk, and Compliance

Information security governance is a process to manage an organization or country's overall information security posture through Governance, Risk Assessment, and Risk Treatment framework; resource optimization and transparency are also part of information security governance. The following should be the functions of the information security GRC department:

a) Design, develop and optimize the information security governance frameworks.
b) Risk Assessment and propose the best treatment options
c) Compliance and identity access management for the national stakeholders
d) Development of cybersecurity policies, procedures, and guidelines for the organizations operating in national cyberspace
e) Advising mechanisms for business continuity and disaster recovery
f) Conducting time-to-time guidelines for third-party risk management and performance monitoring

5.3.8 Child Online Protection

The role of this department is to take necessary actions under the guidelines of ITU GCI and national and international agencies to protect children in the online environment. This department's further detail and functions are mentioned in section 5.2.4.

5.3.9 Cybersecurity Education Training & Awareness

The Cybersecurity education training and awareness department works in line with the capacity development measures of ITU GCI. This department aims to create national cybersecurity awareness and training sessions for the public and private sectors. Further details, roles, and responsibilities are mentioned in the capacity development section of this chapter.

5.4 Capacity Development

About one million new people connect to the internet daily [39]. Capacity Development measures are the surety of a country's cybersecurity workforce supply chain strengthening. These measures aim to create cybersecurity awareness and training nationwide and arrange special competency development programs for cybersecurity professionals. Support educational institutes in designing and launching a cybersecurity course/program at primary, secondary, and higher education levels. Develop, and support research and development programs in the field of cybersecurity.

Capacity development is the mandate of the “Cybersecurity Education Training and Awareness” department under the NCRA. The following should be the core role and responsibilities of the capacity development measures:

a) Take initiative in cybersecurity education programs at school, college, and university levels. The main aim is to equip students with the necessary and latest knowledge of the cybersecurity field.

b) Launch training and certification programs for cybersecurity experts in the public and private sectors.

c) Design and launch cybersecurity awareness campaigns to educate the general public about the threat landscape and their countermeasures.

d) Make arrangements for collaboration between industry and academia to address real cybersecurity challenges of the industry.

e) Establish research and development centers to support excellence in the cybersecurity field.

f) Help the other stakeholders of NCRA with policy and strategy development and planning.

5.5 Cooperation Measures

Cybersecurity collaboration in a country is defined by policy and strategic approach; Cybersecurity brings the community of international experts together for information exchange and to share the latest threats landscape. For example, Interpol and Europol mutually exchange information about cyber crimes and investigate together. The “Cybersecurity Cooperation” department of NCRA will be responsible for national and international cooperation for cybersecurity matters. This measurement's main aim is to gauge countries' partnerships in cybersecurity. The list of primary functions is following:

a) Bilateral agreements on cybersecurity incorporate information exchange, capacity building, and mutual legal assistance as part of this agreement.

b) Organise and participate in national and international cybersecurity drills and activities.

c) Make internationally multiparty agreements, sector-specific or across borders, for cybersecurity activities and information exchange.

d) Arrange public-private partnerships to boost the security of critical infrastructure.

e) Make inter-agencies collaborate for exchanging cybersecurity information at national and international levels.

f) Coordinating cybersecurity research cooperation between national and international industries and academic institutions.

g) This department is also responsible for coordinating cyber diplomacy, incident response, and threat intelligence exchange.

With these fundamental functions, the Cybersecurity cooperation department helps to strengthen the further national cybersecurity posture and fulfills the cooperation measures of ITU GCI.

Chapter 6

Conclusion and Future Work

6.1 Conclusion

New technologies are evolving, and the threat landscape is changing dramatically. Securing national cyberspace is a big challenge in this competitive era. The proposed National Technology Framework, in line with Global Cybersecurity Framework, provides the best practices to boost the national cybersecurity posture of the country. Implementing this framework will uplift the cybersecurity ranking of the state among the top 10 countries in the ITU GCI ranking. A systematic approach is used to identify the gaps between current cybersecurity measures and top-ranked member states. The proposed National Cybersecurity Regulatory Authority (NCRA) will regulate public and private sector organizations concerning cybersecurity. The proposed NCRA will design, develop and update the cybersecurity legislative framework, and it will also take the strategic initiative to define technical measures, organizational measures, capacity building, and cooperation measures for securing critical infrastructure. The ultimate goal of this framework is the development of safe and secure cyberspace for national and international stakeholders.

