PTA

CYBER SECURITY ANNUAL REPORT 2022

www.pta.gov.pk

Acknowledgement

This report has been prepared by the Cyber Security Directorate of Pakistan Telecommunication Authority (PTA), led by Dr. Muhammad Mukaram Khan - Director General CVD. The chapters have been drafted by Mr. Ahmed Bakht Masood- Director Cybersecurity, Mr. Rafay Baloch - Senior Consultant Cybersecurity, Mr. Yousaf Haroon - Assistant Director Cybersecurity, Mr. Ghazanfar Abbas - Assistant Director Cybersecurity, Mr. Wasi Junaidi - Assistant Director Cybersecurity, Mr. Muhammad Nadeem - Assistant Director ICT and Mr. Kamran Khan - ITO CERT. The valuable guidance and directions given by Members of the Authority, led by PTA's Chairman, Maj. Gen. Amir Azeem Bajwa (R), were the primary inspiration behind the contents of this report.

Disclaimer

The information specified in this report has been designed to reflect the cyber security posture of Pakistan Telecommunication Authority (PTA) licensees in order to protect the national and user interests, in accordance with PTA's Critical Telecom Data and Infrastructure Security Regulation (CTDISR) 2020. Furthermore, this information serves as the basis for the Authority's right to inspect licensee organizations related to cyber security arrangements, critical data and infrastructure protection within the licensees' environment.

All information in this report is provided for information purposes only and unless otherwise specified does not constitute a legal contract between PTA and any person or entity. Although every reasonable effort is made to present current and accurate information, yet no guarantee is provided.

Published by

Pakistan Telecommunication Authority
Headquarters, F-5/1,
Islamabad, Pakistan
www.pta.gov.pk

PTA's VISION

"Create a fair regulatory regime to promote investment, encourage competition, protect consumer interests, and ensure high-quality ICT services."

TABLE OF CONTENTS

Purpose

The purpose of Cyber Security Annual Report is to highlight the initiatives of the Authority to uplift cyber security posture of the Telecom Industry and define parameters for assessing risks and prioritizing cyber security initiatives and track the overall progress of the industry. The spirit behind publishing this report is to ensure transparency and fair competition among the Licensees.

Background

Pakistan Telecommunication Authority (PTA) has been making efforts to bring substantial improvements in cyber security of critical telecom assets of Pakistan. In this regard, PTA published CTDISR in 2020, which is based on 16 Security Domains comprising 104 controls. To ensure that organizations can allocate requisite budget/ resources etc. to fulfill the obligations under CTDISR, PTA gave a grace period of 1 year to its licensees for confirming complete compliance. During this period, licensees had to fulfill obligations under CTDISR and conduct 3rd party audits from PTA's approved audit firms (an updated list is available at PTA's website).

Subsequently, PTA formulated Cyber Security Audit Criteria after consultation with the industry, in order to standardize the audit process. To ensure that, PTA's cyber security regulations (CTDISR) are implemented across the board in a uniform manner. PTA released National Telecom Cyber Security Framework-2022. The framework is based on CTDISR and defines the obligations of auditors and licensees. It provides guidance to the auditors for performing gap assessment. This includes interpretation and supporting documents against each clause of CTDISR, along with necessary compensating controls. Additionally, all controls have been classified based on defined Control Levels (CL1 to CL3) – CL1 being the basic level security control and CL3 an advanced level control with continuous improvements in accordance with their degree of criticality.

To ensure compliance against CTDISR, on the completion of 3rd party assessment by PTA's approved audit firms, PTA conducted a validation audit to ensure the quality of audit. PTA, in 2022, has conducted validation audits of top telecom operators, categorized based on customer base, size of network and license type etc. Since, the licensees are large in number, it is not possible to conduct validation audit of every licensee each year, however, PTA will try to validate audit of all major operators.

The Annual Report, on compliance survey of CTDISR, provides semi-anonymized and aggregated information about major telecom sector security incidents and compliance of CTDISR security controls.

1. Executive Summary

The cyber threat landscape has significantly grown over the past decade. This has required a high-level cooperation and joint proactive effort among all stakeholders, including all telecom operators, to detect, protect and mitigate the emerging cyber threats and offensive activities, including state-sponsored attacks, that would result in massive economic and reputational cost and would hinder the digital and technological growth of the nation. In pursuit to uplift the security posture of the Telecom Industry and building secure and resilient cyberspace for Pakistan, PTA's Cyber Security Directorate, after extensive deliberation and consultation with the Telecom Industry and leading cyber security experts, has taken many steps to uplift overall security posture of Telecom sector.

This report is being published to reflect the overall Cyber Security Index (CSI) of Pakistan Telecom Sector. It includes several cyber security initiatives to assess the cyber security readiness and resilience of telecom operators. This report highlights level of compliance, strong and weak areas, and overall ranking of its operators in accordance with CTDISR Domains. The report will also be published on the PTA's website to provide transparency to the customers about the importance that their service providers are giving to protect their personal data. This will also generate a healthy competition among the operators that will help in prioritizing cyber security in their respective organizations at the highest level.

CTDISR COMPLIANCE AUDIT HIGHLIGHTS

The Audit Revalidation of Licensee operators was conducted between January – September 2022.

The 2022 edition of Pakistan Telecommunication Authority Cyber Security Annual report is targeted to assess the nationwide Telecommunication Operators' cyber security posture in line with the CTDISR regulation. This includes audit revalidations from both "Large organizations" and "Small organizations". Organizations were chosen based on multiple factors including size of the network, number of licensees, type and category of licensees and number of customers being served.

CTDISR compliance audit validation activities by PTA Cyber Security Team started this year in January covering Cat-I and Cat-II operators. As per PTA's approved audit criteria, Cat-I comprises all CMOs and large fixed-line operators with multiple licenses, whereas Cat-II includes medium to large operators/ISPs.

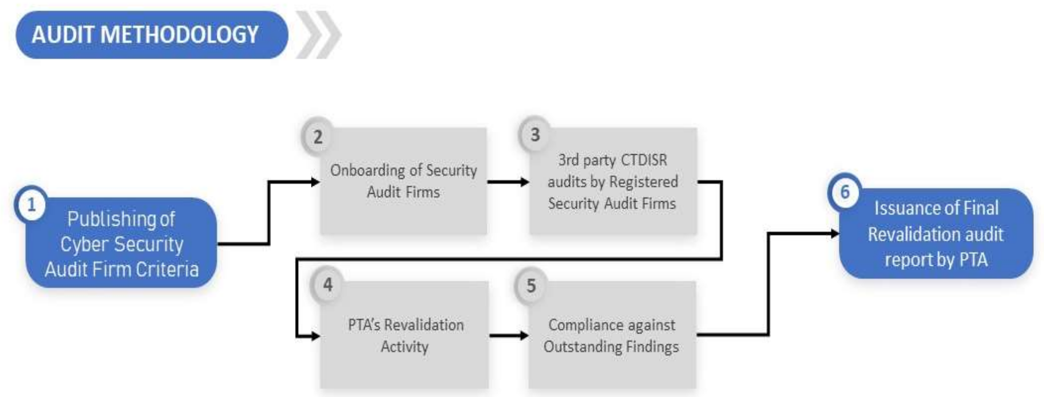
The audit-validation activity covered the audit of 15 major licensee, which was completed in September 2022, following complete CTDISR compliance audit process which is described in the section of "CTDISR Compliance Audit Process". Based on the validation audits of Cat-I and Cat-II operators, performed by PTA Cyber Security Directorate, overall rating of auditees has been performed to encourage the operators' efforts.

In the light of PTA's validation audit, Pakistan Mobile Communications Limited (PMCL) – Jazz has secured the highest percentage of compliance in Cat-I, followed by Telenor Pakistan as runner up. Whereas for Cat-II, Redtone has secured the highest compliance score, followed by Multinet.

Besides this, the report also covers major initiatives being taken by PTA to uplift security posture of Pakistan Telecom Sector as well as future initiatives that will help in shaping secure digital future and pave our way in refining future cyber security audits in subsequent years.

