CYBER SECURITY
Annual Report 2024-2025

www.pta.gov.pk

PTA

CYBER SECURITY

Annual Report

2024-2025

Acknowledgement

The Annual Cyber Security Report 2024-2025, prepared by the Cybersecurity (CS) Directorate of PTA, outlines the significant progress made in strengthening the cybersecurity landscape of Pakistan's telecom sector. The successful compilation of this report is a result of dedicated efforts by CS team, whose collective contributions have been instrumental in shaping its structure, content and relevance. Their consistent commitment to excellence and continuous pursuit of innovation have greatly enhanced the overall quality and impact of PTA's cybersecurity initiatives. The guidance and support of the Honorable Members of the Authority—Major General (R) Hafeez Ur Rehman HI(M), Mr. Muhammad Naveed, and Dr. Khawar Siddique Khokhar—throughout the development and publication of this report have made this possible. Their leadership played a vital role in steering the strategic direction of PTA's cybersecurity efforts. The valuable supervision of Dr. Muhammad Mukaram Khan, Director General (CVD), Mr. Ahmed Bakht Masood, Director CS, Mr. Tanweer Shehzad Khattak, Director (Cybersecurity) has been pivotal to the successful completion of this process.

The Authority further acknowledges the critical role of PTA Cybersecurity Audit Team, which worked in close coordination with internal audit teams of telecom operators and third-party auditing firms. Their joint efforts in identifying gaps and strengthening cybersecurity controls have significantly improved the sector's overall cyber resilience.

In addition, recognition is due to the Governance, Risk and Compliance (GRC) team for developing and refining various cybersecurity regulations and National Telecom Computer Emergency Response Team (nTCERT) for its effective monitoring of cybersecurity health across the telecom sector.

Disclaimer

Various results and analysis presented in this document have been developed to reflect the current cybersecurity posture of Pakistan's Telecommunication Sector, with the objective of promoting continuous improvement across all relevant domains. These efforts aim to safeguard the nation's critical data and infrastructure from potential compromise, in line with the provisions of PTA's Critical Telecom Data and Infrastructure Security Regulations 2020 (CTDISR-2020).

Additionally, the information contained herein reaffirms the Authority's mandate to inspect licensees with respect to their cybersecurity arrangements, protection of critical telecom data and infrastructure and the mechanisms in place for ongoing monitoring within their operational environments.

All information provided in this report is intended solely for informational purposes and unless explicitly stated otherwise, does not establish any legal obligation between PTA and any individual or entity. While every effort has been made to ensure the accuracy and timeliness of the information, changes in contextual or operational circumstances may result in deviations from the stated status.

Published by:
Cyber Vigilance Division
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

Contents

Acronyms

PTA - Pakistan Telecommunication Authority
SOC - Security Operation Center
nTSOC - National Telecom Security Operation Center
SIEM - Security Incident and Event Management
SOAR - Security Orchestration, Automation and Response
TI - Threat Intelligence
TIP - Threat Intelligence Platform
APTs - Advanced Persistent Threats
DRP - Digital Risk Protection
CERT - Computer Emergency Response Team
nTCERT - National Telecom Computer Emergency Response Team
CTDISR - Critical Telecom Data and Infrastructure Security Regulation
CS - Cyber Security
CTI - Critical Telecom Infrastructure
SIRP - Security Incident Response Plan
DNS - Domain Name Security
UEBA - User Entity and Behavior Analytics
SoD - Segregation of Duties
CISO - Chief Information Security Officer
PII - Personal Identifiable Information
VAPT - Vulnerability Assessment and Penetration Test
FBR - Federal Board of Revenue
SECP - Securities Exchange Commission of Pakistan
SBP - State Bank of Pakistan
SCO - Special Communication Organization
NADRA - National Database and Regulatory Authority

The Authority

Major General Hafeez Ur Rehman (R), HI(M)
Chairman PTA

Mr. Muhammad Naveed
Member Finance – PTA

Dr. Khawar Siddique Khokhar
Member Compliance and Enforcement – PTA

Chapter 1: Introduction

- PURPOSE
- BACKGROUND
- EXECUTIVE SUMMARY

1. Introduction

1.1. Purpose

The purpose of PTA's Cyber Security Annual Report is to provide a comprehensive overview of Authority's strategic, regulatory and operational initiatives aimed at enhancing cybersecurity resilience across the national telecom sector. It documents the progress made under CTDISR, highlights sector-specific threats and evolving tactics, evaluates the effectiveness of National Telecom Security Operations Center (nTSOC) and presents insight from regulatory audits and non-intrusive scanning perspective. The report also reflects PTA's efforts to build capacity, foster international cooperation and ensure continuous improvement through data-driven oversight and forward-looking policies.

1.2. Background

In recent years, the increasing digitization of services and dependence on ICT infrastructure have amplified cybersecurity risks across Pakistan's telecom sector. Advanced Persistent Threats (APTs), AI-powered phishing, deep-fake campaigns, cloud vulnerabilities and insider threats have added new dimensions to an already complex threat landscape. Recognizing this shift, PTA introduced CTDISR in 2020 to set a baseline for cybersecurity compliance. However, given the pace of technological change and the emergence of sophisticated attack vectors, a comprehensive regulatory overhaul was necessary. The Critical Telecom Data and Infrastructure Security Regulations 2025 (CTDISR-2025) have been developed in response to these evolutions and challenges bringing a more structured, risk-based and forward-looking framework aligned with global standards, such as ISO/IEC 27001, NIST CSF and Pakistan's National Cybersecurity Policy 2021. It strengthens security requirements across all telecom licensees, mandates the implementation of incident response & business continuity mechanisms and introduces provisions for cloud security, supply chain risk and regulatory audits. This updated framework ensures that Pakistan's telecom infrastructure is resilient, secure and aligned with the country's broader national security objectives.

To assess and improve the security posture of licensees, PTA evaluates them across several parameters, including:

- Non-intrusive fortnightly vulnerability scans
- Revalidation of third-party CTDISR audits
- Integration and alert-sharing quality with the National Telecom Security Operation Centre (nTSOC)
- Compliance with advisories issued via National Telecom Computer Emergency Response Team (nTCERT) Portal
- Threat intelligence sharing
- Implementation of Domain Name System (DNS) Security enhancements
- Contribution to Internet Protocol version 6 (IPv6) readiness

This Annual Report, based on CTDISR-2020 compliance and other above-mentioned parameters, provides **semi-anonymized and aggregated insights** into key cybersecurity incidents, regulatory compliance levels and progress indicators for the telecom industry.

1.3. Executive Summary

The Cyber Security Annual Report 2024–2025 presents a detailed account of PTA's regulatory and operational cybersecurity initiatives during the reporting period. The report is structured around five key pillars; **Legal, Technical, Organizational, Capacity-building and Cooperation** in line with ITU's guidelines.

This report includes:

- **CTDISR-2025:** A restructured version of the original CTDISR-2020, addressing gaps in scope, compliance and alignment with global standards and the latest trends.
- **nTSOC Intelligence:** nTSOC played a pivotal role in monitoring, detecting and reporting real-time threats. **Thirty six (36) licensees have successfully been integrated** with nTSOC so far. The report documents APT campaigns, sector-specific targeting, common initial access vectors, cloud threats, insider risks and the emerging challenge of deep-fakes and AI-powered attacks.
- **Non-Intrusive Scanning Results:** Security posture assessments conducted across licensees revealed varying levels of cyber hygiene with scoring benchmarks helping with risk prioritization and regulatory follow-ups.
- **Regulatory Audit Framework:** PTA conducted extensive CTDISR audits through registered third-party audit firms, covering all categories of telecom operators. A total of **50 licensees** were audited by 3rd party audit firms and 35 of these went through a rigorous regulatory validation audit by PTA.
- **Capacity Building & Collaborations:** PTA, in collaboration with national and international entities (e.g. APNIC, NCERT, Huawei, Nokia, MCMC) organized technical workshops, awareness sessions and skill development programs. These initiatives significantly contributed to improving sectoral readiness and Pakistan's standing in the global cybersecurity index.

Chapter 2: Legal Measures

- CRITICAL TELECOM DATA AND INFRASTRUCTURE SECURITY REGULATION 2025 (CTDISR-2025)

2. Legal Measures

Critical Telecom Data And Infrastructure Security Regulation 2025 (CTDISR-2025)

CTDISR-2020 was introduced by PTA to enhance the cybersecurity posture of Pakistan's telecom sector. It consists of 19 sections and 104 controls. These regulations set forth comprehensive requirements to protect critical telecom data and infrastructure. CTDISR-2020 mandates essential practices in cybersecurity governance, access control, data protection and incident response, thereby fostering uniform and robust cybersecurity standards within the industry.

2.1. The Evolution of Technology

Since 2020, the global technological landscape has undergone a massive transformation, marked by the mainstream adoption of artificial intelligence (AI) and machine learning (ML) across both information and communications technology (ICT) and cybersecurity (CS) domains. These technologies have significantly enhanced automation, office performance and economic activities. They, however have also introduced new risks, such as AI-driven phishing, deep-fake and autonomous malware.

The exponential growth of social media (SM) platforms has reshaped modes of communication, commerce and political engagement. While these platforms have enhanced digital interaction, they have also become key factors in misinformation, social engineering and personal data breaches.

Similarly, the global expansion of broadband infrastructure, the deployment of 5G networks, the emergence of low earth orbit (LEO) satellite internet and the rollout of Wi-Fi 7 have collectively improved digital connectivity and inclusivity. However, these advancements have also widened the cyber-attack surface due to an increased volume of connected devices and intensified data exchange.

These swift technological developments have introduced complex cybersecurity challenges, such as AI-powered threats, Internet of Things (IoT) vulnerabilities and multifaceted supply chain risks, exposing the limitations of traditional security frameworks. CTDISR-2020 played a foundational role in shaping national cybersecurity efforts. Nevertheless, the evolving threat landscape and rapid pace of technological innovation necessitate a revised and more comprehensive governance framework.

2.2. The Need for Revision

Besides technological compulsions stated above, continuous engagement with industry stakeholders over the past four years through cybersecurity audits, consultative sessions and continuous feedback has provided valuable insight into the practical CTDISR implementation challenges being faced by the industry. These interactions have consistently highlighted the need for greater clarity in specific provisions, improved guidance for emerging technologies and a more adaptive framework capable of addressing the rapidly evolving cyber threat landscape.

Key areas identified for enhancement include more robust cyber security governance structure, asset management, risk management, incident response, data privacy, insider threats, cloud security and HR controls, underscoring the need for continuous regulatory evolution to maintain effectiveness and relevance. In parallel, significant updates to global standards—such as ISO/IEC 27001 and the NIST Cybersecurity Framework (CSF) have introduced new domains, controls and governance practices.

Aligning CTDISR with these challenges and international standards has become essential to ensure consistency, relevance, interoperability and adherence to global best practices. This alignment will strengthen national cybersecurity resilience and support proactive risk mitigation in the face of increasingly complex digital threats, reaffirming the need to revise the existing framework.

2.3. CTDISR-2025 – A Strategic and Comprehensive Revision

CTDISR-2025 is a strategic and comprehensive enhancement of its 2020 version, incorporating substantial improvements to address the rapidly evolving cybersecurity landscape. Nearly all existing controls have been thoroughly reviewed and refined for improved clarity, precision and operational applicability enabling more consistent and confident implementation across the telecom sector.

To streamline governance and eliminate redundancies, overlapping or outdated controls have been consolidated, resulting in a more efficient and accessible regulatory structure. CTDISR-2025 introduces several new sections aimed at strengthening national cybersecurity resilience. The Asset Management section now mandates continuous identification, classification and tracking of all digital and physical assets to effectively manage risk exposure. The Risk Management section outlines a structured approach for identifying, analyzing and mitigating cybersecurity threats, enabling adaptive responses to emerging risks. The newly added Data Privacy section aligns security practices with international standards on personal data protection, emphasizing stringent control over data handling and storage.

The introduction of a dedicated Cloud Security section sets clear requirements for safeguarding information and services across public, private and hybrid cloud environments. Enhancements to Access Control provisions require the implementation of robust identity verification, physical and logical access control, role-based access mechanisms and multifactor authentication to protect critical systems and sensitive data. Recognizing the increasing prevalence of internal threats, a specialized Insider Threat Detection section has been included to support detection, monitoring and response to risks posed by employees, contractors and other trusted individuals.

A new Business Continuity Planning (BCP) section has also been introduced, emphasizing the development and maintenance of contingency planning and implementation to ensure operational resilience during and after cybersecurity incidents or other disruptions. It mandates risk-based continuity strategies, periodic testing and alignment with sector-wide recovery objectives to minimize downtime and data loss.

CTDISR-2025 also formally introduces HR Controls as a standalone section, underscoring the importance of human resource functions in cybersecurity governance. These controls cover background verification, cybersecurity training, access alignment and secure onboarding and off-boarding processes to reduce the likelihood of insider incidents.

Furthermore, the regulation emphasizes integration with the nTSOC, facilitating real-time threat intelligence sharing, coordinated incident response and a unified approach to national-level cyber defense. A dedicated section on Roles and Responsibilities of Information Security (IS) Personnel now clearly defines operational, tactical and strategic responsibilities across the cybersecurity domain.

Together, these enhancements establish CTDISR-2025 as a forward-looking, agile and globally aligned cybersecurity framework capable of addressing complex and emerging digital threats. These revisions exhibit the framework's shift toward proactive, risk-based cybersecurity governance. The figures below provide an overview of the main revisions and comparison of the two regulations.

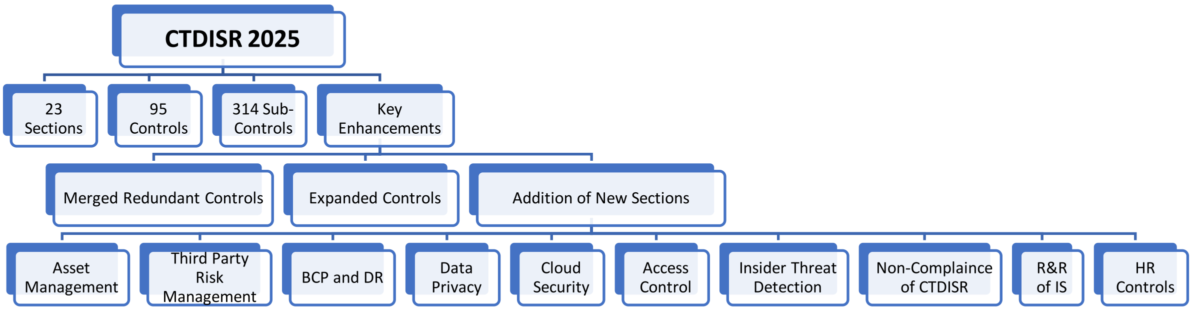


Figure 2.1: CTDISR-2025 - Overview and Key Enhancements

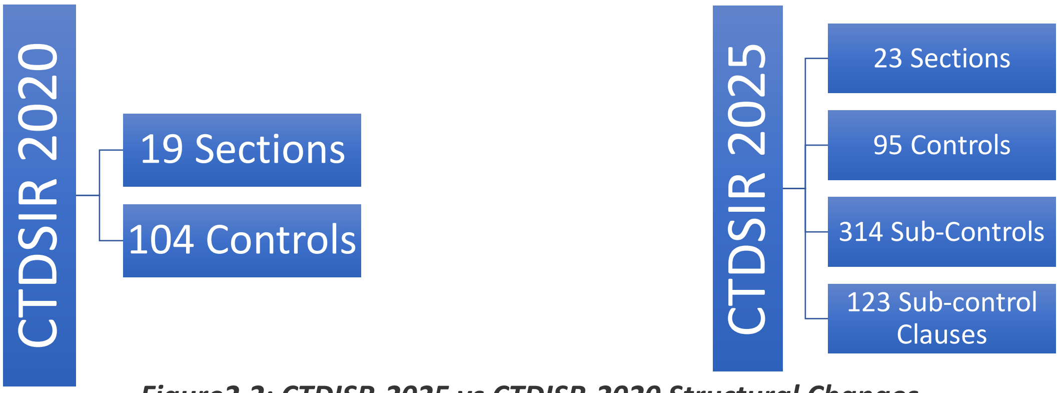


Figure2.2: CTDISR-2025 vs CTDISR-2020 Structural Changes

2.4. Aligning with National and International Standards

To maintain regulatory relevance and ensure global interoperability, CTDISR-2025 has been meticulously aligned with the national cybersecurity policy and internationally recognized standards. At the national level, the framework is harmonized with the Cyber Security Policy 2021, which outlines the Government of Pakistan's strategic vision for securing national digital infrastructure, safeguarding citizens data and promoting cyber resilience across critical sectors. CTDISR-2025 is also closely aligned with the National Computer Emergency Response Team (nCERT) Rules and Guidelines on Cybersecurity Implementation, thereby ensuring that organizational controls and incident response mechanisms remain consistent with national-level cyber incident management and reporting protocols.