6.2 Future Work

The following items are listed for the future work coooresponding to this framework:

a) Development of framework for Social Media Regularization

b) Development of framework for cloud computing

c) Development of framework for information exchanging across the borders

6.3 Action Plan

Action Plan for Government

The following action item are for the government to take action:

a) Legalize this framework

b) Nominate chairman and Governing board members for NCRA

c) Release funds for NCRA

d) Continually monitor and improve the performance of NCA

References

1. https://www.pta.gov.pk/en/laws-&-policies/regulations
2. https://sahsol.lums.edu.pk/law-journal/prevention-electronic-crimes-act-2016-analysis
3. Personal data protection bill 2020, Pakistan Telecommunication Authority, laws-&-policies/regulations.
4. Electronic Data Protection Act 2015, Pakistan Telecommunication Authority, laws-&-policies/regulations.
5. https://www.secp.gov.pk/laws/acts/ Cybersecurity Framework for Insurance Sector 2019
6. Electronic Transection Ordinance 2002 (ETO) , Pakistan Telecommunication Authority, laws-&-policies/regulations.
7. Protection from SPAM, Unsolicited fraudulent and obnoxious communication Regulations, 2009 , Pakistan Telecommunication Authority, laws-& policies/ regulations.
8. Critical Telecom Data and Infrastructure Security Regulations, 2020, Pakistan Telecommunication Authority, laws-& policies/regulations.
9. Regulations | PTA National Cybersecurity Council Act, 2014
10. ECAC Information Security Auditors Registration Regulations 03.06.2008.pdf
11. National CYBER SECURITY POLICY 2021 (moitt.gov.pk)
12. National Center for Cyber Security | Pakistan (nccs.pk)
13. Pakistan introduces its first National Cyber Security Academy (techjuice.pk)
14. https://www.geo.tv/latest/383844-president-alvi-inaugurates-pakistans-first-ever-cyber-security-academy-in-islamabad
15. https://www.niais.org/about National Initiative for Artificial intelligence and Security
16. Presidential Initiative for Artificial Intelligence & Computing PIAIC

17. https://nr3c.gov.pk/index.html Nation Response Center for Cyber Crime

18. https://www.pisa.org.pk/public/Home/index Pakistan Information Security Association

19. International Telecommunication Union ITU Webinar: National Cybersecurity Strategies - Implementing and monitoring https://www.itu.int/en/ITU-D/Cybersecurity/Pages/2020-NCS-IM-webinar.aspx

20. Cybersecurity Framework https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

21. https://datatopics.worldbank.org/world-development-indicators/

22. https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map?selected=Estonia

23. https://cybersecurity.bsa.org/assets/PDFs/country_reports/cs_estonia.pdf

24. https://cybersecurity.bsa.org/assets/PDFs/country_reports/cs_estonia.pdf

25. CERT-EE | Estonian Information System Authority (ria.ee)

26. CAMP - Cybersecurity Alliance for Mutual Progress (cybersec-alliance.org)

27. Ministry of National Defence Republic of Lithuania :: News » News archives » News archive 2015 » News archive (2015 - 11) (kam.lt)

28. https://www.worldometers.info/world-population/australia-population/#:~:text=The%20current%20population%20of%20Australia,of%20the%20total%20world%20population.

