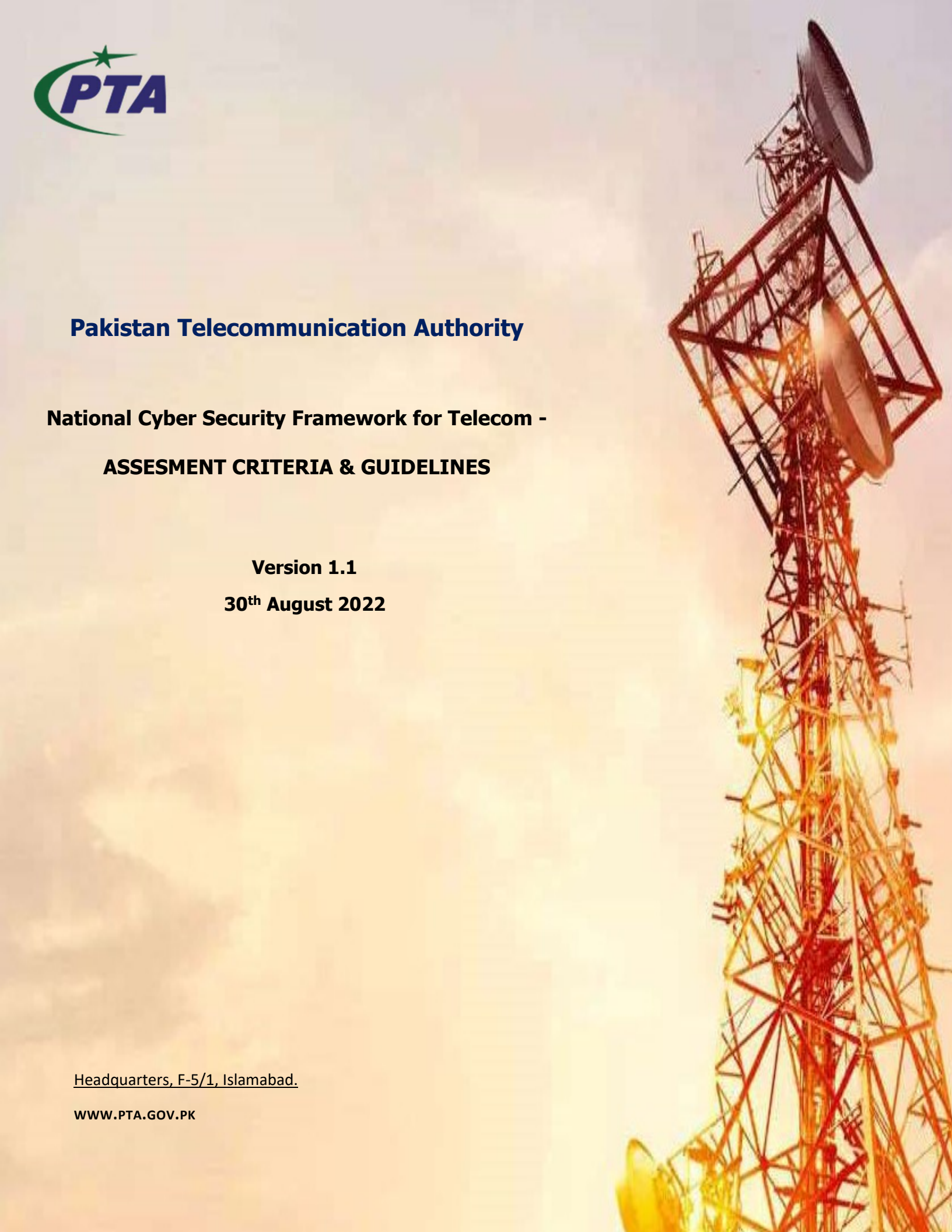

Pakistan Telecommunication Authority

National Cyber Security Framework for Telecom -

ASSESMENT CRITERIA & GUIDELINES

Version 1.1

30th August 2022

Headquarters, F-5/1, Islamabad.

WWW.PTA.GOV.PK

Table of Contents

Overview of CTDISR Requirements

Pakistan Telecommunication Authority (PTA or the Authority) issued the Statutory Notification on September 8, 2020, having reference S.R.O. 1226(I)/2020. In exercise of the powers conferred by Clause, (o) of sub-section (2) of Section 5 of the Pakistan Telecommunication (Re-organization) Act, 1996 (XVII of 1996), the PTA has announced the Critical Telecom Data and Infrastructure Security Regulations (CTDISR) 2020 that needs to be complied with by all PTA Licensees. After the introduction of the CTDISR 2020, PTA has instructed all licensees to have a third-party review of the CTDISR measures from approved auditors and submit the report to the Authority.

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

1. Introduction

This document contains detailed assessment criteria that would act as a guideline for auditors as well as the Licensees when undergoing an Audit. The document contains the list of obligations for both auditors and licensees during the audits. The document also contains the interpretation of CTDISR controls, where necessary, and compensating controls to be accepted along with the required evidence. It is imperative to understand that this framework provides supplementary information and is not intended to override CTDISR regulation (refer to Annexure A), and hence should not be perceived as a replacement for any of the issued regulations and relevant Act.