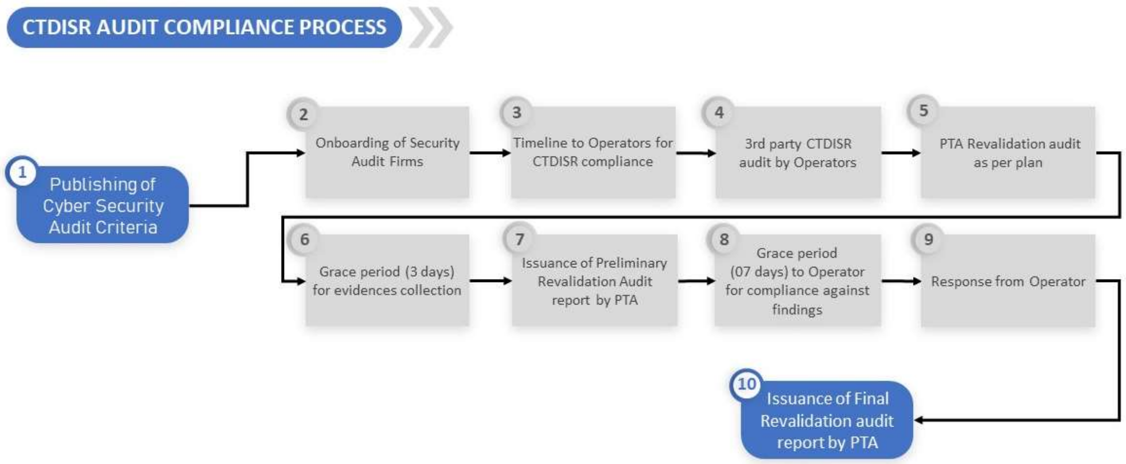
2. Audit Methodology

The process of CTDISR compliance audit is comprised of 6 steps, ranging from "Publishing of Cyber Security Audit Firms' Criteria" to Publishing of rankings as a part of the annual report.


AUDIT METHODOLOGY
1 Publishing of Cyber Security Audit Firm Criteria
2 Onboarding of Security Audit Firms
3 3rd party CTDISR audits by Registered Security Audit Firms
4 PTA's Revalidation Activity
5 Compliance against Outstanding Findings
6 Issuance of Final Revalidation audit report by PTA

2.1. End to End Process Flow of Audit

The following is detailed end to end process flow of complete audit activity:


CTDISR AUDIT COMPLIANCE PROCESS
1 Publishing of Cyber Security Audit Criteria
2 Onboarding of Security Audit Firms
3 Timeline to Operators for CTDISR compliance
4 3rd party CTDISR audit by Operators
5 PTA Revalidation audit as per plan
6 Grace period (3 days) for evidences collection
7 Issuance of Preliminary Revalidation Audit report by PTA
8 Grace period (07 days) to Operator for compliance against findings
9 Response from Operator
10 Issuance of Final Revalidation audit report by PTA

2.1.1. Audit Objectives

The overall objective of the CTDSIR audit is to validate the effectiveness of key controls as identified by the management and compliance with current policies and procedures relating to Information Technology / Information Security Controls and to identify any improvement opportunities.

The CTDISR audit documented the controls within this process that address the following objectives:

- Duties related to Information Technology and Information Security Function(s) process are segregated; and
- Controls are in place to support valid, accurate and timely processing of activities related to Information Technology / Information Security in accordance with the CTDISR.

2.1.2 Audit Approach

Broadly our audit approach includes:

- Interviews of key personnel of management and relevant technical staff.
- Performance of walkthroughs to corroborate the understandings of the process obtained through interviews.
- Review of design and effectiveness of controls installed to mitigate assessed risks to ensure that these Information Technology / Information Security controls are complying with the approved policies and procedures.
- Collecting feedback from the auditees to further improve regulations and framework.

2.2. Compliance Review Criteria

Following criteria was devised by PTA for conducting CTDISR audit validation:

Rating of the Report	Compliance Summary	Rating Explanation – Criteria	Risk Score
Unsatisfactory	Non-Compliant deficiencies noted in the CTDISR Compliance Review. Immediate corrective action required	Controls evaluated are not adequate, appropriate, or effective to provide reasonable assurance that compliance are being managed and objectives are met. Resolution of the weakness(s) would help avoid a potentially critical negative impact involving loss of material assets, customers' relationship, reputation, critical financial information, or ability to comply with the most important laws, policies, or procedures.	Between 50 to 60%
Needs Significant Improvements	Partially Compliant deficiencies noted in the CTDISR Compliance Review. Timely corrective action required.	A High residual risk exists in a major scope or risk area. The controls evaluated are unlikely to provide reasonable assurance that risks are being managed and objectives met.	Between 60% to 75%
Needs Minor Improvements	Adequate System of CTDISR Compliance Review. One or more Partially Compliant observations noted.	Generally, controls evaluated are adequate, appropriate, and effective to provide reasonable assurance that risks are being managed and objectives should be met. One or more moderate risk observations noted, with no major impact on the overall system of internal controls. Recommended control enhancements would improve the reliability of controls to support achievement of management's business objectives.	Between 75 – 90% with at-least one major non-compliance.
Satisfactory	Satisfactory Controls implemented.	Controls are operating effectively and can reliably support the achievement of management's business objectives.	90% above with no major non-compliance.

2.3. Assessment Scale and Scoring

Following is the assessment scale and scoring criteria, along with the action-plan's guidelines against each observation type:

Observation(s)	Observation Definition	Action Plan Guidelines
Non-Compliant	A key control does not exist, is poorly designed or is not operating as intended and the financial, operational and /or reputation risk is more than inconsequential. The process objective to which the control relates in unlikely to be achieved. Corrective action is needed to ensure controls are cost effective and/or process objectives are achieved.	Action plan to be implemented as a matter of urgency.
Partially Compliant	A key control does not exist, is poorly designed or in not operating as intended and the financial and /or reputation risk is more than inconsequential. However, a compensating control might exist. Corrective action is needed to avoid sole reliance on compensating controls and/or ensure controls are cost effective.	Action plan to be implemented. Expected to be implemented in no later than 3 months.
Compliant	Controls are operating effectively and can reliably support the achievement of management's business objectives.	No action plan is needed.

–

2.4. CTDISR Compliance Audit Scoring Criteria

Following scoring criteria was used to determine the “Report Rating” after the PTA’s validation activity:

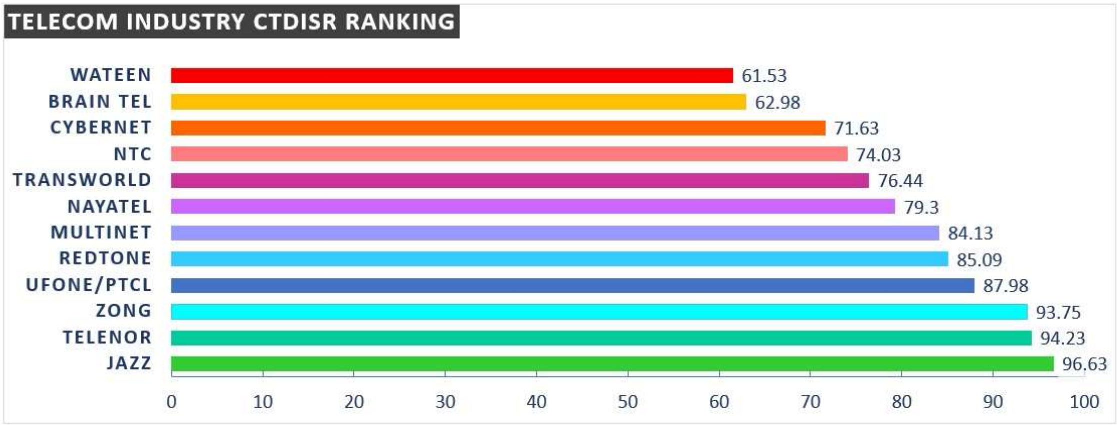
Score	
Non- Compliant	0
Partially Compliant	0.5
Compliant	1

3. Nationwide Outlook – Telecom Cyber Security Index

As a result of CTDISR compliance audit validation by PTA, following is the ranking of the auditees based on the compliance scoring scheme and commitments shown by the licensees towards the cyber security readiness:

PTA Licensee	Assigned Category	CTDISR Compliance Ranking
Jazz	Cat-I	1
Telenor		2
ZONG		3
Ufone/PTCL		4
RedTone	Cat-II	5
Multinet		6
Nayatel		7
Transworld	Cat-I	8
NTC		9
Cybernet	Cat-II	10
Brain Tel		11
Wateen		12

Following graph represents the overall compliance percentage:



In terms of individual category, **Pakistan Mobile Communications Limited (PMCL)** - **Jazz** has secured the highest compliance percentage in Cat-1, whereas for Cat-II **RedTone** has secured highest compliance percentage after PTA's validation audit.