Following international standards, CTDISR-2025 incorporates and complements the latest edition of ISO/IEC-27001:2022, the globally recognized standard for information security of management systems (ISMS), which introduces enhanced controls covering cloud security, threat intelligence and data masking. The regulation also aligns with the NIST Cybersecurity Framework (CSF) 2.0 issued by the United States National Institute of Standards and Technology, which offers a risk-based, structured methodology for identifying, protecting, detecting, responding to and recovering from cyber threats. Additionally, CTDISR-2025 takes into account the provisions of ISO/IEC 20000-1 and 20000-2, the international standards for IT service management systems (ITSMS), to ensure cybersecurity requirements are integrated seamlessly into broader IT governance and service delivery processes.

A comparative alignment exercise conducted between CTDISR-2025, ISO/IEC-27001:2022, NIST CSF-2.0 and ISO/IEC-20000 standards reveals strong synergy across key domains such as risk management, incident response, access control and continuous improvement. This alignment allows organizations operating in multi-regulatory environments to adopt CTDISR-2025 alongside international frameworks with minimal redundancy, thereby supporting a unified, globally compliant and contextually relevant cybersecurity governance model.

A detailed comparison table is provided in this chapter to highlight the similarities and distinctions across these frameworks, offering stakeholders clarity in navigating compliance requirements. Through these enhancements, CTDISR-2025 not only modernizes Pakistan's cybersecurity regulatory landscape but also establishes it as a globally aligned standard enhancing international cooperation, industry trust and digital confidence.

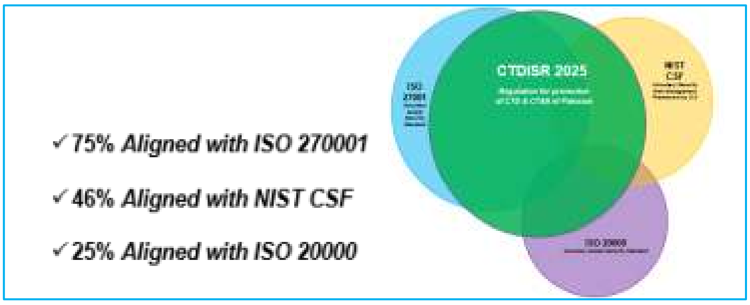

✓75% Aligned with ISO 270001
✓46% Aligned with NIST CSF
✓25% Aligned with ISO 20000
CTDISR 2025
ISO 27001
NIST CSF
ISO 20000

Figure 2.3: CTDISR-2025's Co-relation with International Standards

2.5. Strengthening Telecom Sector Resilience and National Security

The implementation of CTDISR-2025 is anticipated to significantly improve the cybersecurity posture of Pakistan's telecom sector, which serves as the backbone of the country's communication infrastructure and digital economy. Recognizing the strategic importance of this sector, the revised framework introduces comprehensive and forward-looking cybersecurity controls aimed at countering increasingly sophisticated and persistent cyber threats.

Once implemented, the framework will provide telecom operators with enhanced regulatory clarity through well-defined obligations, standardized best practices and structured compliance pathways. This is anticipated to reduce ambiguity, streamline enforcement and foster a culture of proactive cybersecurity management across the industry.

The regulation also introduces advanced controls to address emerging threats such as Advanced Persistent Threats (APTs), ransomware, insider risks and vulnerabilities stemming from third-party vendors and supply chains. By promoting continuous risk assessment, robust incident response planning and collaboration with national cybersecurity authorities, the framework will enhance the sector's overall resilience. Its integration with the nTSOC will enable real-time threat intelligence sharing and coordinated response efforts, thereby reducing the likelihood and impact of cyber incidents.

Moreover, the framework's alignment with international standards, including ISO/IEC-27001:2022 and the NIST Cybersecurity Framework (CSF) 2.0, positions Pakistan to meet global cybersecurity expectations. This alignment is expected to boost investor confidence, facilitate international collaboration and enhance Pakistan's standing in the global cybersecurity landscape. The improved cybersecurity posture resulting from CTDISR-2025 will play a crucial role in protecting critical infrastructure, securing citizen data and ensuring the continuity of essential communication services. These outcomes will directly contribute to an improved Global Cyber Security Index (GCI) rating, national stability, economic resilience and digital trust.

Chapter 3: Technical Measures

- NATIONAL TELECOM SECURITY OPERATIONS CENTER - nTSOC
- NON-INTRUSIVE SCANNING

3. Technical Measures

3.1. National Telecom Security Operations Center - nTSOC

3.1.1. Overview

The last two years marked a pivotal evolution in Pakistan's cyber threat landscape defined by stealthy, identity-driven intrusions, AI-enhanced deception and the blurring of lines between geopolitical conflict and cyberspace. Pakistan faced not only direct cyber-attacks but also coordinated hybrid operations through social media, intended to influence perception, disrupt trust and exploit institutional vulnerabilities.

This chapter gives a comprehensive review of Pakistan's digital landscape, synthesizing insights from the nTSOC, open-source intelligence, information from deep and dark web and data from global cybersecurity partners. It evaluates how Pakistan's telecom infrastructure, public sector networks and national coordination mechanisms responded to these evolving threats especially during the heightened cyber escalation triggered by the Pehalgam incident in April 2025.

nTSOC played a central role in defending national digital space, serving as the fusion center for real-time alerting, inter-operator coordination and actionable threat intelligence sharing. With over 10,000 alerts ingested, 1,500 incidents escalated and over 500 malicious infrastructure elements blocked, nTSOC became the operational backbone of Pakistan's cyber defense.

3.1.1.1. Global Threat Context and Geopolitical Cyber Risk

The global cybersecurity environment in 2024 was defined by malware-free intrusions (79%), industrialized cybercrime models (e.g., RaaS) and supply chain exploitation—according to CrowdStrike, ENISA and Mandiant. Threat actors now focus on credential theft, cloud misconfigurations and living-off-the-land tactics over traditional malware ingestion. Pakistan, as a digitally transforming country in a conflict-sensitive region, experienced targeted campaigns from regional adversaries. The Pehalgam incident catalyzed a wave of denial-of-service attacks, phishing campaigns impersonating federal ministries and mass disinformation pushed via spoofed portals, SM accounts and dark web propaganda.

3.1.1.2. National-Level Cyber Escalation and Response

Between April and May 2025, over 112 major incident claims, 25 DDoS attacks and 104 dark web threats were tracked by nTSOC against Pakistan. A dedicated Cyber Control Room was established by nTCERT, operating round the clock to coordinate containment efforts with MoIT&T, NCERT, Cyber Commands and telecom operators. This event marked the first ever execution of a national cyber crisis protocol, reinforcing the need for pre-defined war rooms, unified C4I system and continuous monitoring, especially during adversarial operational cycles.

3.1.1.3. AI-Driven Threats and Tactical Deception

AI has accelerated cyber offense around the world. In 2025, Pakistan observed:

- Voice-cloning attacks used in telecom fraud
- AI-generated phishing that bypassing detection
- Deep fake impersonations of national officials circulating on Telegram

These synthetic threats created operational confusion, amplified information warfare and highlighted the urgent need for AI-detection infrastructure and content verification standards across public services and telecom channels.

3.1.1.4. Strategic Takeaways

nTSOC has transitioned from a monitoring function to a telecom sector cybersecurity coordination center, coordinating live incident response, cross-sector intelligence fusion and preemptive takedowns. Cyberattacks are now geopolitical tools, requiring alignment among military, telecom, civilian CERTs and diplomatic arms. We need to shift from reactive cybersecurity to predictive defense—leveraging AI, TIPs and behavioral analytics to identify threats before they escalate.

3.1.2. Top Tactics, Techniques and Procedures (TTPs)

In 2024–2025, adversaries operating against Pakistan increasingly adopted low-footprint, evasive attack techniques that blended seamlessly into legitimate system activity. These tactics reflect a global trend toward stealth, persistence and credential abuse prioritizing post-exploitation movement over malware-based infections.

Table 3.1: Expanded View: Top 10 MITRE ATT&CK Techniques Observed

Rank	ATT&CK Technique	Report Count (Last 5 year)
1	Obfuscated Files or Information	194,824
2	Command and Scripting Interpreter	136,747
3	Phishing	124,800
4	Deobfuscate/Decode Files	76,327
5	System Information Discovery	31,561
6	Masquerading	25,928
7	Process Injection	22,106
8	User Execution (Malicious File)	19,877
9	PowerShell	17,654
10	Scheduled Task/Job	15,313

(Source: CTM360)

Leveraging telemetry from nTSOC, enriched by open-source intelligence and mappings from MITRE ATT&CK, CTM360, AlienVault and SOC Radar, the following TTPs were the most frequently observed across the telecom, public and critical sectors in Pakistan:

Table 3.2: Top Tactics Observed in Pakistan

TTP	Description	Occurrence (Last 5 year)
Obfuscated Files or Information	Use of encoding or compression to hide malicious content from detection tools. Often embedded in scripts or emails to bypass static analysis.	~194,824
Command and Scripting Interpreter Abuse	Adversaries executed malicious commands using PowerShell, Bash or cmd.exe, leveraging built-in OS tools (LOLBins) for stealth.	~136,747
Phishing (Spear & Mass)	Social engineering targeting telecom subscribers, ministry employees and university staff. Frequently spoofed official domains.	~124,800
Deobfuscate/Decode Files	Reverse engineering of scripts or payloads to trigger secondary-stage malware, commonly seen in multi-stage phishing kits.	~76,327

(Source: CTM360)

These tactics are consistent with the global shift toward "living off the land" strategies, where adversaries use native system utilities, stolen credentials and cloud access tokens instead of easily detectable binaries.

3.1.2.1. Strategic Implications

- Malware-less intrusions challenge conventional antivirus and SIEM rules. Without payloads, detection must rely on behavioral and contextual analytics.
- Script interpreter abuse indicates gaps in endpoint control policies and privileged access hygiene especially in remote or hybrid work environments.
- Phishing resilience remains low, especially in public-facing institutions with limitedSPF/DKIM/DMARC enforcement and insufficient user awareness.
- The prevalence of obfuscation and deobfuscation techniques suggests active use of commercial malware toolkits and evasion frameworks like Metasploit, Empire and Cobalt Strike.

3.1.2.2. nTSOC Response Strategy

To counter these TTPs, nTSOC implemented the following measures:

- Real-time detection rules for script-based abuse (e.g., PowerShell invoking encoded commands).
- Dark web monitoring to correlate leaked credentials with active phishing lures.
- Threat advisories incorporating Indicators of Compromise (IOCs) from MITRE-mapped attacks and global partner feeds.

These measures have enabled faster escalation, accurate attribution and more effective guidance to stakeholders.

3.1.3. Sector-Specific Areas Targeted in Pakistan

Cyberattacks in Pakistan during 2024–2025 were not indiscriminate. Instead, adversaries demonstrated sectoral-**specific targeting precision,** with motivations ranging from espionage and disruption to psychological influence and data monetization. nTSOC telemetry and partner intelligence feeds revealed distinct adversary preferences for specific institutional verticals, based on their strategic or symbolic value.

Table 3.3: Specific Areas Targeted in Pakistan

Sector	Primary Threats	Actors Involved	Impact
Government	Phishing, spyware, domain spoofing	Sidewinder, APT 36	Espionage, access
Telecom	DDoS, credential stuffing, Outdated Software/firmware	Criminal + Nation-state	Disruption, data theft
Academia	Defacement, ransomware, phishing	Hacktivists, RaaS gangs	Reputation, data loss
Law Enforcement	Judicial record leaks, defacements	R00TK1T, regional groups	Public trust erosion

(Source: nTSOC, CTM360)

Below is a breakdown of key sectors most frequently targeted, with their attack vectors, observed threat actors and impact assessment.

3.1.3.1. Government & Administration

The **federal and provincial e-governance ecosystem** remained a high-value target throughout the reporting period. Campaigns were largely attributed to **Sidewinder** and **APT 36,** which employed spear-phishing emails and trojanized office documents posing as inter-ministerial memos or procurement notices.

- **Spoofed domains** included fake subdomains of critical public sector organizations.
- **Spyware implants** were identified on systems of key policy-making bodies.
- Persistent reconnaissance was detected on government tender and HR portals.

These attacks aimed at **data exfiltration, internal surveillance** and **undermining institutional trust**, often timed with diplomatic or military flashpoints

3.1.3.2. Telecom Sector

Threat Profile: High-value infrastructure was targeted by disruptive and credential-theft campaigns. Telecom operators experienced **multi-vector intrusions**, driven by both **cybercriminals and nation-state actors.** nTSOC detected sustained:

- **DDoS attacks** originating from regional botnets.
- **Remote VPN access (R-VPN) abuse** from foreign jurisdictions.
- **Credential stuffing campaigns** exploiting reused passwords from prior breaches.
- **Router-level attacks**, exploiting outdated firmware and exposed admin panels.

Adversaries sought to compromise the **integrity of subscriber data, eavesdrop on signaling infrastructure and create national-level service disruptions** during geopolitical escalations.

3.1.3.3. Academic Institutions

Threat Profile: Persistent victim of opportunistic and ideological cyberattacks. Universities and research centers across Pakistan were increasingly targeted by hacktivist groups and financially motivated actors. Notable attack vectors included:

- **Mass phishing** campaigns targeting student and faculty email systems.
- **Ransomware deployments** on library systems and research repositories.
- **Website defacements,** often political in nature, by groups aligned with adversarial states.

More than 30 academic websites were either defaced or infected with web shells, while thousands of university credentials appeared on dark web marketplaces. The academic sector's limited cybersecurity funding and decentralized IT governance made it a soft but symbolically potent target.

3.1.3.4. Law Enforcement & Judiciary

Threat Profile: Targeted for disruption and data exposure by politically motivated groups. The judiciary and law enforcement portals were directly targeted by groups such as **R00TK1T,** which sought to:

- Publicly deface case records or leak them.
- Disrupt court proceedings by tampering with digital filing portals.
- Disseminate fake FIRs, court summons and warrants via compromised systems.

These incidents not only posed privacy risks but also had the potential to destabilize public trust in legal and policing institutions. nTSOC attributed several of these operations to Indian-origin hacktivist collectives exploiting narratives of regional unrest.

3.1.4. Adversary Focus: APTs Targeting Pakistan

The cybersecurity threat landscape in Pakistan during 2024–2025 was significantly influenced by persistent targeting from sophisticated nation-state and ideologically motivated adversaries. These Advanced Persistent Threat (APT) groups demonstrated a clear intent to compromise strategic institutions, disrupt services and exfiltrate sensitive information relevant to national security and foreign policy.

Drawing on attribution intelligence from nTSOC investigations, SOC Radar and international partners, the following APT groups were most actively engaged in targeting Pakistan's digital infrastructure:

Table 3.4: Top APTs Targeting Pakistan

Group	Alignment	Key Tactics	Targeted Sectors	Intent
Sidewinder	India-aligned	Phishing, C2 beacons	Government, Defense	Espionage
APT 36	India-nexus	Android spyware, PDFs	Academia, Military	Surveillance, Profiling
APT 41	China-aligned	Supply chain, RATs, Cobalt Strike	Telecom, Energy	Dual-use (State + Financial)
Turla	Russia-linked	Steganography, Watering holes	Military	Covert Access, Infrastructure
R00TK1T	Hacktivist	Defacements, fake data	Judiciary, Police	Psychological Ops

This adversary matrix illustrates that APT campaigns against Pakistan are not random but highly strategic, often tied to diplomatic events, defense milestones or internal unrest. Effective deterrence requires cross-sector threat intelligence sharing, behavioral analytics and attribution-informed mitigation.