29. https://www.homeaffairs.gov.au/cyber-security-subsite/files/cyber-security-strategy-2020.pdf

30. https://www.cyber.gov.au/acsc/view-all-content/glossary/cert-australia

31. https://www.cyber.gov.au/acsc/view-all-content/news/national-cyber-security-exercises-australias-electricity-industry

32. https://www.esafety.gov.au/sites/default/files/2021-07/Online%20Safety%20Act%20-%20Fact%20sheet.pdf

33. Cybersecurity strategy of Australia https://www.homeaffairs.gov.au/cyber-security-subsite/files/cyber-security-strategy-2020.pdf

34. https://datatopics.worldbank.org/world-development-indicators/

35. Global Cybersecurity Report 2018 GCI, ITU, https://www.itu.int/en/myitu/Publications/2021/06/28/13/22/Global-Cybersecurity-Index-2018

36. https://www.dsci.in/sites/default/files/documents/resource_centre/National%20Cyber%20Sec urity%20Strategy%202020%20DSCI%20submission.pdf

37. https://www.itu.int/pub/D-STR-CYB_GUIDE.01

38. Framework for the development of Computer Emergency Response Team in Pakistan, NUST Journal of Engineering Sciences, Vol. 10, No.2, 2017

39. https:// reports .weforum .org/ global -risks -report -2020/ executive -summary/

40. Dawn News NSA spy on Pakistan https://www.dawn.com/news/1279013

41. https://www.bluefin.com/bluefin-news/cyber-attacks-biggest-breaches-2018/

42. Dawn News https://www.dawn.com/news/1578882

43. https://propakistani.pk/2021/08/23/heres-a-recap-of-major-recent-cyber-attacks-in-pakistan/

44. Biannual report 2020 of Pakistan Telecommunication Authority PTA

45. World Population Review https://worldpopulationreview.com/countries/pakistan-population

46. Global Cybersecurity Report 2020 GCI, ITU, https://www.itu.int/en/myitu/Publications/2021/06/28/13/22/Global-Cybersecurity-Index-2020

47. https://www.meity.gov.in/content/national-cyber-security-policy-2013-1

48. https://www.icmec.org/wp-content/uploads/2016/09/UNICEF-Child-Protection-Online-India-pub_doc115-1.pdf

49. https://www.cert-in.org.in/

50. https://nciipc.gov.in/

51. Policy-makers | ITU-COP Guidelines (itu-cop-guidelines.com)

52. https://www.education.gov.in/en/sites/upload_files/mhrd/files/upload_document/revised_policy%20document%20ofICT.pdf

53. https://www.researchgate.net/publication/344840172_Italian_National_Framework_for_Cybersecurity_and_Data_Protection

54. https://www.sicurezzanazionale.gov.it/sisr.nsf/wp-content/uploads/2014/02/italian-national-strategic-framework-for-cyberspace-security.pdf

55. https://unidir.org/cpp/en/state-pdf-export/eyJjb3VudHJ5X2dyb3VwX2lkIjoiMTE0In0

56. https://www.ria.ee/sites/default/files/contenteditors/RIA/cyber_security_in_estonia_2020_0.pdf

57. https://www.cyber.gov.au/sites/default/files/2020-09/ASD-Cyber-Skills-Framework-v2.pdf

58. https://www.dpc.sa.gov.au/__data/assets/pdf_file/0017/126116/South-Australian-Cyber-Security-Framework.pdf

59. https://www.cyber.gov.au/sites/default/files/2021-12/02.%20ISM%20-%20Cyber%20Security%20Principles%20%28December%202021%29.pdf

60. Australian Information Security Manual 2021 https://www.cyber.gov.au/acsc/view-all-content/ism

61. https://www.cyber.gov.au/acsc/view-all-content/advice/cyber-security-principles

62. https://www.jstor.org/stable/pdf/resrep17311.8.pdf

63. National Initiative for Cybersecurity Education (NICE) NIST.800.181 https://www.nist.gov/itl/applied-cybersecurity/nice/nice-framework-resource-center

64. Workforce Framework for Cybersecurity (NICE Framework) https://csrc.nist.gov/publications/detail/nistir/8355/draft

65. https://www.nist.gov/system/files/documents/2021/09/29/FinalSlides_AwarenessWorkshop_28sep2021%20%28508%20Compliant%29.pdf