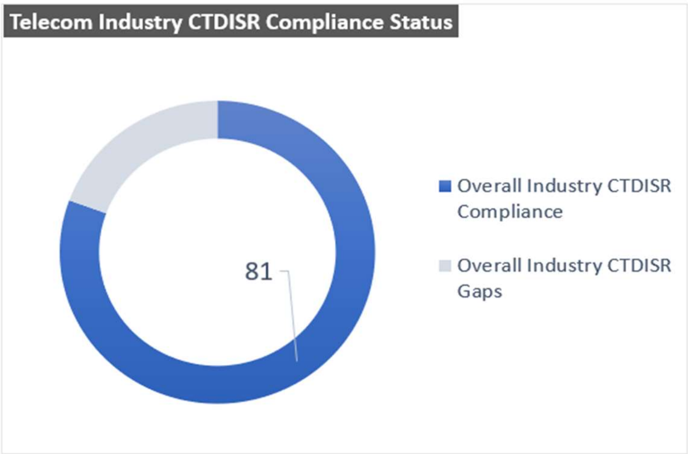
PTA Licensee	CTDISR Compliance Ranking	Assigned Category
Jazz	1	Cat-I
Telenor	2	Cat-I
ZONG	3	Cat-I
Ufone/PTCL	4	Cat-I
Transworld	5	Cat-I
NTC	6	Cat-I

PTA Licensee	CTDISR Compliance Ranking	Assigned Category
RedTone	1	Cat-II
Multinet	2	Cat-II
Nayatel	3	Cat-II
Cybernet	4	Cat-II
Brain Tel	5	Cat-II
Wateen	6	Cat-II

3.1. Telecom Industry Overall CTDISR Compliance Score

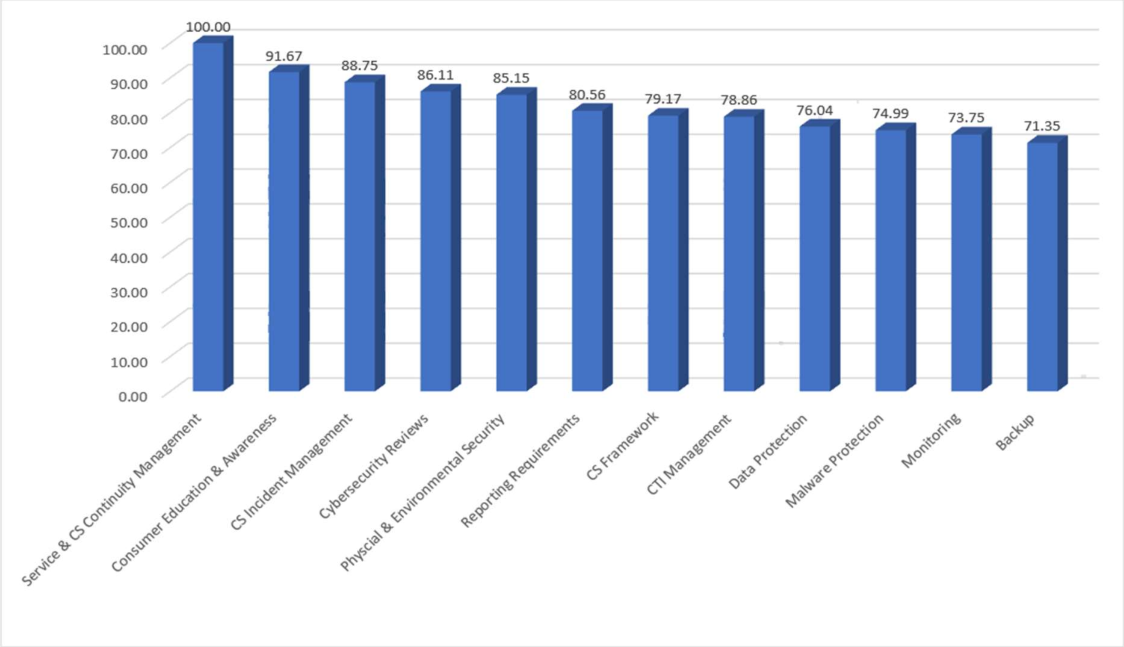
With cybersecurity receiving the central focus globally, it is imperative that all telecom operators comply with the requirements of CTDISR to protect critical telecom data and infrastructure, and stay ahead of other sectors in providing safe experience to telecom users while proactively combating against latest and advanced incoming cyber security challenges.

Based on the validation audits of Cat-I and Cat-II licensee, overall Telecom Industry compliance status is as follows:



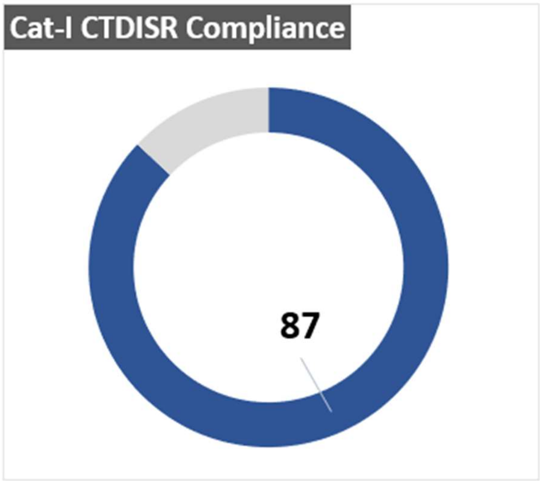
3.2. CTDISR Domain-wise Compliance

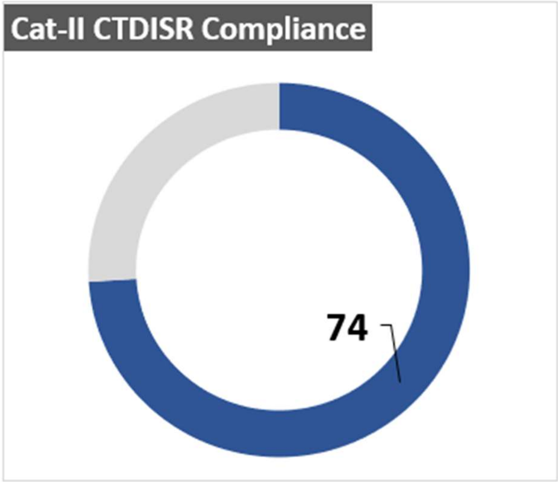
Domain-wise compliance status is as follows – ranging from strongest to the weakest domain in terms of the overall compliance level:



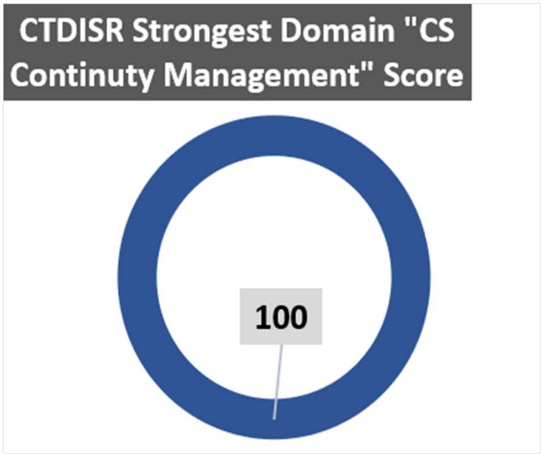
3.3. Category-wise CTDISR Compliance Score