3.1.4.1. Sidewinder

Targeted Entities: Critical Public Sector Organizations
Tactics: Decoy documents, phishing, embedded command-and-control (C2) beacons

Sidewinder was the **most active APT group targeting Pakistani entities in 2024–2025,** using an arsenal of crafted documents mimicking internal communications from government and military organizations. These documents often carried embedded macro payloads that established communication with attacker-controlled command-and-control infrastructure.

The group demonstrated a high degree of localization, with document titles and spoofed emails referencing actual government programs, military exercises or ministry updates. Sidewinder's campaigns were particularly effective in targeting defense and telecom infrastructure, exploiting inherent trust in internal email workflows.

3.1.4.2. APT 36 (Mythic Leopard)

Targeted Entities: Academia, Defense Personnel, Civil Institutions
Tactics: Android spyware, weaponized PDFs, phishing

APT 36 continued its operations using malicious Android APKs and trojanized academic research documents to spy on university faculty, military cadets and recruitment boards. The group leveraged fake scholarship offers and fraudulent academic collaborations invitations as lures, a technique effective in targeting students and early-career professionals.

Its mobile implants could exfiltrate SMS messages, call logs and contact lists, making it a high-threat actor in espionage and identity profiling.

3.1.4.3. APT 41 (Winnti Group)

Targeted Entities: Telecom, Energy, Government Contractors
Tactics: Software supply chain manipulation, open-source tool abuse, lateral movement

APT 41 blended state-sponsored espionage with financially motivated intrusion, making it a unique hybrid threat actor. In 2024, the group was observed exploiting software update mechanisms of telecom vendors and backend administrative tools of power companies.

Tools such as Cobalt Strike, Impacket and custom remote access trojans were used in conjunction with publicly available frameworks. The group's use of legitimate toolchains and encrypted traffic made APT 41 particularly difficult to detect using traditional indicators.

3.1.4.4. Turla

Targeted Entities: Military Communication Gateways
Tactics: Steganography, malware hidden in benign images, watering hole attacks

Turla was linked to covert reconnaissance on defense networks, often leveraging steganographic techniques—hiding payloads in image files distributed via spear-phishing. The group also repurposed compromised infrastructure from previous APT incidents in Pakistan, reflecting an emerging "APT-on-APT" piggybacking tactic.

Their operations exhibited surgical precision, extended dwell times, and the use of deceptive network traffic patterns to obfuscate command-and-control (C2) activity.

3.1.4.5. R00TK1T (Hacktivist/Ideological group)

Targeted Entities: Judiciary, Police, Health & Municipal Portals
Tactics: Website defacements, fake database leaks, digital mockery

R00TK1T conducted high-visibility defacement campaigns, often using politically charged imagery and narratives. They claimed responsibility for numerous breaches of provincial judiciary portals, police systems and health department websites, often displaying fabricated FIRs and court orders to spread disinformation.

These campaigns were designed for psychological impact, seeking to erode public trust in state institutions, particularly in politically sensitive or volatile region.

3.1.5. nTSOC & Telcos Operational Effectiveness (2024)

In a year marked by intensifying regional cyber turbulence and the evolution of threat actor capabilities, the nTSOC demonstrated its notable strategic and technical maturity. As the central cybersecurity coordination hub for Pakistan's telecom sector, nTSOC enabled real-time threat monitoring, proactive alerting and tactical incident response.

These efforts were executed in close coordination with both national stakeholders, thus reinforcing Pakistan's cyber defense posture amid an increasingly complex threat environment.

3.1.5.1. Key Operational Metrics

- 10,000+ critical security alerts were ingested by nTSOC through its monitoring systems and threat intelligence platforms.

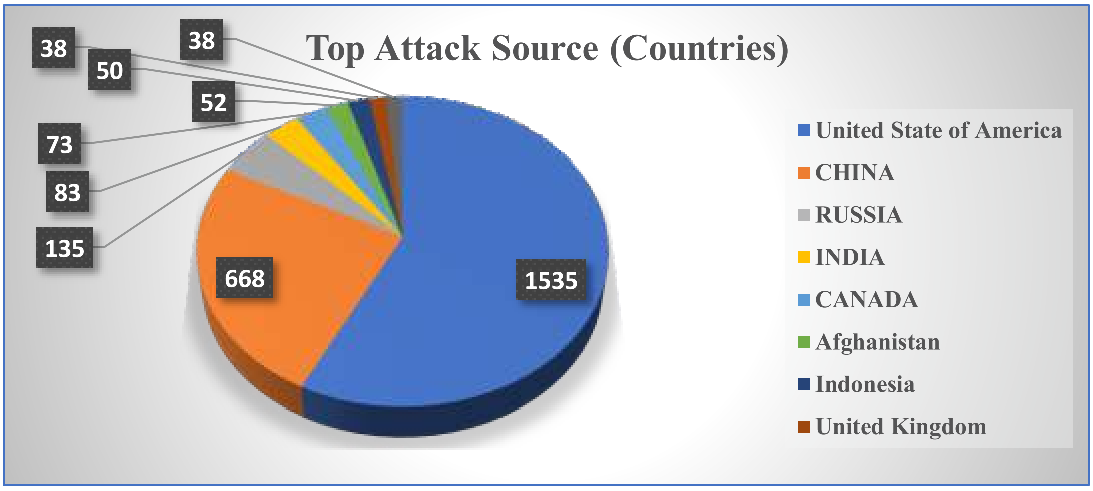


Figure 3.1: Top Attack Sources

- Of these, approximately 1,500 alerts were escalated and investigated in collaboration with relevant telecom operators and ISPs, resulting in targeted litigation efforts and detailed incident reporting.

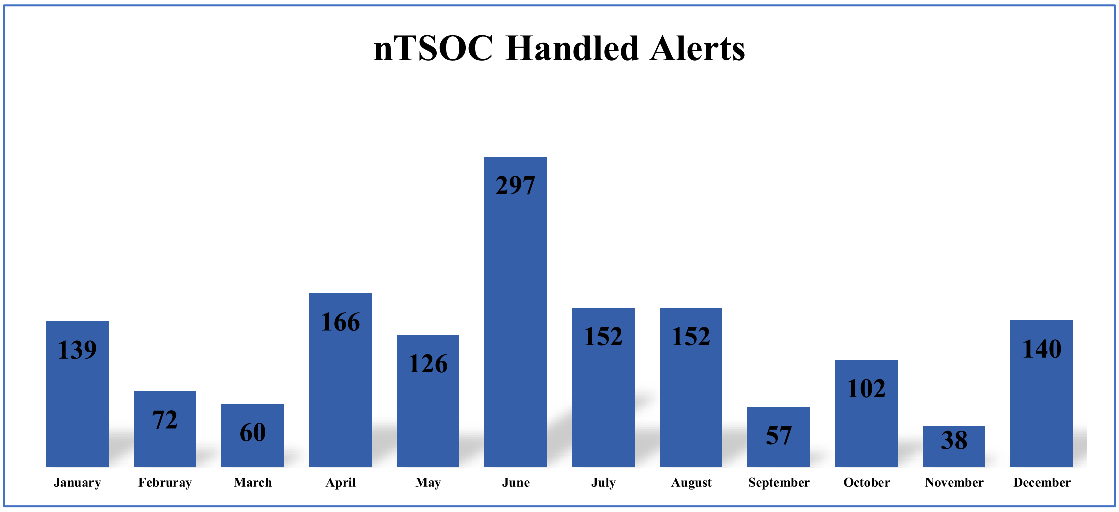


Figure 3.2: nTSOC Handled Alerts

- 151 cyber threat advisories were formally issued via the CERT portal, focusing on critical vulnerabilities (CVEs), phishing campaigns, ransomware IOCs and state-sponsored campaigns impacting the telecom ecosystem.
- A few hundred leaked credentials associated with Public Sector, Pakistani telecom users and enterprise infrastructure were identified through nTSOC's dark web surveillance program and shared with the affected operators or stakeholders for prompt remediation.

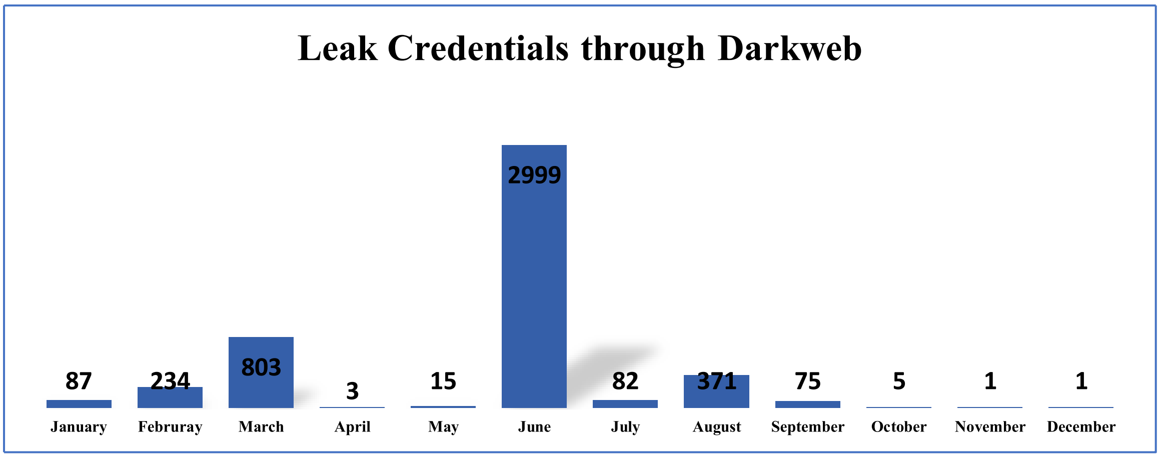
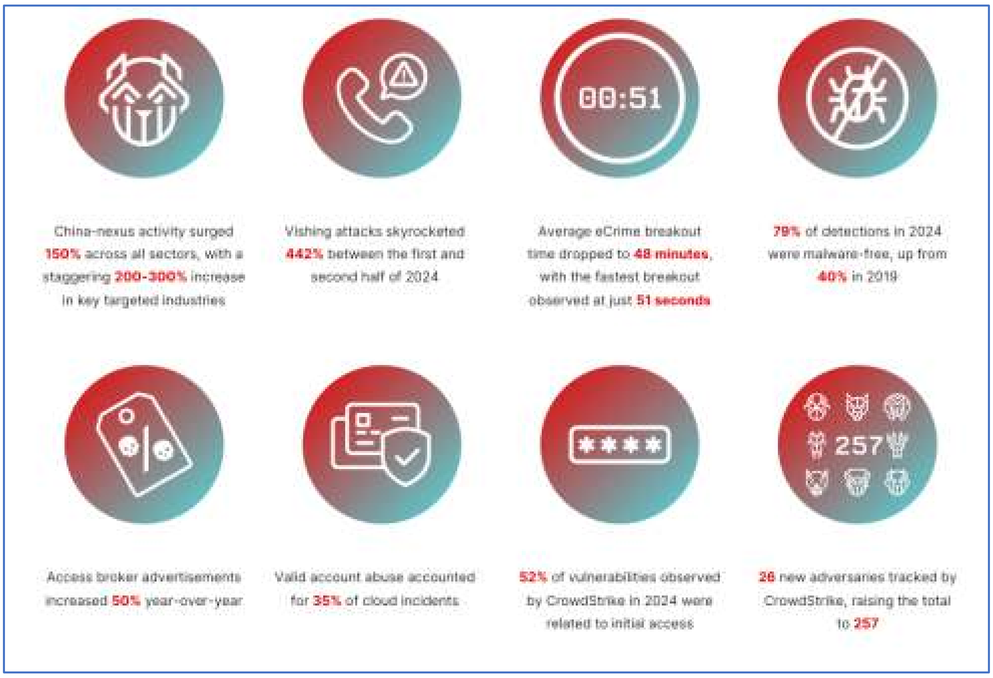


Figure 3.3: Leaked Credentials Through Darkweb

- 534 malicious IP addresses and domains were attributed to ongoing attacks and subsequently blackholed or blocked, leveraging cross-Telco coordination and upstream ISP action.

- ~25 Distributed Denial-of-Service (DDoS) attacks were successfully mitigated by telecom operators during the April–May 2025 cyber escalation. These attacks varied in intensity and duration (from 1 to 60 minutes) and coincided with regional geopolitical flashpoints.



China-nexus activity surged **150%** across all sectors, with a staggering **200-300%** increase in key targeted industries

Vishing attacks skyrocketed **442%** between the first and second half of 2024

Average eCrime breakout time dropped to **48 minutes**, with the fastest breakout observed at just **51 seconds**

79% of detections in 2024 were malware-free, up from **40%** in 2019

Access broker advertisements increased **50%** year-over-year

Valid account abuse accounted for **35%** of cloud incidents

52% of vulnerabilities observed by CrowdStrike in 2024 were related to initial access

26 new adversaries tracked by CrowdStrike, raising the total to **257**

Figure 3.4: Cyber-attacks Overview (Source: Crowdstrike 2025 Global Threat Report)

3.1.5.2. Strategic Impact

These figures reflect the evolving resilience and operational maturity of Pakistan's national cyber defense framework. nTSOC's ability to detect early signals, escalate critical alerts and drive coordinated response across diverse operators demonstrates:

- A functional and responsive incident handling ecosystem
- Increasing reliance on domestically developed intelligence and tooling
- Stronger vertical and horizontal communication channels within the national telecom sector

The emphasis on proactive dark web surveillance, public-private information exchange and rapid advisory issuance positions nTSOC as a cornerstone critical enable of Pakistan's national cybersecurity strategy.

3.1.6. Initial Access Vectors Observed in Pakistan

Understanding how adversaries gain their initial foothold is essential to disrupting attack chains and hardening national digital infrastructure. During the period of 2024–2025, nTSOC observed that threat actors leveraged low-cost, high-impact access methods, aligning with global trends reported by Mandiant and Verizon DBIR.

These methods often bypass traditional perimeter defenses by exploiting human error, credential exposure and third-party weaknesses. The following were the most frequently exploited access vectors in the Pakistani cyber landscape:

3.1.6.1. Phishing (Email/SMS/Web Lures)

Phishing remained the primary access vector for both nation-state and criminal actors. Attacks were characterized by:

- Custom-crafted emails spoofing domains of Public Sector organizations, telecom operators and academic institutions.
- Malicious attachments posing as procurement tenders, government notifications and billing statements.
- Fake login portals that mimicked national service portals.

Despite ongoing awareness campaigns, phishing remains effective due to inconsistent user education, poor email security hygiene and inadequate implementation of SPF/DKIM/DMARC policies.

3.1.6.2. Credential Stuffing and Password Reuse

nTSOC detected large-scale login attempts against VPNs, email gateways and self-care portals using previously leaked credentials:

- These credentials were often sourced from compromised academic institutions; telecom portals and SaaS applications compromised in prior years.
- Attackers used automated tools like OpenBullet, SentryMBA and SilverBullet to test username-password pairs across multiple services.
- The lack of MFA enforcement and use of shared departmental accounts across departments amplified the success rate of these attacks.

3.1.6.3. Exploitation of Known Vulnerabilities (CVEs)

Public-facing infrastructure hosted by telecom operators, ministries and academic institutions frequently lacked timely patching. Key exploits included:

- CVE-2024-49112: Targeting unpatched CMS deployments (e.g., Joomla, Drupal, WordPress).
- Log4Shell (CVE-2021-44228): Some older systems still carried vulnerable log4j libraries.
- VPN and firewall vulnerabilities: Exploited Fortinet, SonicWall and Pulse Secure gateways not upgraded to recommended builds.
- Attackers used Shodan, Censys and publicly available proof-of-concept (PoC) exploits on GitHub to identify and compromise exposed services.