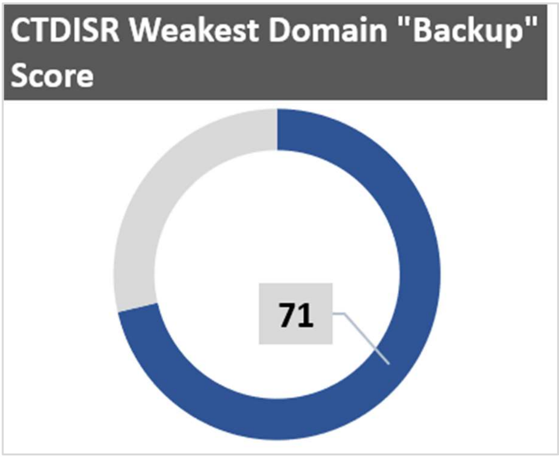
The following graphs illustrate Category-wise compliance score:





Following graphs show score of the strongest and weakest domains:





4. Cyber Security Readiness Through Continuous Security Posture Assessments

For Cyber Security Readiness, efficacy and efficiency of security controls implemented by the licensees were assessed through various parameters, including external security posture assessments by PTA, participation in PTA CERT portal coordination, and compliance against PTA's cyber security advisories.

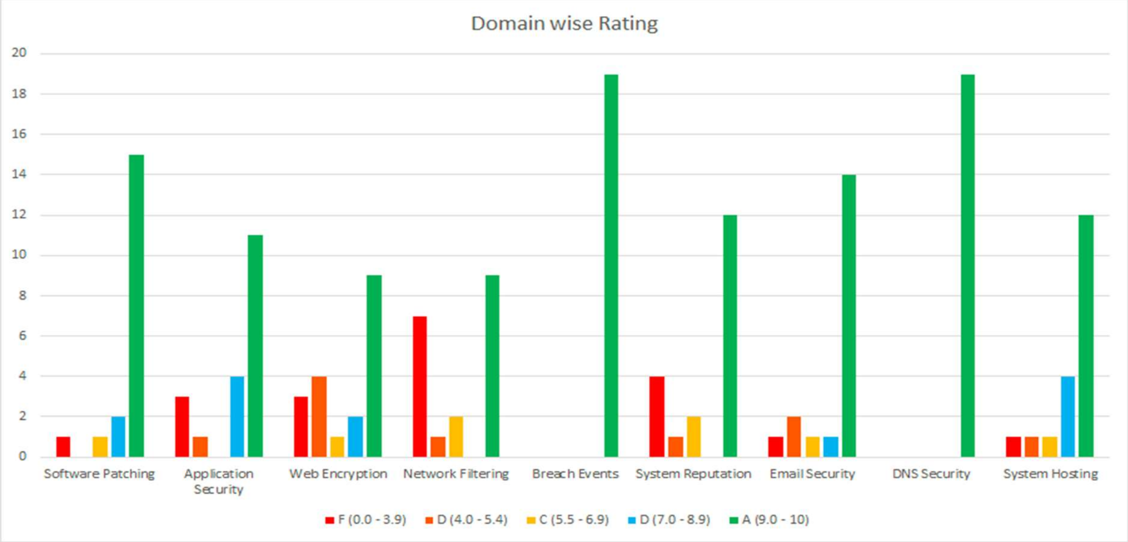
4.1. External Security Posture Assessment

To combat evolving and sophisticated cyber threats, it is important to conduct continuous external CS posture assessments to proactively detect threats and take measures to mitigate their effect. For this purpose, PTA is performing weekly non-intrusive vulnerability assessment and penetration testing exercise using tools such as RiskRecon (ex. MasterCard) and shares its report with the telecom operators to bridge the gaps. This is in alignment with PTA's strategy of securing the cyber space of telecom sector with a blend of AI and data-driven advanced technologies.

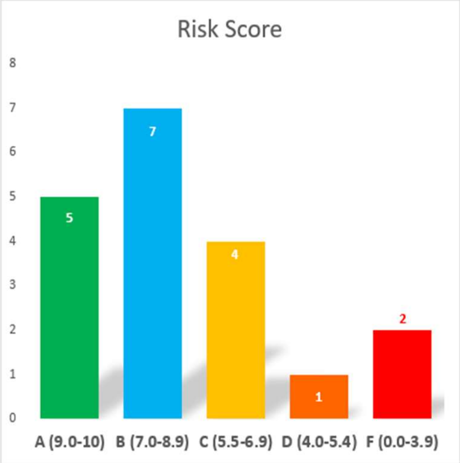
For this purpose, PTA's weekly scan of publicly exposed assets of PTA's licensees, analyses the CS posture of each licensee in terms of 39 critical CS parameters such as Software Patching, Application Security, Web Encryption, Network Filtering, Breach Events, System Reputation, Email Security, DNS Security, and System Hosting etc. Details against these categories can be found in **Annex-A**.

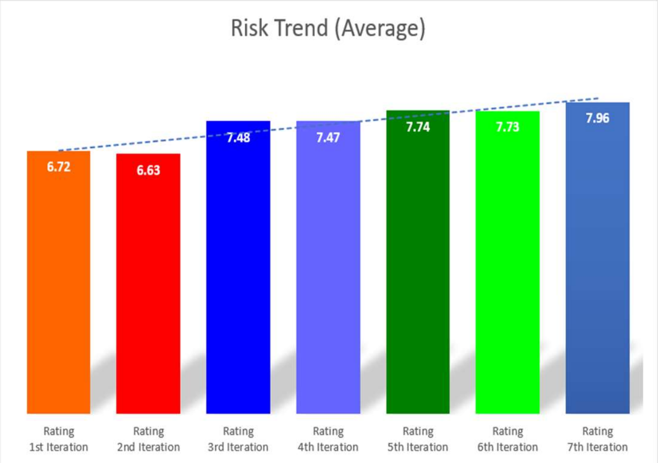
Following graph shows the domain wise rating of publicly exposed assets of licensees in scope:

Domain	F (0.0-3.9)	D (4.0-5.4)	C (5.5-6.9)	B (7.0-8.9)	A (9.0-10)
Software Patching	1	0	1	2	15
Application Security	3	1	0	4	11
Web Encryption	3	4	1	2	9
Network Filtering	7	1	2	0	9
Breach Events	0	0	0	0	19
System Reputation	4	1	2	0	12
Email Security	1	2	1	1	14
DNS Security	0	0	0	0	19
System Hosting	1	1	1	4	12



PTA performed 7 Iterations of this non-intrusive scanning of public-acing assets of its licensees to assess the cyber security readiness of the telecom industry. During, the 1st Iteration the overall industry's CS risk score was **6.72/10,** which improved to **7.96/10** after the 7th iteration. The graph below highlights the overall risk scoring of the telecom industry





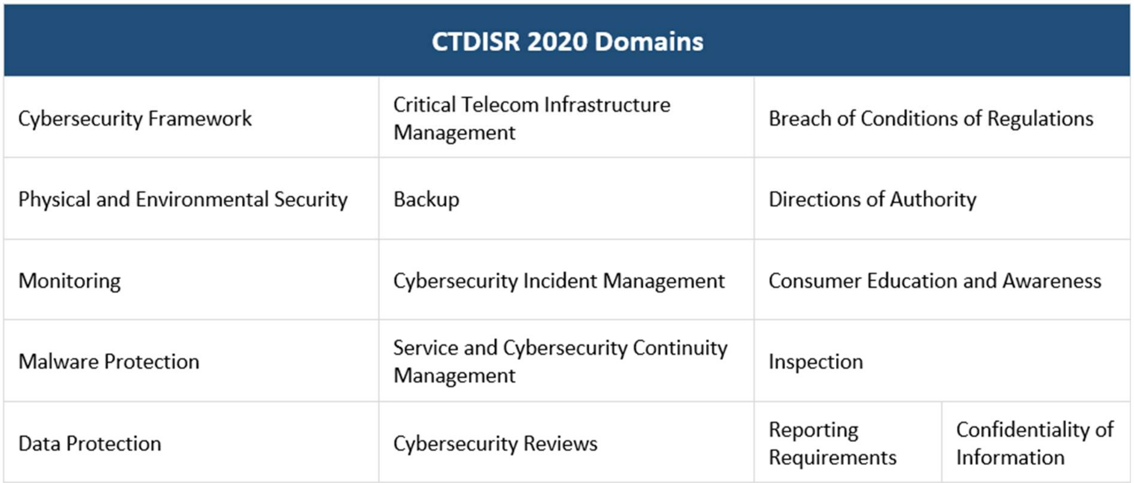
5. PTA Cyber Security Initiatives

Keeping in view the emerging cyber security threats and enabling cyber security resilience in telecom sector, PTA has initiated several cyber security initiatives, such as:

5.1. CTDISR - Cyber Security Regulation

PTA published the CTDISR in November 2020. To ensure that telecom operators can plan well and allocate requisite budget/ resources etc., PTA gave a grace period of one year to its licensees to comply with these regulations. During this period, licensees had to fulfil all obligations and conduct a third-party audit from PTA's approved audit firms. There are 16 domains and 104 security controls in CTDISR covering mandatory and essential cyber security requirements for ensuring resilient and mature security landscape of our telecom sector.

Following is a list of the CTDISR domains:



CTDISR 2020 Domains			
Cybersecurity Framework	Critical Telecom Infrastructure Management	Breach of Conditions of Regulations	
Physical and Environmental Security	Backup	Directions of Authority	
Monitoring	Cybersecurity Incident Management	Consumer Education and Awareness	
Malware Protection	Service and Cybersecurity Continuity Management	Inspection	
Data Protection	Cybersecurity Reviews	Reporting Requirements	Confidentiality of Information

5.2. Cyber Security Audit Firms Registration Criteria

PTA has formulated a well-defined process of registering cyber security firms interested in carrying out third party audit of telecom operators following a well-defined qualification criterion in order to facilitate its licensees in CTDISR audit compliance. Subsequently, PTA formulated cyber security audit criteria (**Annex-B**) after consultation with the industry, to standardize the audit firms' audit process.

The approved criteria has three minimum baselines as under:

- Mandatory Minimum Baseline Criteria for the Audit Companies.
- Mandatory Minimum Baseline Criteria for Individual Resources
- General Rules for Cyber Security Audit Firms

5.3. Onboarding of Cyber Security Firms

Cyber security audit firms have grown to a reasonable number in Pakistan. PTA issues yearly timelines to its licensees for conducting 3rd party CTDISR compliance audits. For this purpose, PTA has formulated a process of onboarding/registering Cyber security audit firms following "Cyber Security Audit Firms Criteria" after going through extensive due-deliberation and consultation process with telecom operators and renowned cyber security audit firms. Such firms can submit their applications to PTA and get themselves registered after a due diligent process of document verification and capacity assessment, after which these can be assigned to their respective categories.

5.4. Categorization of Licensee

For the 3rd party audit, all the licensees are divided into 4 categories based on their infrastructure, user-base, service-profile and revenue etc. Cat-I comprised of CMO's and large operators with multiple licenses, Cat-II comprised of large operators, Cat-III comprised of medium size LDI operators and Cat-IV includes small operators.

Licensees' mapping to their respective categories with the corresponding security audit firms' criteria can be found at **Annex-C**.

5.5. Category Allocation of Cyber Security Audit Firms

Similar to the operators' categorization, PTA has categorized the cyber security firms into 4 categories on the basis of "**Cyber Security Audit Firms Criteria**" with a purpose to allow its licensees to get their 3rd party audit from a cyber security audit firm capable in expertise and capacity commensuration the size of the telecom operator.

Based on the Cyber Security Audit Firms Criteria, following is the current list of firms listed in accordance with their categories. This list will be continuously updated, as new security firms are approved or categories of existing firms are reviewed. Similarly, existing firms can also elevate their category by furnishing new evidence.

Category Allocated	Security Audit Firm	Email Address	Point of Contact
Cat-I	**Ebryx**	ali.shahbaz@ebryx.com	Mr. Ali Shahbaz
Cat-I	**EY**	imran.saeed@pk.ey.com	Mr. Imran Saeed
Cat-I	**Risk Associate**	kashif.hassan@riskassociates.com	Mr. Kashif Hassan
Cat-I	**Trillium**	aniqa.fareed@infosecurity.com.pk	Ms. Aniqa Fareed
Cat-I	**SGS Pakistan**	waqas.awan@sgs.com	Mr. Waqas Awan
Cat-I	**BDO**	sshah@bdo.com.pk	Mr. Shoukat Shah
Cat-II	**Compliance wing**	syed.saad@compliancewing.com	Mr. Syed Muhammad Saad
Cat-II	**Eunomatix**	farooq@eunomatix.com	Mr. Muhammad Farooq
Cat-II	**Mutex Systems**	samihaider@mutexsystemsltd.com	Mr. Sami Haider
Cat-II	**Veiliux**	safina@veiliux.com shahmeer@veiliux.com	Ms. Safina, Mr. Shahmeer
Cat-II	**YLinx**	muhammad.kashif@ylinx.pk	Mr. Muhammad Kashif
Cat-II	**Horizon Tech**	pmo@horizon.com.pk	Horizon Tech
Cat-II	**Security Experts**	sidra@securityexperts.com.pk	Ms. Sidra
Cat-II	**Xcelliti**	kashif.jamil@xcelliti.com	Mr. Kashif Jamil
Cat -II	**Cansol Consulting**	azfarbaig@cansolconsulting.com	Mr. Azfar Baig
Cat-III	**Catalyic Consulting**	info@catalyic.com	Catalyic Consulting
Cat-III	**Cyberisk**	atif@cyberisk.com.pk	Mr. Atif Abro
Cat-IV	**CyberShell**	tayyaba_nafees@cybershellsol.com	Ms. Tayyaba

It is significant to mention that, as per approved cyber security audit criteria, audit firms can perform the audit of their respective categories or below in the hierarchy. For example, firms qualifying for Cat-I can also perform security audits of licensees falling under Cat-II to Cat-IV. Similarly, firms qualifying for Cat-II, can also perform audit of Cat-III and Cat-IV, however, it cannot perform audit of licensees upward in the hierarchy i.e., Cat-I.

5.6. National Telcom Cyber Security Framework for Telecom

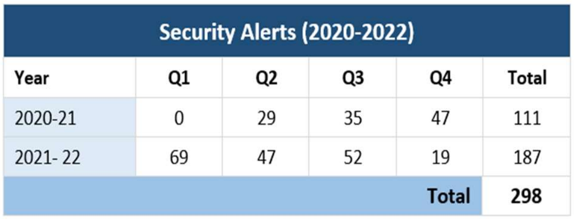
To ensure that, PTA's cyber security regulations (CTDISR) are uniformly implemented across the board. PTA released the "National Telecom Cyber Security Framework" in 2022. The framework is based on CTDISR regulation and defines the obligation of auditors and licensees. It guides auditors in performing gap assessment. This includes interpretation and supporting documents against each clause, along with necessary compensating controls. Additionally, all controls have been classified based on Control

Levels (CL1 to CL3), where CL1 is the basic security control while CL3 is an advanced level control with continuous improvements following its degree of criticality.

Module activities focus on defining and establishing processes to identify, analyze and manage Telecom-specific risks to licensee's critical infrastructure and data (CTI&CTD) to ensure smooth functioning of essential information/ communication systems under ordinary circumstances and their continuity on a minimum level during critical situations.