3.1.6.4. Remote Access & VPN Misuse

A surge in foreign-origin VPN activity (R-VPN alerts) was observed during sensitive periods, such as:

- National holidays and public unrest
- Election-related events
- Geopolitical incidents (e.g., Pehalgam crisis)

Unauthorized tunneling originating from suspicious geographies—frequently obfuscated via proxy services or Tor exit nodes—was directed at telecom backend systems and .gov.pk subnets. This activity indicated probable credential compromise and highlighted persistent gaps in network access segmentation and zero-trust enforcement.

3.1.6.5. Supply Chain Compromise

Attackers increasingly exploited third-party contractors, IT integrators and outsourced vendors:

- Use of outdated or vulnerable software packages in national assets
- Shared credentials between vendors and government systems without proper revocation protocols.
- Lack of vendor risk assessments.

This technique was notably used by APT 41 and Sidewinder, exploiting trust relationships to pivot into sensitive infrastructure undetected.

3.1.7. Sectoral Risk Deep Dive

The threat landscape in Pakistan's digital environment is unevenly distributed, with each sector facing a unique combination of technical vulnerabilities, threat actor motivations and systemic weaknesses. nTSOC's investigations during 2024–2025 revealed sector-specific threat patterns that call for tailored mitigation strategies.

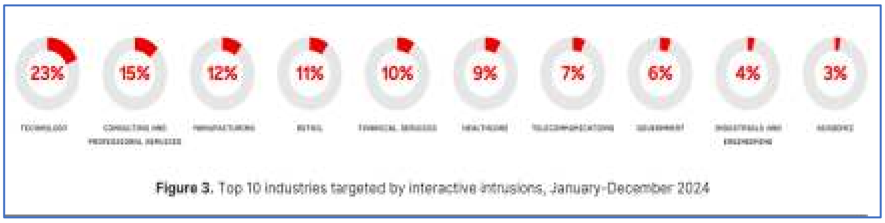


Figure 3.5: Sectoral Risk (Source: Crowdstrike 2025 Global Threat Report)

3.1.7.1. Telecom Sector

The telecom industry continues to face persistent probing and infrastructure-level attacks, largely due to its critical role in communications, surveillance and data routing. Threat actors—both financially and politically motivated have actively exploited weak configurations and delayed patching within service provider environments.

Table 3.5: Sectoral Threat Posture

Sector	Key Threats	Exposure Type	Observed Weaknesses
Telecom	Router exploits, C2, phishing, DDoS	Infrastructure & Email	Weak creds, limited network segmentation

3.1.8. Cloud & Insider Threat Landscape

As Pakistan's digital infrastructure rapidly shifts toward cloud adoption and hybrid IT environments, threat actors are increasingly exploiting identity mismanagement and insider vulnerabilities. While the cloud offers scalability and cost-efficiency, its improper configuration and weak access governance have introduced new threat vectors across the public and telecom sectors.

nTSOC assessments during 2024–2025 uncovered widespread cloud misconfigurations and insider risk patterns, particularly in public cloud deployments used by ministries, universities and telecom partners.

3.1.8.1. Cloud Infrastructure Misconfigurations

- Identity and Access Management (IAM) weaknesses emerged as one of the most pressing challenges. nTSOC identified recurring cloud security failures including:
- Hardcoded default credentials left active in production environments, particularly in administrative portals and API interfaces.
- Over-permissive IAM policies granting unrestricted access to storage, compute and database layers contradicting least-privilege principles.
- Unencrypted data backups hosted on publicly accessible Amazon S3 buckets, exposing sensitive telecom logs, HR records and archived reports.
- Absence of network segmentation or IP whitelisting, allowing attacker lateral movement once initial access is gained.

In multiple incidents, attackers located these misconfigured assets using open-source scanning tools such as Shodan, Censys or even simple Google dorking.

3.1.8.2. Insider Threats: Negligence, Abuse & Oversight Gaps

While technical perimeter defenses are improving, insider-driven incidents—both negligent and intentional—remain dangerously underreported. These primarily result from a lack of auditability, policy enforcement and behavioral monitoring.

Key patterns observed by nTSOC included:

- Unauthorized USB data exports from sensitive workstations, with no Device ControlPolicy (DCP) or Data Loss Prevention (DLP) mechanisms in place.
- Use of personal email accounts (e.g., Gmail, Yahoo) by employees to forward internal documents and reports, bypassing organizational controls.
- Former contractors and vendors retaining access tokens post-contract, due to unrevoked identities or shared administrative credentials.
- Zero user behaviour analytics (UEBA) deployed across most .gov.pk and .edu.pk institutions, making insider anomalies invisible until post-incident reviews.

In at least three high-profile cases, critical data exfiltration occurred over a period of weeks before being noticed—due to the absence of audit logs and alerts for anomalous access behavior.

3.1.8.3. Strategic Implications

- The convergence of misconfigured cloud platforms and unmonitored insider behavior presents a compounded risk.
- Data exfiltration can occur silently, bypassing traditional perimeter defense tools.
- Credential abuse persists long after access is no longer required, especially in outsourced or multi-stakeholder environments.

In the absence of DLP, UEBA and centralized Cloud Security Posture Management (CSPM), breaches remain undetected until threat actors publish or sell the stolen data.

3.1.8.4. nTSOC Recommendations.

- To mitigate these dual-threat domains, nTSOC advises:
- Mandatory implementation of Multi-Factor Authentication (MFA) across all cloud console access points.
- Use of role-based access control (RBAC) with time limited privileges for contractors and vendors.
- Implementation of cloud-native CSPM tools (e.g., AWS Security Hub, Microsoft Defender for Cloud).
- Enforcement of DLP and USB lockdown policies across government and telecom environments.
- Real-time User Behavior Analytics (UEBA) to flag anomalous internal activities.

3.1.9. AI-Driven Threats & Deepfake Incidents

The rise of Artificial Intelligence (AI) has introduced a transformative and increasingly weaponized dimension to cybersecurity. Adversaries now deploy AI not only to automate reconnaissance and exploit development but also to craft highly convincing social engineering content, undermining traditional detection mechanisms and overwhelming human verification.

In Pakistan, nTSOC identified a notable uptick in AI-driven attacks in 2024–2025, particularly in the telecom, financial and defense-related digital ecosystems. These threats are often low-cost, high-impact, requiring minimal technical skill while producing socially and psychologically disruptive effects.

- Synthetic Threat Trends Observed
- Voice Cloning in Fraud and Extortion

nTSOC recorded at least four confirmed incidents where threat actors used AI-generated voice clones of telecom executives and public sector officers to:

- Instruct billing departments to release sensitive customer datasets.

- Convince staff to bypass verification procedures during backend changes.
- Orchestrate payment diversions under the guise of "emergency approvals."

Voice synthesis tools like ElevenLabs, Descript and open-source models have made these attacks accessible and nearly indistinguishable from authentic conversations—particularly over poor-quality phone lines.

3.1.9.1. AI-Powered Phishing & Social Engineering

- Phishing emails generated using large language models (LLMs) now contain flawless grammar, realistic context and tone customized based on prior breaches (e.g., internal writing styles).
- nTSOC detected spear-phishing attempts that referenced real projects, colleagues and organizational structures possibly scripted via AI trained on scraped LinkedIn and leaked email data.
- These emails bypassed traditional spam filters and keyword-based detection, leading to a 28% increase in clicking-through rates in controlled phishing simulations.

3.1.9.2. Deepfake Videos & Disinformation Campaigns

During the April–May 2025 cyber escalation, deepfake videos were circulated on platforms like Telegram, TikTok and politically themed Facebook pages, impersonating:

- Senior military officials announcing fictitious troop movements.
- Public sector leaders delivering fabricated policy statements.
- "Whistleblower" videos featuring cloned voices and AI-simulated facial expressions.

Although quickly debunked, these clips amassed thousands of views and were widely reshared by coordinated, showcasing how AI-powered media manipulation can achieve tactical confusion at national scale.

3.1.9.3. Risks & Challenges for Pakistan

- The convergence of AI with adversarial intent has resulted in:
- A breakdown of digital trust across voice, video and email communication channels.
- Accelerated velocity and volume, overwhelming traditional human-led moderation and incident response mechanisms
- The rise of zero-day narratives—false or misleading information that spreads faster than it can be verified or countered.

These dynamics directly threaten electoral integrity, crisis response coordination and national image management in an already tense geopolitical environment.

3.1.9.4. nTSOC Position & Recommendations.

- To combat synthetic threats, nTSOC recommends adopting a national-level counter-AI posture with the following priorities:
- Deploy AI-driven content detection systems for telecom, media and government agencies (e.g., deepfake detection APIs, speech authenticity validators).
- Enforce robust verification protocols for high-risk communications (e.g., callbacks, multi-person confirmation).
- Embed synthetic threat modules in national cybersecurity drills.
- Launch targeted awareness campaigns educating civil servants, journalists and social media users on recognizing AI-generated misinformation.
- Partner with social media platforms and international allies to takedown disinformation content at scale.

3.1.10. Major Incidents: April–May 2025 Cyber Escalation

The Pehalgam incident on 22 April 2025 triggered a wave of coordinated cyber operations against Pakistan, marking one of the most significant cyber escalation events in the region's recent history. Within hours, threat actors launched multi-vector campaigns targeting Pakistan's telecom infrastructure, public institutions and digital services. These were strategically timed to exploit political distraction and psychological disruption.

The nTSOC, under PTA, swiftly transitioned into emergency response mode, acting as the national coordination hub. On 9 May 2025, a Cyber Control Room was formally activated by MoITT to handle high-priority incidents in real time, backed by direct collaboration with PTA, NCERT and the Cyber Commands of Pakistan Army and PAF.

Table 3.6: Operational Snapshot (April 22 – May 16, 2025)

Category	Volume/Details
Cyber Incident Claims Monitored	112 total (35 Public Sector, 75 Private, 2 Telecom)
Dark Web Claims Monitored	439 against Pakistan (104 in this period)
Advisories Issued	15 Critical (DDoS, phishing, APT, malware)
Threat Artifacts Analysed	~75,000 IPs, ~2,400 domains
Blocked IPs/Domains	534 (300+ during escalation period)
Category	Volume/Details
DDoS Attacks Mitigated	25 (1 min – 1 hr duration)

3.1.10.1. Telecom Sector

- Distributed Denial of Service (DDoS) attacks were launched against major telecom operators lasting from several minutes to an hour.
- Credential harvesting attempts targeting consumer-facing routers used by telecom SME, largely ineffective due to misattribution or timely preventive blocking measures.
- Telcos also observed spoofed phishing campaigns using themes such as SIM suspension, billing disputes or wartime service disruptions.

3.1.10.2. Federal and Public Services

- Phishing emails spoofing government, defense, and telecom SMEs carried malicious payloads disguised as policy updates or internal documents.
- There were 23 major claims of data breaches reported during this period, affecting multiple sectors beyond the telecom sector.
- Seven access leaks were identified, impacting several sectors in addition to telecom.

3.1.10.3. Dark Web & Psychological Operations

- A total of 104 Pakistan-related claims on dark web forums were monitored, of which 30–35% were proven false, including fabricated DDoS and data breach reports.
- nTSOC preemptively notified some victims before they became aware, marking a milestone in national cyber threat readiness.

3.1.10.4. National Response Coordination: Cyber Control Room

nTSOC played a pivotal leadership role, driving tactical and strategic response across:

- Real-time collaboration with the National CERT, telecom SOCs, ISPs, sectoral CERTs, MoITT, law enforcement agencies (LEAs) and military cyber arms.
- Establishment of a dedicated hotline for rapid operator engagement and threat validation.
- Launch of critical threat advisories, including IOCs related to active APT campaigns.
- Technical intervention to blacklist malicious infrastructure, minimizedwell time and escalate takedown requests with upstream providers.

3.1.10.5. Key Achievements

- Pre-emptive threat detection from dark web chatter and attribution tools.
- Operational alerting issued before target systems had confirmed compromise.
- Cyber diplomacy coordination via NCERT and international CERT channels.
- Incident war-room simulations are being institutionalized as part of post-crisis preparedness protocols.

3.1.10.6. Strategic Reflections

- The April–May 2025 cyber response validated the importance of central orchestration (led by nTSOC) and cross-domain communication.
- There is a growing need to institutionalize cyber crisis protocols, dark web intelligence feeds, and sector-specific response playbooks.
- With over 100 unique claims in under a month, this escalation event demonstrated how cyber incidents now move at the pace of political developments.

3.1.11. Strategic Actions & Recommendations for 2025

The threat landscape in 2024–2025 has revealed both the growing sophistication of adversaries and critical structural vulnerabilities in Pakistan's digital defenses. To build a resilient, future-proof cybersecurity ecosystem, nTSOC recommends the following strategic national-level initiatives:

3.1.11.1. Deploy a Federated Threat Intelligence Platform (TIP)

nTSOC is establishing a centralized TIP that aggregates IOCs from APT campaigns, dark web intelligence and regional threat indicators in real time. This platform will:

- Ingest data from global CERTs, telecom SOCs and dark web crawlers.
- Support sector-specific dashboards for telecom, government, academia and other critical infrastructure sectors.
- Enable automated IOC distribution and seamless integration into national and local SIEM ecosystems.

Output: Faster detection, improved attribution and scalable incident response

.

3.1.11.2. Mandate Sector-Wise Cyber Drills and SOC Readiness Assessments

Enforce quarterly cyber drills across telecom operators, government IT departments and financial institutions. Activities should include:

- Simulated ransomware and phishing attacks
- War-gaming exercises with red-blue team engagements
- Readiness audits of existing SOC capabilities

Output: Enhanced muscle memory and cross-sector coordination under pressure

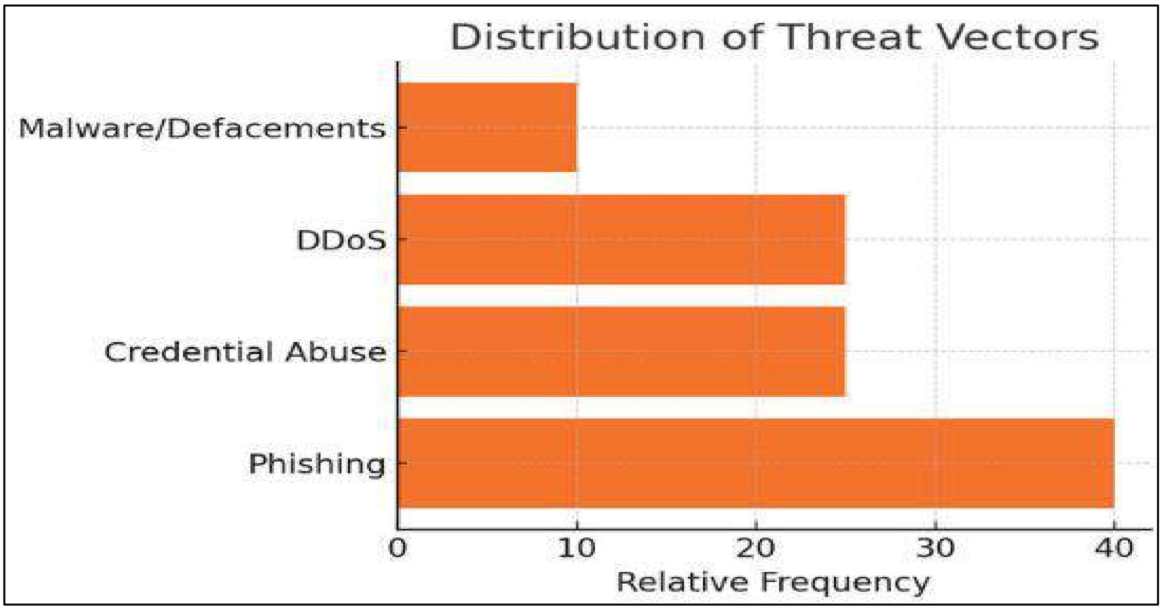


Figure 3.8: Distribution of Threat Vectors

3.1.11.3. Implement MFA and Zero Trust Architecture by Policy Mandate

- Mandatory multi-factor authentication (MFA) for all sensitive systems and cloud services
- Adoption of Zero Trust principles, including least privilege access, network segmentation and device trust scoring

Output: Minimized lateral movement and reduced blast radius in the event of credential compromises.

3.1.11.4. Expand nTSOC Role to Private Sector Integration

Enhancement of nTSOC capabilities for threat intelligence-sharing and escalation hub for critical infrastructure sectors beyond telecom through nCERT, including:

- Financial services
- E-commerce and tech platforms
- Energy
- Aviation

Output: Nationwide threat visibility and unified escalation framework.

3.1.11.5. Establish a Legal Framework for Critical Infrastructure Breach Disclosures

- All critical entities report breaches within 48 to72 hours of confirmation to nCERT or relevant sectoral CERT
- Failure to disclose may incur legal and financial penalties
- Sectoral CERTs maintain a secure breach disclosure mechanism channel and an anonymized incident database

Output: Improved transparency and proactive public-private response mechanisms.

These recommendations are not aspirational—these are operational imperatives, technically and strategically necessary for Pakistan to retain cyber resilience. Execution will require high-level political commitment, inter-agency alignment and long-term investment in both advanced technologies and skilled human capital.

3.1.12. Conclusion

The cyber domain is no longer a peripheral battlefield— it has become a central front in both regional and global contestations. Today's threats are stealthy, identity-driven, and increasingly AI-powered—engineered not just to disrupt services, but to manipulate perception, erode public trust, and exploit systemic vulnerabilities.

Pakistan's exposure during the April–May 2025 escalation was not due to technological inferiority, but rather a reflection of evolving adversary capability, the fluid geopolitical environment, and asymmetric intent. The speed, sophistication and targeting precision of these campaigns reinforce a critical truth: defense alone is no longer sufficient—anticipation and adaptability are now strategic imperatives.

The NTSOC has emerged as the nerve center of Pakistan's cyber defense posture. Its ability to correlate threat intelligence orchestrate multi-operator responses and operationalize proactive mitigation has directly contributed to national resilience.

Yet, much work remains. To sustain momentum and achieve cyber maturity at scale, Pakistan must now:

- Institutionalize cyber coordination across all sectors and provinces
- Invest in AI-native defense capabilities
- Elevate cyber readiness as a core national security priority
- Recognize every sector—public or private—as an integral link in the national security chain

This report is not merely a retrospective—it is a strategic call to action. The threats of tomorrow are already in motion today. Only through sustained investment, joint readiness and a unified vision can Pakistan remain secure, sovereign and digitally self-reliant in the decade ahead.

3.2. Non-Intrusive Scanning

In response to the evolving cyber threat landscape, the PTA has implemented a fortnightly, non-intrusive scanning program to continuously assess the external security posture of telecom licensees. This proactive measure simulates the view of a potential attacker by evaluating publicly exposed infrastructure without disrupting operations.

Scans cover critical domains, including software patching hygiene, TLS/web encryption status, application-layer vulnerabilities, DNS and email misconfigurations, IP/system reputation, and geo-hosting anomalies. By employing AI-enabled scanning engines, PTA delivers timely, actionable threat intelligence to each operator.

Licensees are mandated to remediate reported vulnerabilities within seven days of issuance. Repeated non-compliance may lead to formal regulatory proceedings. This initiative underscores PTA's shift toward intelligence-driven, risk-prioritized cybersecurity oversight to safeguard national telecom infrastructure

Table 3.7: Major Scanning Domains

External Posture Security Assessment Domains	
Software Patching	Enumerates systems running end-of-life and vulnerable software. Since end-of-life software is no longer supported by the OEM, it cannot be patched against known security issues or new vulnerabilities, increasing the likelihood of system compromise. An unpatched system is always vulnerable to the reported or zero-day threats.
Application Security	The Application Security domain evaluates each discovered web application for adherence to widely accepted security practices using passive techniques. Consistent deployment of appropriate web application security controls is crucial to defend against application-level attacks, considering the system's risk context.
Web Encryption	A non-intrusive scanning tool uses passive techniques to analyze web encryption security configurations. Properly configured web encryption is essential to protect communications from eavesdropping and to allow users to verify the system's authenticity.
Network Filtering	Analyzes company networks and systems for unsafe network services and IoT devices. Properly controlling services exposed to the internet is a fundamental security practice, as unsafe network services and IoT devices are common vectors for system and network compromises.
Breach Events	The Breach Event domain summarizes the organization's experienced breaches. Recent breaches highlight gaps in the breach protection program.

External Posture Security Assessment Domains	
System Reputation	The System Reputation domain identifies company-owned systems communicating with monitored C2 servers, sinkholes, honeypots or exhibiting hostile activity. The presence of the organization's assets in threat intelligence feeds indicates inconsistent and ineffective security controls, increasing vulnerability to malware infections and system abuse.
DNS Security	The DNS Security domain evaluates the controls to prevent unauthorized modifications of domain records, which can lead to domain hijacking.
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.

3.2.1. Cybersecurity Risk Scores from Non-Intrusive Scanning (2024–2025)

To evaluate the cybersecurity resilience of Pakistan's telecom sector, the PTA conducted regular, non-intrusive scans of licensees' public-facing digital assets throughout 2024. These scans focused on identifying external threat exposures across critical infrastructure elements, providing insight into sector-wide cybersecurity posture.

In 2024, the telecom industry recorded an average cybersecurity risk score of **8.4 out of 10**, indicating a moderately strong defense against external threats. By June 2025, this average improved to **8.6,** reflecting positive trends in vulnerability management, threat detection, and timely remediation by several operators.

The following table presents month-wise average risk scan scores of PTA licensees for the period January 2024 to June 2025, highlighting the sector's progressive enhancement in cyber hygiene and risk posture.

Table 3.8: Average Risk Scan Score

A	B	C	D	F
(9.0-10)	(7.0-8.9)	(5.5-6.9)	(4.0-5.4)	(0.0-3.9)

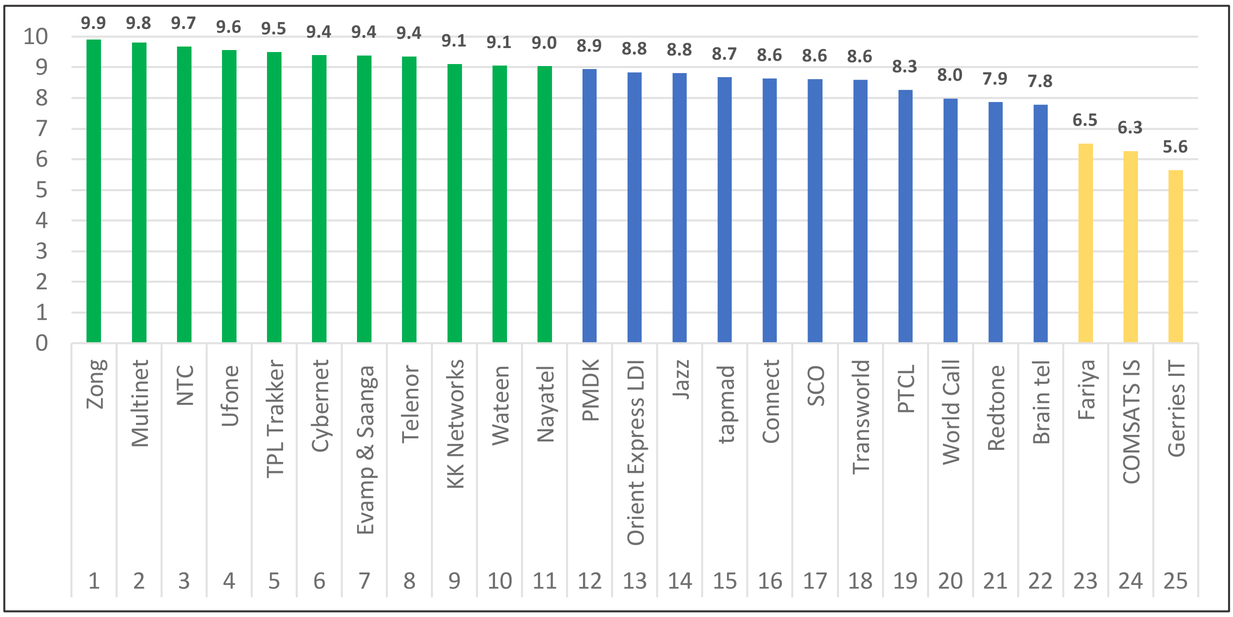


Figure 3.9: Industry-wide Risk Scan Score

Tthe data illustrated in the graph shows that **44% of licensees achieved an 'Excellent' cybersecurity rating, while 44% maintained a 'Very Good' score. In contrast, 12% fell below the threshold for a 'Good' ranking,** indicating the need for targeted improvement in the cybersecurity posture.

3.2.2. Security Domain Ratings – Sector-Wide Cybersecurity Posture

The domain-wise evaluation of PTA licensees' cybersecurity readiness reveals a mixed yet insightful picture of sector-wide strengths and areas requiring further attention. The assessment identifies high-performing domains, moderate-risk areas, and critical weaknesses that demand immediate remediation.

3.2.2.1. Strong Domains

The telecom industry consistently demonstrates high performance in the following areas:

- **Breach Events:** No major incidents were reported or detected, indicating effective incident prevention and containment.
- **DNS Security:** Strong DNS configurations are in place, minimizing risk of hijacking and unauthorized modifications.
- **System Hosting:** Public-facing infrastructure is well-managed and securely hosted, reflecting sound architectural and operational practices.
- **Email Security:** Compliance with standard email authentication protocols is high, but gaps remain in full adoption across all systems.

These results suggest that foundational infrastructure and domain-layer security controls are mature and well-maintained across the sector.

3.2.2.2. Moderate-Risk Domains

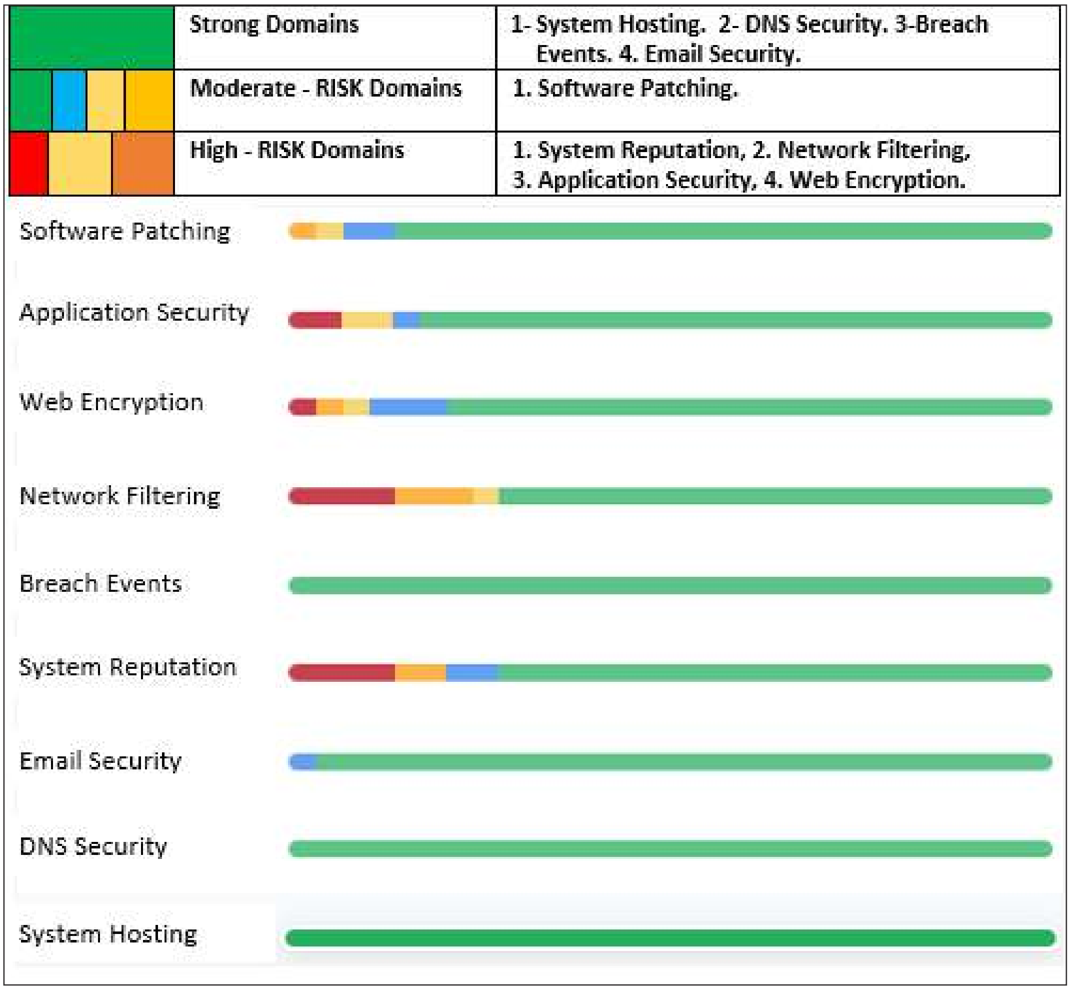
This domain show moderate exposure and require continued vigilance:

- **Software Patching:** While most systems are updated, some still operate on outdated or unsupported software.

3.2.2.3. High-Risk Domains

Critical weaknesses were of few licensee observed in the following areas:

- **Application Security and Web Encryption:** These remain the weakest links, with several licensees displaying insecure development practices and misconfigured or outdated encryption standards.
- **System Reputation:** Certain IPs and domains have been flagged in global threat intelligence feeds, indicating possible compromise or poor outbound traffic controls.
- **Network Filtering:** Inconsistent implementation of access controls has left some systems exposed to unsafe services and unmanaged IoT devices.



🟩	Strong Domains	1- System Hosting. 2- DNS Security. 3-Breach Events. 4. Email Security.
🟩🟦🟨🟨	Moderate - RISK Domains	1. Software Patching.
🟥🟨🟧	High - RISK Domains	1. System Reputation, 2. Network Filtering, 3. Application Security, 4. Web Encryption.

Figure 3.10: Domain-wise Score

These findings highlight the need for improved secure development life cycles, encryption hygiene network filtering and threat detection mechanisms.

While the telecom sector has established strong security foundations in areas such as systems hosting, email security, DNS security, and breach prevention.
However, significant gaps persist at systems reputation, network filtering, application security encryption security and outbound threat monitoring layers. These deficiencies could be exploited by threat actors, posing serious risks to service availability, data integrity and sector-wide trust.

To enhance the sector's overall cybersecurity posture:

- Licensees must prioritize the remediation of high-risk domains.
- Greater emphasis is needed on secure software development, modern encryption protocols, network filtering and real-time threat detection and prevention.
- PTA will continue its proactive, non-intrusive scanning program and enforce accountability to drive improvements.

Sustained progress in these areas will reduce exposure to modern cyber threats and help ensure a resilient, secure and trusted telecom infrastructure

Chapter 4: Organizational Measures

- CTDISR REGULATORY AUDITS
- THIRD PARTY AUDIT FIRMS

4. Organizational Measures

4.1. CTDISR Regulatory Audits

The regulatory audits conducted by PTA between October 2024 and February 2025 under CTDISR represent a major step toward strengthening cybersecurity across the telecommunications sector. Covering 35 licensees, this initiative reflects PTA's commitment to enforcing a robust national telecom cybersecurity framework and ensuring that operators adhere to defined security standards.

The CTDISR audit process underscores a proactive and adaptive regulatory approach designed to safeguard the telecom sector against rapidly evolving cyber threats. Beyond risk identification, the audits aimed to foster a culture of continuous improvement, encouraging licensees to align with emerging cybersecurity best practices and respond effectively to dynamic threat landscapes.