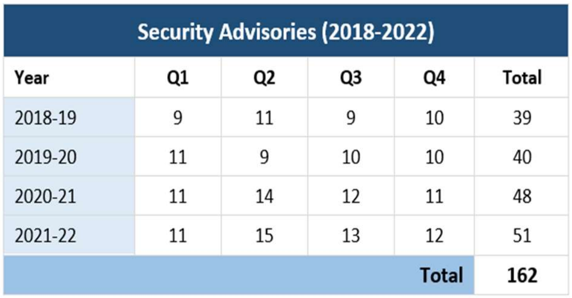
5.7. PTA Computer Emergency Response Team (CERT) Private Portal

PTA has introduced a private CERT portal for its licensees in 2021, in continuation to its efforts to improve security posture of Pakistan Telecom Sector and to protect and safeguard National Critical Telecom Data and Infrastructure. PTA is in a process of establishing National Telecom CERT (nTCERT) with a dedicated National Telecom Security Operations Centre (nTSOC) to continuously monitor CTI&CTD in real time and respond to cyber incidences. The CERT Portal will be integrated with the nTCERT/ nTSOC. This initiative will enable PTA and its licensees to share Threat Intelligence with each other to achieve regulatory compliance of PTA cyber security regulations.



Security Alerts (2020-2022)

Year	Q1	Q2	Q3	Q4	Total
2020-21	0	29	35	47	111
2021- 22	69	47	52	19	187
				Total	298



Security Advisories (2018-2022)

Year	Q1	Q2	Q3	Q4	Total
2018-19	9	11	9	10	39
2019-20	11	9	10	10	40
2020-21	11	14	12	11	48
2021-22	11	15	13	12	51
				Total	162

This portal has been established after close coordination and input from the telecom operators. Primarily, this portal will facilitate information sharing and exchange between PTA and telecom service providers on latest cyber security threats, incidents, vulnerabilities, security news and other related information. Continual improvements in the portal are being carried out based on operational requirements.

PTA shares cyber security advisories, latest threats and security vulnerabilities through its CERT Portal. Furthermore, licensees also share their threat intelligence with PTA and other operators through the same CERT Portal, shared with overall industry.

5.8. Cyber Security Early Warnings and Surprise Visits

PTA has been actively collaborating with local security companies, threat intelligence partners and its operators to proactively assess security risk and has been taking measures for improving the cyber security readiness and resilience of telecom operators. Based on trend analysis, PTA keeps issuing special early warnings, security alerts and advisories to telecom industry on special occasions, especially national/ religious days etc. On such occasions, PTA also plans to conduct surprise visits/ audits to evaluate readiness level of our operators' cyber security teams.

5.9. National Telecom Computer Emergency Response Team (nTCERT) Public Portal

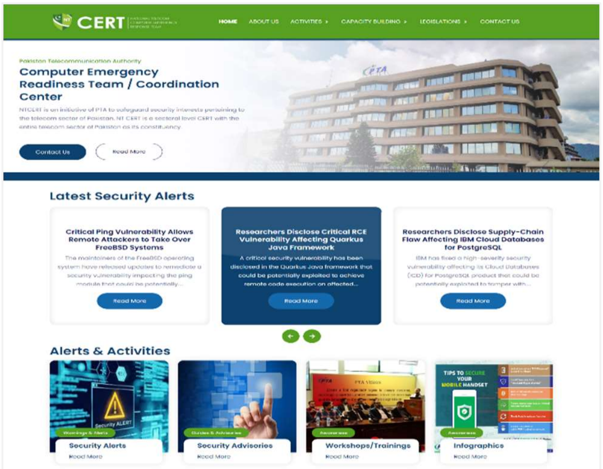
In order to extend cyber security support to general public, PTA launched a public portal of nTCERT in 2022 with the following objectives:

- Sharing latest security advisories and alerts with the general public.

- Awareness messages on safe usage of the Internet services.
- Information on capacity-building initiatives and workshops.
- Latest information regarding CTDISR.
- Public feedback on emerging threats and suggestions for improvement.
- An interface to the general public for sharing any threat intelligence information.

5.10. Capacity Building & Awareness

PTA collaborates with various national and international organizations, such as ISOC, PKSIG, APNIC, ITU etc. to arrange online and face-to-face trainings for the telecom industry and other related organizations. PTA keeps developing and issuing various infographics to raise public awareness and apprise end-users of the security measures that they can take to recognize and respond to threats and scams on social media.



Pakistan Telecommunication Authority

Computer Emergency Readiness Team / Coordination Center

NTCERT is an initiative of PTA to safeguard security interests pertaining to the telecom sector of Pakistan. NT CERT is a sectoral level CERT with the entire telecom sector of Pakistan as its constituency.

Latest Security Alerts

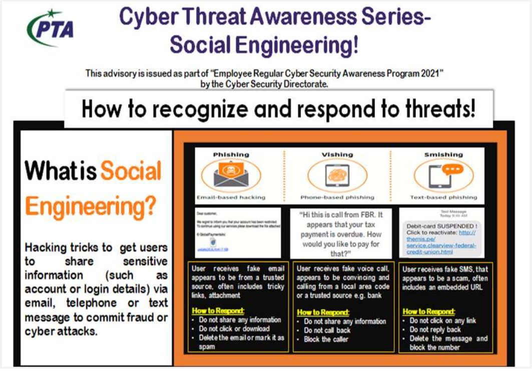
Critical Ping Vulnerability Allows Remote Attackers to Take Over FreeBSD Systems
The maintainers of the FreeBSD operating system have released updates to remediate a security vulnerability impacting the ping module that could be potentially...

Researchers Disclose Critical RCE Vulnerability Affecting Quarkus Java Framework
A critical security vulnerability has been disclosed in the Quarkus Java framework that could be potentially exploited to achieve remote code execution on affected...

Researchers Disclose Supply-Chain Flaw Affecting IBM Cloud Databases for PostgreSQL
IBM has fixed a high-severity security vulnerability affecting its Cloud Databases (ICD) for PostgreSQL product that could be potentially exploited to tamper with...

Alerts & Activities

Warnings & Alerts
Security Alerts
Read More
Guides & Advisories
Security Advisories
Read More
Awareness
Workshops/Trainings
Read More
Awareness
Infographics
Read More
TIPS TO SECURE YOUR MOBILE HANDSET



Cyber Threat Awareness Series-
Social Engineering!

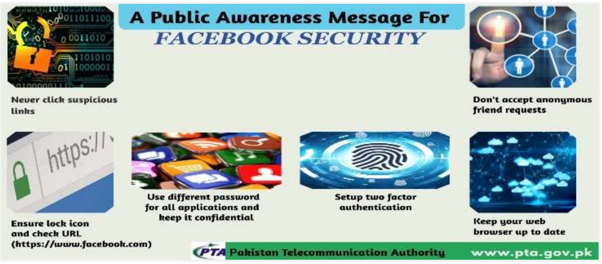
This advisory is issued as part of "Employee Regular Cyber Security Awareness Program 2021" by the Cyber Security Directorate.

How to recognize and respond to threats!

What is Social Engineering?

Hacking tricks to get users to share sensitive information (such as account or login details) via email, telephone or text message to commit fraud or cyber attacks.

Phishing	Vishing	Smishing
Email-based hacking	Phone-based phishing	Text-based phishing
	"Hi this is call from FBR. It appears that your tax payment is overdue. How would you like to pay for that?"	Debit-card SUSPENDED ! Click to reactivate: http://themis.pe/service.clearview-federal-credit-union.html
User receives fake email appears to be from a trusted source, often includes tricky links, attachment	User receives fake voice call, appears to be convincing and calling from a local area code or a trusted source e.g. bank	User receives fake SMS, that appears to be a scam, often includes an embedded URL
How to Respond: • Do not share any information • Do not click or download • Delete the email or mark it as spam	How to Respond: • Do not share any information • Do not call back • Block the caller	How to Respond: • Do not click on any link • Do not reply back • Delete the message and block the number



A Public Awareness Message For
FACEBOOK SECURITY

Never click suspicious links

Don't accept anonymous friend requests

Ensure lock icon and check URL (https://www.facebook.com)

Use different password for all applications and keep it confidential

Setup two factor authentication

Keep your web browser up to date

Pakistan Telecommunication Authority www.pta.gov.pk

6. Way Forward & Future Plans

PTA is making all out efforts to improve security of critical telecom assets of Pakistan. In this regard, some new initiatives are in progress to improve and uplift the cyber security posture of telecom sector.

6.1. CTDISR Control Level Compliance

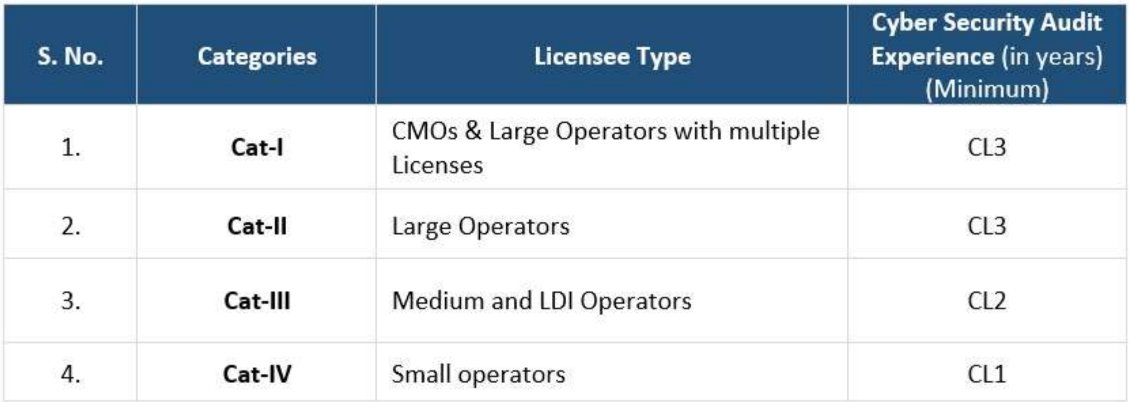
Since, the National Telecom Cyber Security Framework is based on CTDISR and defines obligation of auditors and licensees, it provides guidance to auditors for performing gap assessment in the light of the CTDISR. This includes interpretation and supporting documents against each clause along with necessary compensating controls. Additionally, all CTDISR controls have been classified based on Control Levels (CL1 to CL3) with CL1 being basic security control and CL3 with advanced with continuous improvements.

National Telecom Cyber Security Framework has defined three maturity levels based on the complexity of the controls:

a. **Control Level 1 (CL1)**: **CL1** includes basic security requirements and controls.
b. **Control Level 2 (CL2): CL2** includes advanced security requirements and controls in addition to the existing requirements within CL1.

c. **Control Level 3 (CL3): CL3** includes requirements and security controls that are more focused on continuous monitoring and continuous process improvements to controls/requirements defined in **CL1** and **CL2** to achieve compliance with a higher level, compliance with all preceding levels is required.

Since, Control Level 3 comprises of advanced controls which require higher level of organization's maturity, PTA has mapped Control Levels in accordance with the categories of licensees. Following is mapping of licensee categories against respective control levels. Detailed table of individual licensee mapping can be found under **Annex-D**.



S. No.	Categories	Licensee Type	Cyber Security Audit Experience (in years) (Minimum)
1.	**Cat-I**	CMOs & Large Operators with multiple Licenses	CL3
2.	**Cat-II**	Large Operators	CL3
3.	**Cat-III**	Medium and LDI Operators	CL2
4.	**Cat-IV**	Small operators	CL1

6.2. CTDISR Audit Plan for 2023

In addition to the National Telecom Cyber Security Framework and in pursuit of the mission of PTA for uplifting the security posture of the Telecom Industry and achieving secure and resilient Pakistan's cyberspace considering the continual security improvement aspect, PTA has issued deadline of April 2023 for completing 3rd party CTDISR audits by all licensees for their mandatory compliance.

6.3. National Telecom CERT/SOC

PTA is establishing nTCERT and nTSOC to coordinate CTI&CTD security and resilience efforts across nationwide telecom operators using trusted partnership and cooperation among all public/ private stakeholders. Following are the main components of nTSOC:

- Security Information and Event Management (SIEM), integrated with all major Telecom Operators' SIEMs and critical assets of Telecom Sector to form a unified security monitoring system to provide oversight of national cyber defense.
- Threat Intelligence Platform (TIP), integrated with trust global threat intelligence feeds upward and with the TIPs deployed by telecom operators downward to share alerts about the threats/incidences and advising about best remedial measures.
- Building case management tools for industry regulatory compliance.
- Providing context-aware real-world risk assessment and incident analysis to the constituency.
- Forensic lab to investigate incidences taking place in the telecom sector.
- Developing Human capability including skilled and certified workforce to manage SOC/CERT operations (L2/3 analysts, system/NW experts for generating/coordinating response, Deep Analysis team to carry out analysis of new threats with the help of labs with academia and other relevant stakeholders)
- Supporting small sized operators in deploying cost effective security solutions to integrate their NWs with PTA's unified platforms and meet compliance.

6.4. Revamping of nTCERT Portal

PTA has introduced the private CERT portal in 2021 for its licensees, in continuation to its efforts to improve security posture of Pakistan Telecom Sector and to protect and safeguard National Critical Telecom Data and Infrastructure. This initiative will enable PTA and its licensees to share Threat Intelligence with each other to achieve regulatory compliance of PTA Cyber Security regulations.

This portal has been established after close coordination and input from the telecom operators. Primarily, this portal is facilitating information sharing between PTA and telecom service providers on latest cyber security threats, incidents, vulnerabilities, security news and other related information. Continual improvements in the portal will be carried out based on operational requirements.

With the goal to enhance capacity, capability, and effectiveness of nTCERT, PTA will take the following steps:

- Integrating this portal with own TIP and other global CERTs such as AP CERT, FIRST CERT, Pakistan’s National CERT nCERT, and other national CERTS for sharing of threat intelligence, advisories and security alerts and ensure active participation in these forums.
- Automating CERT functions with proactive and reactive actions, such as real-time email/SMS notifications, advisory attachments in alerts and incident forwarding.
- CTDISR Survey form & Statistics/Graphs Logging of user activities in Portal.
- Integration with ticketing systems and CTI/CTD pipeline for DevOPs environment.

ANNEXURES

Annex-A

External Posture Security Assessment Domains

Domain Rating	Description
Breach Events	The Breach Event domain summarizes the breach events the organization has experienced. Recent breach events indicate gaps in the breach events protection program.
Software Patching	Enumerates systems that are running end-of-life and vulnerable software. Because end-of-life software is not supported by the vendor, it cannot be patched against known security issues or new vulnerabilities that might be discovered, increasing likelihood of system compromise.
Web Encryption	RiskRecon used passive techniques to analyze web encryption security configurations. Correctly configured web encryption is essential to ensuring that communications are protected from eavesdropping and that people can verify the authenticity of the system.
DNS Security	The DNS Security domain assesses the use of controls to prevent unauthorized modification of domain records resulting in domain hijacking. This domain also enumerates the DNS hosting providers to determine level of fragmentation.
Email Security	The Email Security domain analyzes the security configuration of email services.
System Hosting	The System Hosting domain provides insight into the Internet attack surface of the company, detailing the number of systems, the system hosting providers, and the system geolocations. How the organization has instantiated its internet presence is a driver of the complexity of managing IT security, privacy, and regulatory risk.
System Reputation	The System Reputation domain enumerates systems owned by the company that are communicating with monitored C2 servers, sinkholes, honeypots, or are exhibiting other hostile activity. The presence of the organization's assets in threat intelligence feeds is an indicator of lack of consistent and effective security controls deployed to all systems necessary to prevent malware infection and system abuse.
Application Security	The Application Security domain assesses each discovered web application for compliance with widely accepted application security practices that can be assessed using passive techniques. Consistent deployment of web application security controls appropriate for the risk context of the system is important to defend against application-level attacks.
Network Filtering	Analyzes company networks and systems for the presence of unsafe network services and IoT devices. Proper control of the services exposed to the Internet is a basic security practice, as unsafe network services and IoT devices are a common vector for compromising systems and networks.