4.1.1. End-to-End Process Flow of Audit

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

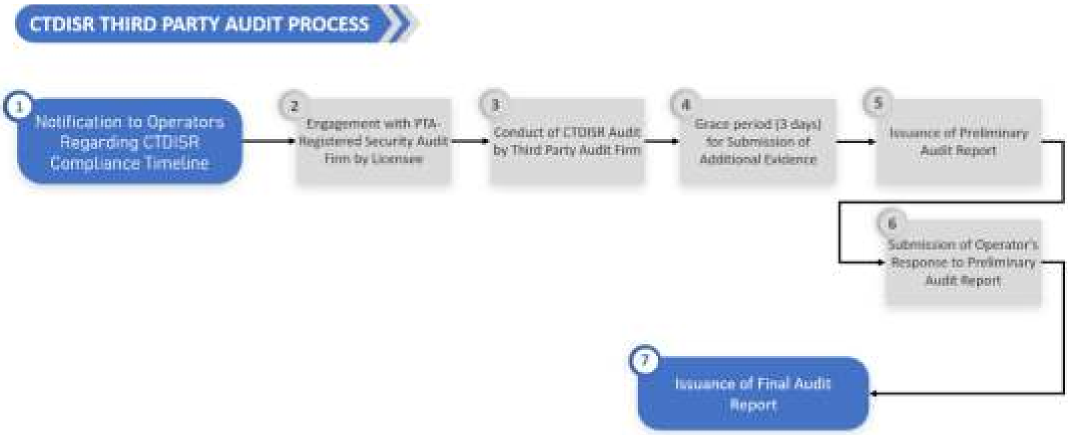

CTDISR THIRD PARTY AUDIT PROCESS
1
Notification to Operators Regarding CTDISR Compliance Timeline
2
Engagement with PTA-Registered Security Audit Firm by Licensee
3
Conduct of CTDISR Audit by Third Party Audit Firm
4
Grace period (3 days) for Submission of Additional Evidence
5
Issuance of Preliminary Audit Report
6
Submission of Operator's Response to Preliminary Audit Report
7
Issuance of Final Audit Report

Figure 4.1: Flow of conducting 3rd Party Audit by Licensee

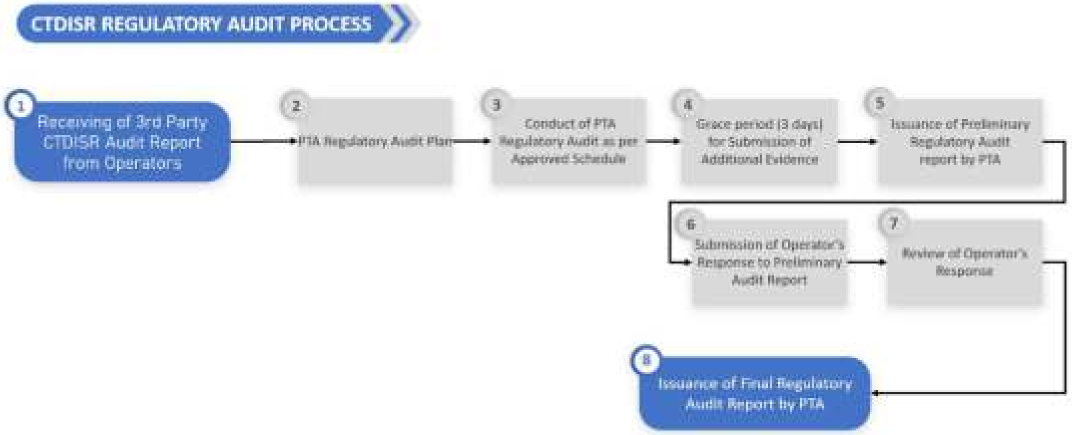

CTDISR REGULATORY AUDIT PROCESS
1
Receiving of 3rd Party CTDISR Audit Report from Operators
2
PTA Regulatory Audit Plan
3
Conduct of PTA Regulatory Audit as per Approved Schedule
4
Grace period (3 days) for Submission of Additional Evidence
5
Issuance of Preliminary Regulatory Audit report by PTA
6
Submission of Operator's Response to Preliminary Audit Report
7
Review of Operator's Response
8
Issuance of Final Regulatory Audit Report by PTA

Figure 4.2: Flow of Conducting PTA Regulatory Audit

4.1.2. Audit Objectives.

CTDISR regulatory audit plays a pivotal role in assessing and enhancing the robustness and resilience of cybersecurity infrastructure across the telecom sector. As part of its broader objective, CTDISR revalidation audit is designed to evaluate the extent to which licensees comply with the regulatory framework and maintain consistent alignment with national cybersecurity objectives.

Specifically, the audit assesses whether licensees:

- Conform to the implementation requirements set forth in CTDISR framework.
- Provide relevant information and evidence demonstrating compliance with CTDISR controls.
- Conduct regular monitoring, measurement, reporting, and review activities against defined performance objectives, to ensure alignment with CTDISR targets.
- Maintain operational controls and processes that align fully with CTDISR requirements.
- Fulfill all applicable statutory, regulatory, and contractual obligations related to cybersecurity.

Through this evaluation process, PTA aims to reinforce a culture of accountability, drive continuous improvement and strengthen the overall cyber resilience of Pakistan's telecom ecosystem.

4.1.3. Importance of Regulatory Audits by PTA

Regulatory audits conducted by PTA are a cornerstone of national efforts to strengthen cybersecurity governance within the telecom sector. These audits are not merely compliance checks they serve as strategic instruments to promote accountability, improve sector-wide resilience and ensure consistent implementation of CTDISR.

One of the primary objectives of PTA's audits is to foster transparency. By conducting audits in a structured, impartial and evidence-based manner, the Authority reinforces trust among licensees and stakeholders. A transparent process ensures that audit findings are objective, clearly documented and comprehensible to all parties, thereby encouraging openness and cooperation throughout the audit lifecycle.

Thoroughness is another defining feature of PTA's regulatory audits. Each audit undergoes a comprehensive review to ensure all critical areas of cybersecurity governance are covered. This detailed approach minimizes the risk of overlooking vulnerabilities, weak controls or gaps in implementation thereby reducing the potential for systemic security failures.

A key strength of PTA's audit model lies in its comparative review mechanism. The Authority evaluates third-party audit reports alongside its own independent assessments, allowing for the identification of discrepancies, misinterpretations or areas requiring further validation. This dual-review process enhances audit accuracy, balances external and internal viewpoints and ensures alignment with CTDISR expectations.

Moreover, regulatory audits act as a quality assurance mechanism. They assess whether third-party audit firms have conducted their evaluations with sufficient depth and in accordance with PTA's regulatory intent. This oversight not only verifies the integrity of audit results but also offers valuable feedback for improving third-party audit methodologies. In doing so, PTA contributes to raising the overall standard of cybersecurity assessments within the sector.

In essence, PTA's regulatory audits provide a foundation for informed decision-making, sectoral benchmarking and continuous improvement. They ensure that cybersecurity measures are not only compliant on paper but also effective in practice ultimately safeguarding Pakistan's critical telecom infrastructure in an increasingly complex threat environment.

4.1.4. Overview of CTDISR Audit Coverage by PTA

Over the past three years, PTA has progressively expanded the scope of its cybersecurity regulatory audits to ensure comprehensive compliance with the CTDISR across all categories of licensees. A year-on-year comparison reflects this sustained enhancement in oversight and regulatory enforcement.

Table 4.1: Year-wise Comparison

2022-23	2023-24	2024-25
13	21	35

Table 4.2: City-wise Comparison

2022-23			2023-24			2024-25		
Islamabad	Lahore	Karachi	Islamabad	Lahore	Karachi	Islamabad	Lahore	Karachi
8	2	3	11	6	4	16	9	10
Total: 13			Total: 21			Total: 35		

In 2022, audits were conducted for 13 licensees, primarily focusing on Category I and II operators, including major telecom providers such as Jazz, Telenor, ZONG, PTCL and Ufone.

In 2023, the audit coverage increased to 21 licensees, extending for the first time to Category III and IV entities. This included firms such as Web Concepts orient LDI and PMD, reflecting a shift toward a more inclusive audit regime.

By 2024, PTA's regulatory audit initiative expanded further, covering 35 licensees and achieving full-spectrum oversight across Categories I to IV. Notable entities audited during this cycle included NTC, SCO, TPL Trakker, EdotCo and AWAL Telecom, reaffirming PTA's commitment to a comprehensive and risk-informed approach to cybersecurity compliance.

This progression highlights PTA's deliberate and structured strategy to broaden its regulatory reach, identify systemic cybersecurity gaps and promote best practices across all tiers of Pakistan's telecom sector.

4.1.5. Evolving Cybersecurity Landscape: Key Audit Findings (2022–2025)

The cybersecurity landscape within Pakistan's telecom sector has undergone notable changes from 2022 to 2025, as reflected in the findings of annual regulatory audits conducted by PTA. These audits have played a vital role in identifying systemic gaps and informing strategic efforts to strengthen defenses against a rapidly evolving threat environment.

A comparative analysis of audit findings across these four years reveals both areas of sustained improvement and emerging vulnerabilities. The recurrence of certain findings, highlighted in green in the accompanying table, indicates persistent challenges that remain unaddressed and require renewed focus. Conversely, the absence of repeated issues related to phishing simulations, information security policies and critical asset classification suggests meaningful progress and successful interventions in those domains.

As cyber threats continue to grow in complexity, it is essential for telecom operators to adapt their cybersecurity practices accordingly. Continuous monitoring, timely remediation of identified gaps and reinforcement of existing controls will be critical to ensuring a resilient and secure digital infrastructure in the years ahead.

Table 4.3: Key Audit Findings

S.No	Findings in 2022	Findings in 2023-24	Findings in 2024-25
1	Lack of complete IS Policies and Procedures	CNIC, Address, MSISDN and other PII data is not encrypted in rest	CNIC, Address, MSISDN and other PII data is not encrypted in rest
2	Cyber Security Head is not independent, reports to CTO	Cyber Security Head is not independent, reports to CTO	Cyber Security Head is not independent, reports to CTO
3	Critical Assets are not properly classified	Absence of Privilege Access Management (PAM) Solution/Control	Absence of Privilege Access Management (PAM) Solution/Control
4	No Phishing Simulation exercises conducted	Absence of Data Loss Prevention (DLP) Solution/Control	Absence of Data Loss Prevention (DLP) Solution/Control
5	No Cyber Security Awareness exercises conducted for customers	Absence of Vulnerability Assessment & Penetration Testing (VAPT) Tracking Mechanism	Unattended Alerts in SIEM and Data Center (DC) POD

S.No	Findings in 2022	Findings in 2023-24	Findings in 2024-25
6	Lack of Critical Assets' Integration with SIEM	Absence of Mechanism to prohibit the use of unlicensed & unauthorized software	Absence of Mechanism to prohibit the use of unlicensed & unauthorized software
7	No Audit Trail of Actions performed by Admin user	Absence of Centralized Asset Management System	No Audit Trail of Actions performed by Admin user
8	Insufficient Access Controls Implementation in Secure Areas	Use of Production Data in the staging environment	Delayed Closure of Critical Vulnerabilities
9	Multiple server racks were found to be unlocked	Multiple server racks were found to be unlocked	Multiple server racks were found to be unlocked
10	-	Lack of automated mechanism to continuously analyze systems for unauthorized and unlicensed software	Lack of automated mechanism to continuously analyze systems for unauthorized and unlicensed software

4.1.6. Ranking Framework for Telecom Licensees

Following the completion of CTDISR regulatory audits by PTA, telecom licensees are ranked based on their adherence to regulatory requirements and their overall commitment to enhancing cybersecurity readiness. The Telecom Cybersecurity Index serves as a nationwide benchmarking tool, enabling comparative assessments of cybersecurity maturity across the sector.

4.1.6.1. Ranking Criteria for 2022

In 2022, the licensee rankings were based solely on their performance in CTDISR Regulatory Audit. This initial approach established a baseline for evaluating compliance with the cybersecurity framework.

4.1.6.2. Ranking Criteria for 2023-24

In 2023–24, the evaluation criteria were broadened to reflect a more holistic view of cybersecurity performance. Rankings were calculated using the following weightage distribution:

- CTDISR Audit Score = 60%
- Threat Intelligence Sharing with ntSOC = 15%
- Performance in Riskrecon = 10%

- Performance in nTCERT = 10%
- Feedback & Suggestions for Betterment = 5%

4.1.6.3. Ranking Criteria for 2024-25

For the 2024–25 period, the ranking methodology was further refined to incorporate additional performance indicators aligned with evolving sectoral needs and technological trends. The following domains and their associated weightages were introduced:

Table 4.4: Ranking Criteria 2024-25

Sr.no	Domain	Weightage	Remarks
1	CTDISR Regulatory Audits Audit Score	65%	Reflects the organization's compliance with CTDISR, sharing third-party audit report within due date and timely submission of documents for stage 1 for PTA Regulatory Audits audit. • 1 mark for each week delay in submission of documents for stage 1 for PTA Regulatory Audits audit will be deducted, up-to maximum of 5 marks. • Deduction of up-to 5 marks for submission of incomplete documentations for stage 1 PTA Regulatory Audits audit.
2	Performance in Non-Intrusive Scanning of Public facing Infrastructure (Annual Avg)	10%	Maintain consistent high scores by resolving identified vulnerabilities promptly and adhering to security best practices.
3	Threat Intelligence Sharing with nTSOC	10%	Smooth integration of licensees SOCs with nTSOC and actively participate in sharing actionable threat intelligence and security alerts regularly, ensuring timely detailed reporting and appropriate response to threats along with analysis and justification.
4	Performance in nTCERT	5%	Actively engage with nTCERT, report all security incidents promptly, collaborate in incident response exercises and ensure timely compliance with all advisories.
5.	IXP Participation	5%	Join and actively participate in Internet Exchange Point (IXP) to ensure accessibility of locally hosted services and enhance network efficiency and resilience.
6	DNSSEC Validation Score (Annual Avg on APNIC website)	5%	Implement and maintain DNSSEC across all domains, ensuring high availability and integrity of DNS responses.

The expanded criteria represent a comprehensive, multi-dimensional approach to assessing cybersecurity posture across the telecom sector. The index not only incentivizes compliance but also encourages continuous improvement, proactive risk management and alignment with global cybersecurity best practices.

4.1.7. Domain-Wise CTDISR Compliance Performance of PTA Licensees

The domain-wise analysis of average CTDISR compliance scores for 2024 provides valuable insight into the strengths and improvement areas across telecom licensees. This assessment serves as a strategic reference for future audits and regulatory planning.

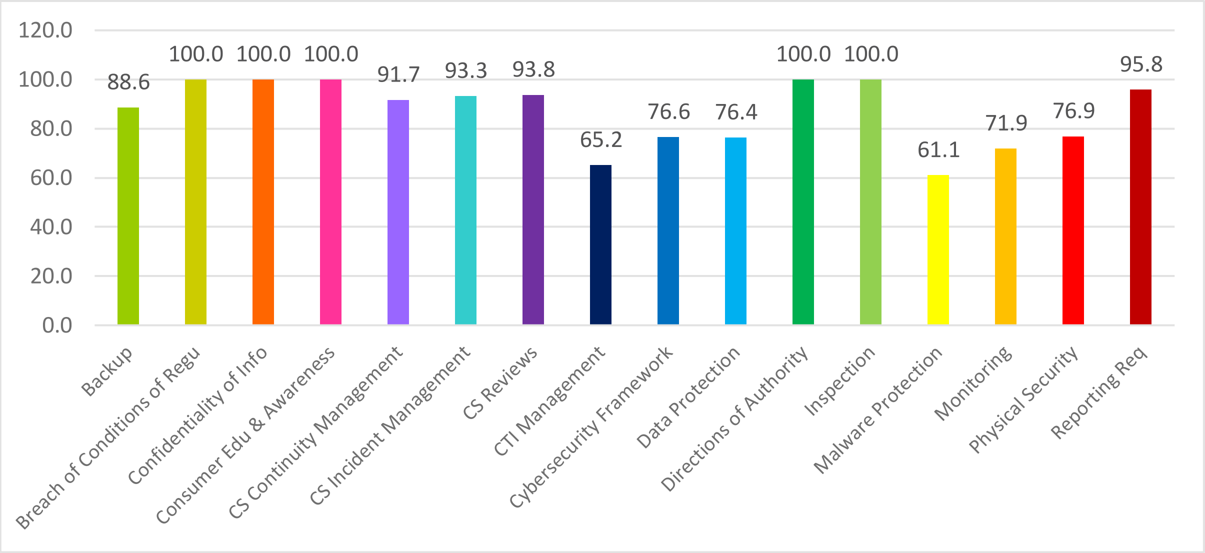


Figure 4.3: Domain-wise Ranking

Licensees exhibited full compliance (100%) in several key regulatory domains, including Inspection, Consumer Education & Awareness, Confidentiality of Information, Breach of Regulatory Conditions and Directions of the Authority. These results reflect strong adherence to legal obligations and consumer protection mandates.