Annex-B

Cyber Security Audit Firm Registration Criteria

Audit Firm Registration Criteria		
Scope: This policy is applicable for companies/firms conducting Cyber Security audits/Penetration Testing/Red Teaming engagements across infrastructure/information systems of PTA's Licensees.		
A	**Mandatory Minimum Baseline Criteria for Company**	
1	Taxpayer	Active Taxpayer + Sales tax registration
2	Registration	SECP
3	Incorporation Time	1 year
4	Grace Period Timeline	March 2022
5	Audits Experience	2 Cyber Security Audit/Pentesting/Red Teaming projects of similar scope/project size of relevant category.
6	Company Profile & Documentation	As defined in section C
7	No. of Technical Resources	Minimum two (02)
8	No. of Certified Resources	Cyber Security audit firm should have at least two (02) certified, permanent technical employees, each having relevant security certification, from at least two (02) of the following bodies: ISACA, (ISC)^2, SANS, EC-Council and Offensive Security, ISO
B	**Mandatory Minimum Baseline Criteria for Individual Resource**	
1	Qualifying Certification Bodies	ISACA, (ISC)2, EC-Council, Offensive Security, SANS, ISO
2	Cyber Security Auditing Experience	2 years
3	Pentesting Experience	2 years
4	Certifications	At least two (02) certified resources from qualifying certification bodies ISACA, (ISC)^2, SANS, EC-Council, Offensive Security
5	Association with Company as a permanent employee	6 months
C	**General Rules for Cyber Security Audit Firms**	
1	Cyber Security audit firm should be registered with SECP or relevant Registrar of firms. Company/firm should appear Active Taxpayer list (ATL) of income and sales tax issued by FBR.	
2	Cyber security audit must not be performed by a subsidiary/affiliate/associate firm of the Licensee in order to avoid conflict of interest.	
3	Cyber Security Audit Firm should not outsource its Cyber security auditing/pentesting/red teaming engagement to any foreign 3rd party assessor, auditor and audit firm.	
4	Foreign companies having their local representation Branch office in Pakistan can also apply, subject to registration with SECP and FBR or relevant registrar of firms in Pakistan.	
5	Cyber Security audit Firm should not be a blacklisted firm/company in Public/Private sector within Pakistan or abroad, due to any factor including but not limited to unsatisfactory performance, breach of general/specific instructions or NDA, corrupt practices and/or any fraudulent activity.	
6	Cyber Security audit firms can perform audit of their respective categories or downward in the hierarchy. For instance, firms qualifying for Cat-I, can also perform audit of licensees falling under	

	Cat-II to Cat-V, similarly, firms qualifying for Cat-II, can also perform audit of Cat-III to Cat-V, however, firms qualifying for Cat-V cannot perform audit of licensees upward in the hierarchy i.e. Cat-IV to Cat-I.
7	Cyber security audit firm should have documented policies and procedures including but not limited to Information Security processes and procedures, Personnel security and development.
8	While assessing the cyber security audit firm, PTA may review several key areas of discipline including but not limited to assessment methodology, profiles of certified individuals/resources, data storage and retention policies, Information sharing policy and procedure, Tools and reporting methodology.
9	Upon being listed under Cyber Security Audit Firm's approved list, PTA reserves the right to conduct a full assessment at any given point of time, which may require re-submission of all relevant documents submitted at the time of registration or any other additional document which may be required for additional scrutiny.
10	In case of violation of any clause in the NDA by the approved Cyber Security Audit Firm, licensee is mandated to provide information including necessary details to PTA. In that case, PTA reserves the right to terminate the membership of the Cyber Security Audit Firms and initiate legal proceedings wherever necessary. In case of termination of membership, prior intimation shall be provided to all the licensees and duly updated on the website.
11	List of approved Cyber security audit firms will be published on PTA website and would be updated on regular basis.
12	PTA reserves the right to revise Cyber Security Audit Firm Registration Criteria at any given point of time on need basis. Licensees shall be apprised prior to revision of this criteria.

Annex-C

Licensee Categorization and Audit Firm Mapping

S. No.	Categories	Licensee Type	Licensee/ Telecom Operators	Cyber Security Audit Experience (in years) (Minimum)	No. of Permanent Technical Resources (Minimum)	No. of Technical Resources Certification (Minimum)
1.	**Cat-I**	CMOs & Large Operators with multiple Licenses	Ufone, Telenor, JAZZ, ZONG, PTCL, TWA, SCO, NTC	**6**	**7**	**7**
2.	**Cat-II**	Large Operators	Brain Telecom, Comsats Internet Services, Connect Communications, Cyber Internet Services, Fariya, KK networks, LinkDotNet, Master Communication, Multinet, Nayatel, REDtone, Wateen Telecom, Web Concepts, Wi-Tribe	**4**	**5**	**5**
3.	**Cat-III**	Medium and LDI Operators	DV Com Data, 4B Gentle, 7 Star telecom, ADG LDI, Aero Communication, Apex Internet, Apollo Telecom, AT & T Global, Circle Net, Cube Xs Weatherly, Dancom, East Tel AJK, Ebone Network, Equant Pakistan, Eureka Net, Evamp & Sanga, FDI Fast Developers, Fiber Beam, Fiber Link, Fiber2home, Future Networks, Galaxy Technology, Gemnet Enterprises, Geo IT, Gerry's, Hajwari Net Zone, Hazara Communication, Helium Communication, IJ Internet Services, Infostructure, Instacom, Khyber Internet Services, Micronet Broadband, Multan Cable and Internet, Multi City Broadband, Nexlinx, Optix , Orient Expresslid, Pak Datacom, Paragon Telecom, Prime Vision Communications , QuBees/Sharp Com, Satcomm, Sharp Tel, Sky Telecom, Smart telecom, Soft Ends AJK, Superior Connections, Supernet Limited, Telecard , Telenex, The Professional Communication, Tufa Telecommunication, Vision Telecom, WanCom, Waylink, Wideband Communication, WiseCom, Zeta Technologies	**3**	**3**	**3**
4.	**Cat-IV**	Small operators	Rest others…	**1**	**2**	**2**

Annex-D

Telecom Operators Categorization

S. No.	Categories	Licensee Type	Licensee/ Telecom Operators	Cyber Security Audit Experience (in years) (Minimum)
1.	**Cat-I**	CMOs & Large Operators with multiple Licenses	Ufone, Telenor, JAZZ, ZONG, PTCL, TWA, SCO, NTC	CL3
2.	**Cat-II**	Large Operators	Brain Telecom, Comsats Internet Services, Connect Communications, Cyber Internet Services, Fariya, KK networks, LinkDotNet, Master Communication, Multinet, Nayatel, REDtone, Wateen Telecom, Web Concepts, Wi-Tribe	CL3
3.	**Cat-III**	Medium and LDI Operators	DV Com Data, 4B Gentle, 7 Star telecom, ADG LDI, Aero Communication, Apex Internet, Apollo Telecom, AT & T Global, Circle Net, Cube Xs Weatherly, Dancom, East Tel AJK, Ebone Network, Equant Pakistan, Eureka Net, Evamp & Sanga, FDI Fast Developers, Fiber Beam, Fiber Link, Fiber2home, Future Networks, Galaxy Technology, Gemnet Enterprises, Geo IT, Gerry's, Hajwari Net Zone, Hazara Communication, Helium Communication, IJ Internet Services, Infostructure, Instacom, Khyber Internet Services, Micronet Broadband, Multan Cable and Internet, Multi City Broadband, Nexlinx, Optix , Orient Expresslid, Pak Datacom, Paragon Telecom, Prime Vision Communications , QuBees/Sharp Com, Satcomm, Sharp Tel, Sky Telecom, Smart telecom, Soft Ends AJK, Superior Connections, Supernet Limited, Telecard , Telenex, The Professional Communication, Tufa Telecommunication, Vision Telecom, WanCom, Waylink, Wideband Communication, WiseCom, Zeta Technologies	CL2
4.	**Cat-IV**	Small operators	Rest others…	CL1

Pakistan
Telecommunication
Authority

Point of Contact
Dr. Muhammad Mukaram Khan
Director General (Cyber Vigilance), PTA
Email: mukaramkhan@pta.gov.pk