High compliance was also recorded in areas related to Cybersecurity Incident Management (93.3%), Cybersecurity Continuity Management (91.7%) and Reporting Requirements (95.8%), indicating operational maturity in incident response, business continuity and regulatory communication.

However, comparatively lower compliance was observed in the following technical domains:

- **Malware Protection: 61.1%**
- **CTI Management: 65.2%**
- **Monitoring: 71.9%**
- **Cybersecurity Framework Implementation: 76.6%**

These gaps suggest the need for targeted improvements in foundational security controls, threat intelligence readiness and real-time monitoring capabilities. PTA is expected to address these deficiencies through strengthened audit follow-up mechanisms and sector-wide capacity-building initiatives under the 2025–26 CTDISR audit cycle.

This domain-wise performance review will guide regulatory priorities, support continuous improvement and help ensure a more resilient and secure national telecom infrastructure.

4.2. Third Party Audit Firms

4.2.1. PTA's Audit Firm Registration and Evaluation Framework

In order to institutionalize cybersecurity assurance across the telecom sector, PTA introduced the concept of third-party audit firm registration under a defined eligibility and evaluation framework. This initiative is grounded in CTDISR and aims to ensure that only qualified, credible and technically competent firms are engaged by licensees for cybersecurity audits.

PTA’s registration process involves rigorous criteria, including recognized certifications, demonstrable technical expertise, domain-specific experience and qualified human resources. The objective is to establish a trusted pool of firms capable of delivering consistent, high-quality audits aligned with CTDISR requirements. In parallel, PTA monitors the performance of registered firms by assessing the quality of audits conducted and the alignment of their findings with PTA’s own regulatory assessments.

4.2.2. Flow of Third-Party Registration

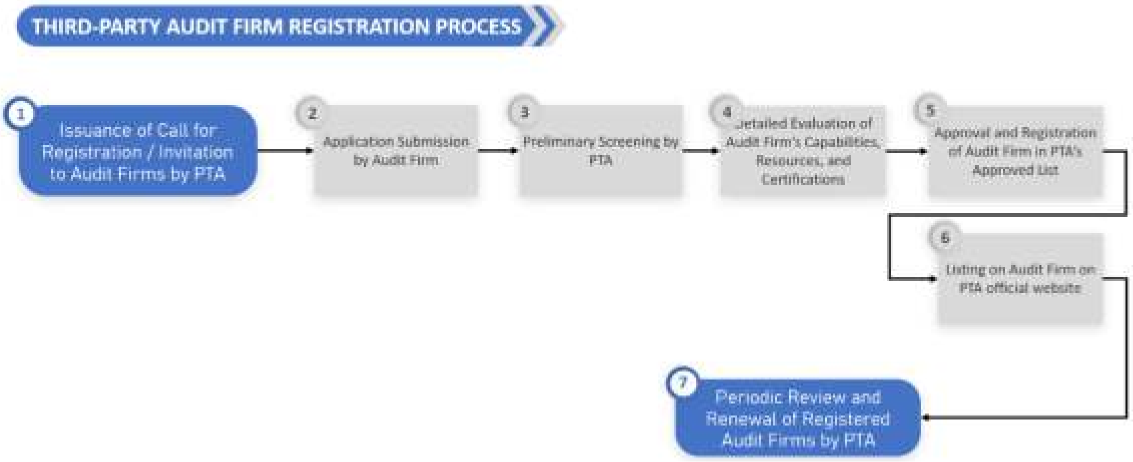

THIRD-PARTY AUDIT FIRM REGISTRATION PROCESS
1 Issuance of Call for Registration / Invitation to Audit Firms by PTA
2 Application Submission by Audit Firm
3 Preliminary Screening by PTA
4 Detailed Evaluation of Audit Firm's Capabilities, Resources, and Certifications
5 Approval and Registration of Audit Firm in PTA's Approved List
6 Listing on Audit Firm on PTA official website
7 Periodic Review and Renewal of Registered Audit Firms by PTA

Figure 4.4: Third Party Audit Firms Registration Process

4.2.3. CTDISR Third-Party Audits: Market Trends and Shifts (2022–2024)

The landscape of third-party audit project allocations has evolved considerably between 2022 and 2024–25, reflecting dynamic market competition, shifting client preferences and growing demand for cybersecurity assurance services. This progression highlights both the changing leadership among audit firms and broader trends within the compliance ecosystem.

In 2022, Trillium led the market with 10 project wins, establishing a strong footprint in the telecom sector. SGS followed with 5 projects, while EY secured 3, maintaining its presence through selective engagements.

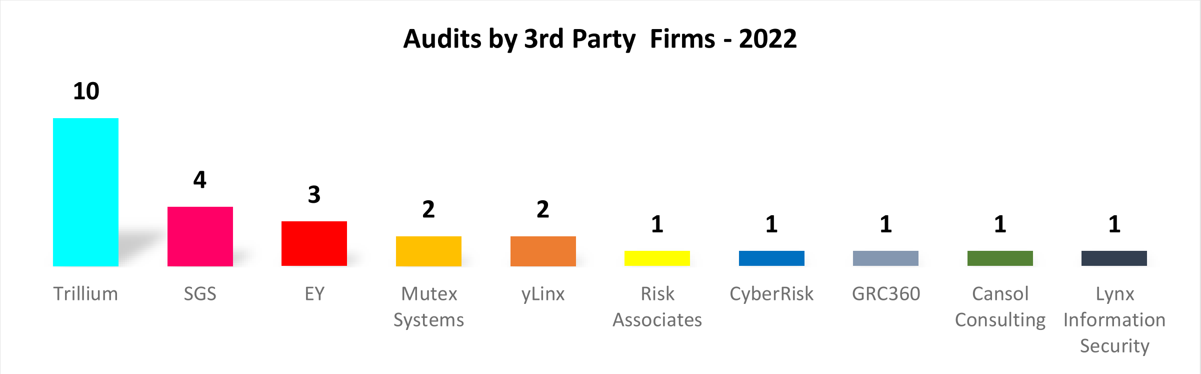


Figure 4.5: Third Party Audits

In 2023, Trillium strengthened its lead by capturing 15 projects an increase of 50% year-over-year. Meanwhile, yLinx secured 5 projects, matching SGS's performance from the previous year. Risk Associates and Compliance Wing won 4 projects each and CyberRisk followed with 3 engagements.

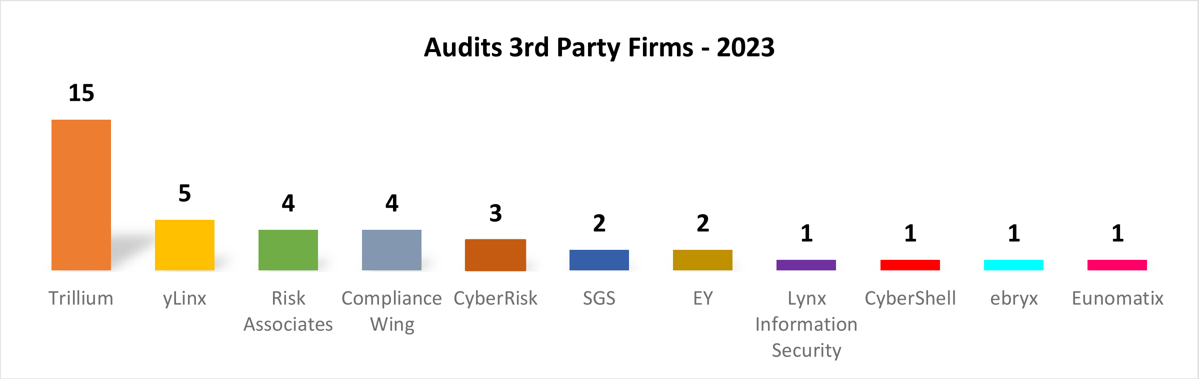


Figure 4.6: Third Party Audits - 2023

In 2024, Trillium maintained its leadership position with 12 project wins. CyberRisk emerged as a strong contender securing 9 projects. Ebryx and Mutex followed closely, with 8 engagements each. SGS delivered 4 projects, while yLinx executed 3. BDO and Risk Associates each conducted 2 audits, and LynxInfoSec, Catlytic, and 360 Technologies contributed with 1 project each.

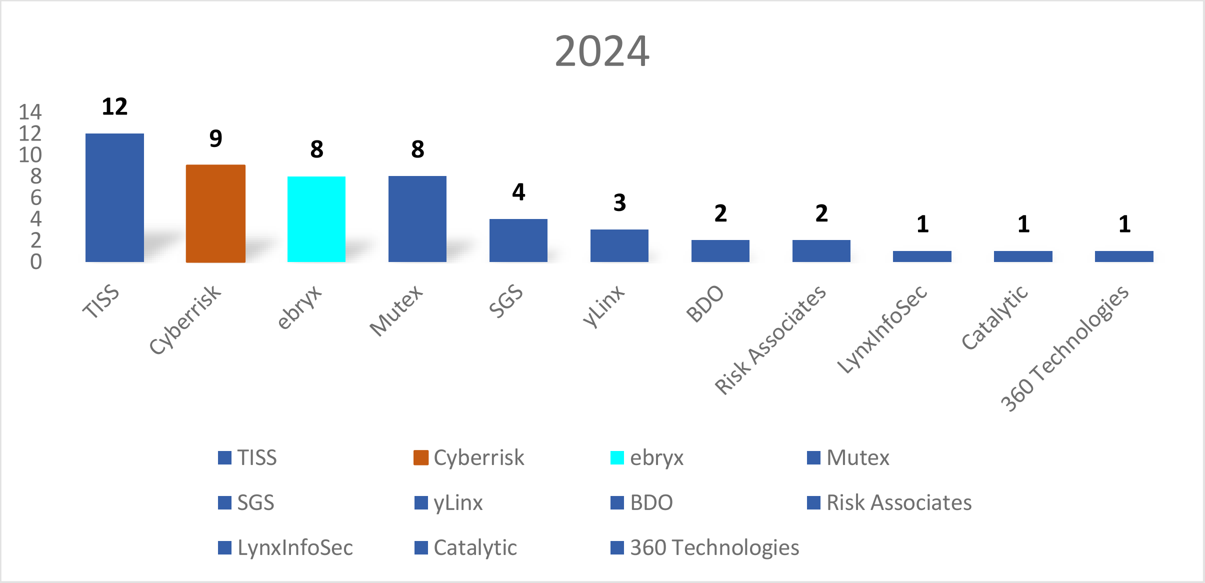


Figure 4.7: Third party Audits - 2024

Chapter 5: Capacity Building

- PTA AND APNIC COLLABORATE ON CYBERSECURITY INCIDENT RESPONSE AND CERT WORKSHOPS IN LAHORE AND ISLAMABAD
- CYBERSECURITY AWARENESS WEEK 2024
- PTA HOSTS TRAINING ON INTERNET EXCHANGE POINTS (IXPS)
- RPKI CAPACITY BUILDING WORKSHOP TO STRENGTHEN ROUTING SECURITY
- SANOG 42 CONFERENCE HELD IN ISLAMABAD WITH A FOCUS ON DIGITAL CONNECTIVITY

5. Capacity Building

PTA is playing a pivotal role in strengthening the cybersecurity and digital resilience of Pakistan's telecom sector. Among its most strategic efforts is implementing capacity building measures. These measures especially focus on new technologies and cybersecurity challenges, besides capacity building of small operators which lack enough financial capacity and technical resources. PTA-led capacity programs help ensure uniform security maturity across all licensees. PTA's capacity building isn't just a regulatory activity it's an investment in national cyber sovereignty. By empowering telecom operators with the skills and tools needed to defend their infrastructure, PTA ensures Pakistan's digital future is secure, inclusive and resilient.

5.1. PTA and APNIC Collaborate on Cybersecurity Incident Response and CERT Workshops in Lahore and Islamabad

In line with its ongoing commitment to enhancing cybersecurity awareness and response, PTA, in collaboration with the Asia-Pacific Network Information Centre (APNIC), successfully conducted a series of workshops on "Incident Response and CERT". The workshops took place over three days, with sessions held in Lahore and Islamabad. The Lahore workshop was jointly organized with the Punjab Information Technology Board (PITB), further strengthening regional partnerships. The training sessions were led by Mr. Adli Wahid, Senior Internet Security Specialist at APNIC Australia, who brought a wealth of experience in cybersecurity, particularly within the Asia-Pacific region. The workshops were designed to provide both theoretical insights and practical training in CERT operations, with a focus on forensic analysis management and the best practices for handling and mitigating security incidents.

Cybersecurity professionals from PTA, National Cyber Emergency Response Team (NCERT) and several telecom operators actively participated in the workshops, fostering a collaborative environment for knowledge exchange. Participants gained a comprehensive understanding of the essential functions of CERTs and enhanced their skills in managing cyber incidents.

The training concluded with a certificate distribution ceremony, during which Mr. Muhammad Naveed, Member Finance PTA, Dr. Muhammad Mukarram Khan, Director General of the Cyber Vigilance Directorate at PTA and Mr. Adli Wahid, Senior Internet Security Specialist at APNIC, presented certificates to all participants, recognizing their commitment to strengthening cybersecurity capabilities.

PTA expressed its gratitude to APNIC for their invaluable support in organizing the event and both organizations reaffirmed their dedication to continuing their collaborative efforts to build capacity and resilience within Pakistan's cybersecurity community.

PTA
SOC

5.2. Cybersecurity Awareness Week 2024

PTA successfully organized Cybersecurity Awareness Week 2024 from 9th to 15th December 2024. This week-long activity was designed to raise awareness about digital safety, data privacy and the legal dimensions of cybercrimes under the Prevention of Electronic Crimes Act (PECA) 2016 at both individual and organizational levels.

During the week, a series of expert-led discussions, webinars and informational sessions were conducted, aimed at equipping participants with essential knowledge and practical guidelines to protect themselves against rapidly evolving cyber threats. The sessions comprehensively covered critical areas such as:

- Best practices for **online security**
- **Data protection and privacy awareness**
- Understanding the **legal framework for cybercrimes** in Pakistan
- Prevention strategies against **common cyber risks**

The event saw active participation from operators, corporate organizations, academia and public sector stakeholders. PTA's official social media platforms were extensively utilized throughout the campaign to disseminate educational content, cybersecurity tips and awareness messages for the general public. The audience was also encouraged to engage with, share and amplify the awareness material to extend the campaign's outreach.

This collective effort significantly contributed to enhancing public understanding of cybersecurity challenges, promoting responsible online behavior and reinforcing the country's commitment to building a secure and resilient digital environment. The initiative effectively fostered a culture of cybersecurity awareness in alignment with Pakistan's national cyber safety objectives.

5.3. PTA Hosts Training on Internet Exchange Points (IXPs)

In line with its commitment to enhancing Pakistan's internet infrastructure, PTA, in collaboration with the PITB, successfully organized a three-day Capacity Building Training on IXPs from April 14 to 16, 2025, at PITB premises in Lahore.

The training, led by international experts, focused on enhancing technical expertise among telecom professionals. Participants engaged in hands-on labs, routing simulations and configuration exercises, equipping them with practical skills and knowledge on Internet Exchange Points (IXPs) operations.

This initiative is a significant step in supporting PTA’s ongoing efforts outlined in the Telecom Policy 2015, which has already led to the establishment of IXPs in major cities such as Lahore, Karachi and Islamabad, with a fourth IXP currently underway in Multan. The establishment of these IXPs is a key strategy to improve service quality, strengthen network security and reduce dependence on international bandwidth.

PTA remains dedicated to fostering digital resilience and reinforcing Pakistan’s internet infrastructure, ensuring the continued growth and development of the country's digital landscape.

5.4. RPKI Capacity Building Workshop to Strengthen Routing Security

PTA, in collaboration with APNIC, Internet Society (ISOC) and PITB, successfully organized a Capacity Building Workshop on Resource Public Key Infrastructure (RPKI) on April 16, 2025, at PITB premises, Lahore.

The one-day technical workshop aimed to enhance operational capacity within Pakistan's telecom sector, focusing on securing internet routing practices. The session was attended by senior management and network engineers from various telecom organizations.

The workshop was led by expert trainers from APNIC and ISOC, covering the following key areas:

- An overview of **Routing Security** and the significance of **RPKI**
- Practical training on **Route Origin Validation (ROV)**
- Procedures for **creating Route Origin Authorizations (ROAs)**
- **Hands-on configuration of RPKI on edge routers**

Through a combination of technical lectures, interactive sessions and hands-on lab exercises, the workshop aimed at building operational expertise and encouraging the adoption of RPKI within Pakistan's telecommunication industry.

This initiative is part of PTA's ongoing commitment to improving the country's position in global internet routing security rankings and strengthening collaboration with global internet governance organizations.

5.5. SANOG 42 Conference Held in Islamabad with a Focus on Digital Connectivity

The 42nd South Asian Network Operators Group (SANOG) Conference was successfully held in Islamabad from 21st to 24th October 2024, bringing together leading experts, network operators and IT professionals from across the Asia-Pacific region. The conference served as an essential platform for addressing critical topics such as data networking, cybersecurity, regional collaboration and digital infrastructure security.

During the event, notable addresses were delivered by key dignitaries, including the Minister of State for IT & Telecom, Ms. Shaza Fatima Khawaja, who highlighted the government's initiatives to promote digital connectivity. These included the deployment of new submarine cables, distribution of 1.1 million laptops and the establishment of National and Provincial Computer Emergency Response Teams (CERTs) to strengthen Pakistan's cybersecurity framework.

Chairman of PTA, Major General (R) Hafeez Ur Rehman, emphasized Pakistan's notable progress in the digital space, mentioning improvements in IPv6 traffic adoption, DNSSEC revalidation and preparations for the upcoming 5G spectrum auctions.

SANOG Chair, Mr. Rupesh Shrestha, underscored the importance of regional capacity-building and collaboration among South Asian network operators. Similarly, APNIC Director General, Mr. Jia Rong, stressed the need for enhanced regional cooperation to establish a resilient and secure digital landscape.

Over the course of four days, the conference featured technical sessions, workshops and expert panel discussions on crucial topics including cybersecurity, routing security, network automation and best practices for internet infrastructure management. PTA's active participation in this international forum reinforced Pakistan's ongoing efforts to strengthen its digital ecosystem and contribute meaningfully to the region's secure internet future.

Islamabad (21st October 2024): Experts from across the Asia-Pacific region convene at SANOG 42 to discuss digital connectivity, cybersecurity, and regional collaboration

SANOG 42

Chapter 6: National and International Cooperation

- PTA AND NCERT SIGN MOU TO STRENGTHEN CYBERSECURITY RESILIENCE
- PTA AND HUAWEI PAKISTAN SIGN MOU TO STRENGTHEN COLLABORATION IN IT AND TELECOM SECTOR
- PTA COLLABORATION WITH MALAYSIAN COMMUNICATIONS AND MULTIMEDIA COMMISSION (MCMC)
- PTA COLLABORATION WITH MALAYSIAN CERT

6. National and International Cooperation

PTA strongly believes in collaborative efforts to enhance the cybersecurity posture of telecom sector. Collaboration between the PTA, telecom operators and other critical sectors is essential for strengthening the national telecom cybersecurity ecosystem. Cyber threats often span networks of interconnected operators, vendors, and allied sectors, making joint efforts indispensable. Through collaborative frameworks, PTA can collect, share, and disseminate threat intelligence in real time, coordinate early warnings, and enable rapid responses to threats such as DDoS attacks, malware, and nation-state intrusions. PTA can collectively harmonize cybersecurity controls across telecom licensees and with other sectoral regulators through collaborative development of common standards and compliance frameworks.

6.1. PTA and NCERT Sign MoU to Strengthen Cybersecurity Resilience

On December 5th 2024, the Pakistan Telecommunications Authority (PTA) and the National Computer Emergency Response Team (NCERT) signed a Memorandum of Understanding (MoU) to enhance cooperation in cybersecurity and safeguard Pakistan's digital infrastructure.
The signing ceremony, held at PTA headquarters, marked a joint commitment to addressing cyber threats and building national resilience against emerging digital challenges. The agreement outlines collaborative efforts to strengthen cybersecurity, ensuring the safety and reliability of Pakistan's digital ecosystem.

Chairman PTA emphasized the critical role of cybersecurity in protecting communication networks and national IT infrastructure, underscoring the importance of collaboration in an increasingly complex threat landscape. Director General NCERT echoed these views, stressing the need of a unified response to tackle growing cyber risks impacting critical sectors.

This partnership represents a significant step in reinforcing Pakistan's cybersecurity capabilities, fostering a secure and interconnected digital environment for all stakeholders.

PTA
MOU SIGNING CEREMONY
BETWEEN
PAKISTA ELECOM AUTHORITY (PTA)
AND
NA AL COMP MERGENC SPONSE TEAM (nCERT)
00 PM

Islamabad 5th December 2024: Representatives from PTA, Dr. Mukaram Khan (DG Cyber Vigilance Division), and NCERT, Mr. Altaf Ur Rehman (Director Labs, National CERT), signing the MoU to enhance cybersecurity cooperation and strengthen Pakistan's digital infrastructure. The ceremony, held at PTA headquarters, also featured officials from PTA and NCERT.

6.2. PTA and Huawei Pakistan Sign MoU to Strengthen Collaboration in IT and Telecom Sector

On December 31st, 2024, PTA and Huawei Pakistan signed a Memorandum of Understanding (MoU) to strengthen collaboration in the IT and Telecom sectors. The agreement, signed at PTA Headquarters, focuses on capacity building, technology innovation, cybersecurity, and digital inclusion.

The partnership aims to drive advancements in 5G, Artificial Intelligence, and IoT while promoting secure digital infrastructure and bridging the digital divide. The Chairman PTA remarked, “This MoU represents a significant step in Pakistan’s digital transformation, enabling enhanced infrastructure and fostering innovation for sustainable growth.” The Deputy CEO of Huawei Pakistan highlighted, “Huawei remains committed to empowering Pakistan’s digital ecosystem and advancing its technological capabilities.”

This collaboration aligns with Pakistan’s vision of a digitally empowered economy, fostering technological excellence and equitable access to IT services nationwide.

Islamabad (31st December 2024): Pakistan Telecommunication Authority (PTA) and Huawei Technologies Pakistan Pvt. Ltd. sign a Memorandum of Understanding (MoU) to enhance collaboration in the ICT sector. The partnership aims to foster innovation, digital transformation, and capacity-building initiatives to support Pakistan's digital economy.

6.3. PTA Collaboration with Malaysian Communications and Multimedia Commission (MCMC)

Director of Cybersecurity at PTA undertook a visit to the MyCERT headquarters in Malaysia as part of efforts to foster international collaboration in cybersecurity. In this recent engagement, PTA and MyCERT discussed practical ways to enhance cooperation, strengthen incident response coordination, and share threat intelligence to address the growing challenges of the digital landscape. Both sides emphasized the importance of proactive information exchange, technical collaboration, and capacity building to safeguard critical digital infrastructure and promote a secure and resilient cyberspace. The visit reaffirmed the shared commitment of PTA and MyCERT to working collectively towards advancing cybersecurity readiness and regional digital safety.

6.4. PTA Collaboration with Malaysian CERT

Director Cybersecurity PTA undertook a visit to the MyCERT headquarters in Malaysia as part of efforts to foster international collaboration in cybersecurity. In this recent engagement, PTA and MyCERT discussed practical ways to enhance cooperation, strengthen incident response coordination and share threat intelligence to address the growing challenges of the digital landscape. Both sides emphasized the importance of proactive information exchange, technical collaboration and capacity building to safeguard critical digital infrastructure and promote a secure and resilient cyberspace. The visit reaffirmed the shared commitment of PTA and MyCERT to working collectively towards advancing cybersecurity readiness and regional digital safety.

Chapter 7:The Way Forward

- DEVELOPMENT OF NATIONAL TELECOM CYBER SECURITY FRAMEWORK
- 5G SECURITY GUIDELINES
- ANTI DDOS IMPLEMENTATION GUIDELINES
- ZERO TRUST NETWORK ACCESS
- IN-HOUSE AUDIT AUTOMATION WEB APPLICATION
- CTDISR AUDIT PLAN FOR 2025-26

7. The Way Forward

PTA is making all out efforts to improve security of critical data and infrastructure of Pakistan Telecom Sector. In this regard, some new initiatives are in progress to improve and uplift the cyber security posture of telecom sector. These are in line with the Pakistan Telecom Cybersecurity Strategy 2023-28.

7.1. Development of National Telecom Cyber Security Framework:

PTA will lead the development of a robust, sector-specific Cyber Security Framework aligned with the revised CTDISR 2025. The primary objective of this Framework is to provide clear, actionable guidance to licensees for implementing the regulation in a consistent and effective manner. It will define control-specific expectations, technical and procedural benchmarks, and includes examples where necessary. At the same time, the Framework will offer clarity to auditors by specifying how to assess and validate compliance for each control— detailing the evidence to be reviewed, the criteria for evaluating effectiveness, and the method for determining the level of compliance. This initiative aims to support harmonized implementation, reduce ambiguity, and promote a more transparent and measurable approach to regulatory audits across the telecom sector.

7.2. 5G Security Guidelines:

As Pakistan prepares for the widespread adoption of 5G technology, PTA will prioritize the development of comprehensive 5G Security Guidelines. These guidelines will address the evolving threat landscape associated with next-generation networks, including aspects such as network slicing, virtualization, supply chain risks, and critical core infrastructure. The objective is to ensure the secure deployment and operation of 5G services, with a focus on architectural integrity, data protection, and end-to-end ecosystem security.

7.3. Anti DDoS Implementation Guidelines

During the April-May 2025 cybersecurity escalation, PTA collaborated with the telecom industry to formulate comprehensive guidelines to mitigate such incidents in future by employing hybrid (combination of on-premises and cloud solutions) and coordinated (inter-operator threat sharing and mitigation synchronization) anti-DDoS solution. This will be further enhanced by maximum possible passive measures and processes to maximize its effectiveness. The final draft will be shared with the industry for consultation after presenting it to the Authority.

7.4. Zero Trust Network Access

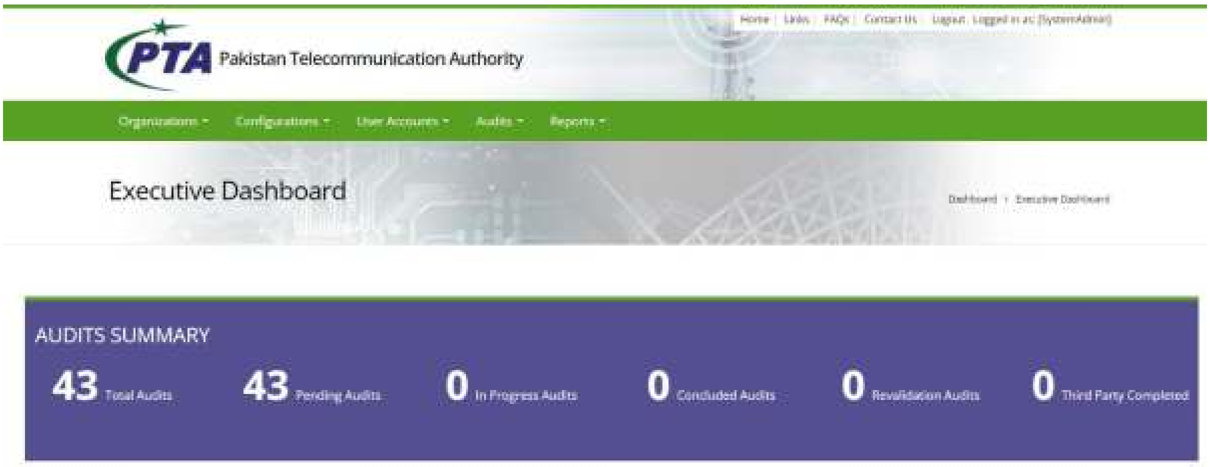
Telecom Cybersecurity Strategy 2023-28 marks this year for the implementation of Zero Trust Network Access. (ZTNA) across the telecom industry. PTA has always led the technology adoption and has implemented the concept before asking the operators to comply. It will further improve the already exemplary cybersecurity measures taken by PTA to protect its critical data and infrastructure from any compromise. This concept being widely adopted worldwide to mitigate diverse and numerous emerging threats. PTA expects the telecom operators to follow the suit in order to make the entire industry safe from new challenges. With 5G, edge computing, remote workforce, and third-party vendors, the perimeter-based defense has dissolved. ZTNA assumes that breaches are highly probable and verifies every access request, regardless of location or user. Adoption of ZTNA will reduce the attack surface, limit lateral movement in the network and protect core assets like switching centers, DNS, and signaling systems in order to protect the national critical infrastructure of Pakistan's Telecom Sector. Rather than relying on traditional cybersecurity measures, ZTNA supports secure access for employees, contractors, and field engineers without relying on outdated VPNs by authenticating users continuously, enforcing least privilege access and preventing compromised credentials from enabling deep access

7.5. In-house Audit Automation Web Application

This application is currently under development and relevant data is being entered to validate its workflow and functionality. It is planned to be fully deployed before the upcoming audit cycle this year. The application is designed to fully automate the third-party audit and PTA's revalidation processes. It covers the entire lifecycle — starting from the engagement of a third-party audit firm by the licensee, all the way through PTA's revalidation audit and final report finalization, including the ranking of telecom operators and cybersecurity audit firms.

By digitizing and automating these steps, the application will simplify the audit process, reduce manual effort and ensure greater transparency. It will also introduce a performance ranking system for both the third-party audit firms and licensees, that will be visible to all relevant stakeholders. This will help promote accountability, performance tracking and informed decision-making across the board.

By digitizing and automating these steps, the application will simplify the audit process, reduce manual effort and ensure greater transparency. It will also introduce a performance ranking system for both the third-party audit firms and the licensees, which will be visible to all relevant stakeholders. This will help promote accountability, performance tracking and informed decision-making across the board.


Home | Links | FAQs | Contact Us | Logout Logged in as (SystemAdmin)
PTA Pakistan Telecommunication Authority
Organizations
Configurations
User Accounts
Audits
Reports
Dashboard / Executive Dashboard

Executive Dashboard

AUDITS SUMMARY

43 Total Audits
43 Pending Audits
0 In Progress Audits
0 Concluded Audits
0 Revalidation Audits
0 Third Party Completed

Figure 7.1: Executive Dashboard View of the Cybersecurity Audit Application

7.6. CTDISR Audit Plan for 2025-26

PTA will issue a formal deadline for all licensees to complete third-party CTDISR audits as part of their mandatory compliance obligations. This directive will follow the release of the revised version of CTDISR, which includes updated requirements aligned with emerging threats and international best practices.

For 2025–26 audit cycle, PTA will:

- Mandate 100% coverage of licensees in Category-I and Category II.
- Randomly select five licensees from each of Category III and Category-IV for revalidation audits.
- Update the audit ranking criteria based on current performance metrics and risk assessments.
- Circulate the revised ranking methodology to all licensees prior to the initiation of the revalidation phase, ensuring transparency and preparedness.

This plan reflects PTA's ongoing commitment to strengthening cybersecurity resilience across all tiers of the national telecom ecosystem through structured oversight and data-driven prioritization

Pakistan
Telecommunication Authority
Cyber Security Directorate
www.pta.gov.pk

Point of Contact:

Dr. Muhammad Mukaram Khan
Director General, Cyber Vigilance Division
Email: mukaramkhan@pta.gov.pk