2. Definitions:

a. **Interpretation:** Each CTDISR clause represents controls to be implemented by the Licensee. “Interpretation” means understanding what each control means and the methodology auditor should use to assess compliance.

b. **Compensating Control:** “Compensating control” means a mechanism that is put in place to satisfy the requirement and mitigate the risk associated with a CTDISR clause, where-by the licensee cannot meet the requirement due to legitimate business and documented technical constraints. Compliance with Compensating Control would only result in Partial compliance.

c. **Supporting Evidence:** “Supporting Evidence” means the information associated with the control for example: Approved documents/snapshots/configurations/walkthroughs and physical inspection.

d. **CTI (Critical Telecom Infrastructure): “**Critical Telecom Infrastructure (CTI)" means equipment/assets whether physical or virtual, which are vital for the provision of telecom licensed services and for storing, processing, and transferring data. National interest includes violation of conventions and treaties adverse damage to the reputation of the country, diplomatic relations and political affiliations, operational efficiency of the security or intelligence operations of military forces, national economy, national infrastructure, and Government functions. It is imperative to mention here that, any system including the intermediatory system that is used to process Critical Data can be classified as Critical Telecom Infrastructure.

e. **CTD (Critical Telecom Data):** "Critical Telecom Data" means Personal data related to PTA licensee, licensee users/customers, Secret customer data belonging to government agencies or institutions, which is retained by the telecom licensee, and such information which is critical for the operations, confidentiality, and security of the licensee telecom systems including voice/data communication of its users/customers being handled by the telecom licensee. Furthermore, any data can result in a financial loss that leads to the inability of organizations to perform their duties or a major loss of competitive abilities or combination thereof, and/or can also be classified as CTD (Critical Telecom Data).

Similarly, any information system where-by Critical Data is stored, processed, or transferred would be referred as Critical Telecom data.

3. Scope of applicability:

The CTDISR applies only to the licensee of PTA. The auditor will be verifying CTDISR controls and ensuring they not only describe but adequately demonstrate the control objectives are being achieved. Licensees will have maximum flexibility on how CTDISR review could be conducted and will be encouraged to apply the guidance in this document so that the various needs of the licensee can be addressed, and the activities can be integrated into broader National Cyber Security Framework for Telecom. Both, Licensee and Cybersecurity audit Firms will be responsible to carry out CTDISR audit as per their respective category (refer to Annexure B).

3.1 Scope of Assessment of Licensee:

Approved Audit firm must agree on the scope of the CTDISR applied to a Licensee in line with the requirements of the PTA including the Geographical scope (e.g., Data centers, sites, locations, etc.) as well as the Technical Scope (e.g., Infrastructure / Network / Applications / Data / Systems etc).

4. Compliance Target

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

a. **Control Level 1 (CL1)**: CL1 includes basic security requirements and controls.
b. **Control Level 2 (CL2)**: CL2 includes advanced security requirements and controls in addition to the existing requirements within CL1.
c. **Control Level 3 (CL3):** CL3 includes requirements and security controls that are more focused on continuous monitoring and continuous process improvements to controls/requirements defined in CL1 and CL2 to achieve compliance with a higher level, compliance with all preceding levels is required.

5. Responsibility of Licensees:

a. **Protection** and retention of Audit Records and relevant evidence for e.g., compliance with regulatory requirements.
b. Document the findings and recommendation and present them to the top management.
c. Define and implement the Internal Audit process to verify compliance against the observations.
d. Ensure that the relevant departments and functions are required to implement the Action Plan.
e. Top management to oversee implementation of the action plan and ensure compliance.

f. Upon receiving preliminary Audit report from PTA, the licensee shall revert back along with relevant evidences of remediation of the findings within timeframe 7 calendar days. In the light of the evidences, PTA will issue final report to the licensee.

g. During the course of audit, the licensee, shall be bound to provide any evidences required by PTA within time-frame of 3 days upon initiation of the request. PTA may grant additional time subject to justifiable technical and business limitations and constraints.

h. The licensee is required to submit the PTA's Final CTDISR Audit/Compliance report to the Chief Executive Officer (CEO) who, after placing the same before the Board of Directors (If applicable), shall revert to Authority i.e., PTA with action items and timelines to comply with observations mentioned in the report.

i. The Licensee will have the right to appeal to Authority, no later than 10 calendar days of issuance of the final report, in case if the licensee does not agree with the findings of the final report. The appeal would be moved through the office of DG CVD, in case of review, no new evidence shall be accepted.

j. Upon completion of audit, Licensee will provide auditor provide risk treatment plan in the light of the conditions as laid in this framework.

k. Findings marked as minor non-compliant will be moved to major non-compliance, in case if compliance is not achieved within the stipulated timeframe.

6. Responsibility of Auditor:

a. Protect the Audit Records from unauthorized access, modification, and destruction.

b. Maintain professional independence and high standards of conduct and character when performing audits.

c. Evidence should be substantial when concluding investigations.

d. Maintain privacy and confidentiality of the information obtained during audit, unless disclosure is required by the authority.

e. In case where auditor finds that a suitable compensating control has been implemented to sufficiently mitigate the risk. Auditor may mark observation as partially compliant.

f. Auditors should only accept discrete, substantial, and documented evidence in physical/digital form).

Failure to comply with obligations mentioned in the assessment criteria (refer to Annexure C) may result in necessary regulatory proceedings against the Licensee or the Audit firm.

7. Compliance Evaluation Criteria

7.1 Definition of Findings

Observation(s)	Observation Definition	Action Plan Guidelines
Non-Compliant	A key control does not exist or is not operating as intended and the financial, operational, and /or reputation risk is more than inconsequential. The process objective to which the control relates is unlikely to be achieved. Protecting human life and preventing harm is the most vital aspect of all security solutions. Hence, any missing control directly/indirectly posing risk to human life will be treated as non-compliant. Corrective action is needed to ensure controls are cost-effective and/or process objectives are achieved.	Action plan to be implemented as a matter of urgency.
Partially Compliant	A control exists, however is poorly designed/implemented or is not functioning as intended and would unlikely lead to major consequences and does not hinder organization's ability to meet their security objectives. However, a compensating control is present to partially address the risk. Corrective action is needed to avoid sole reliance on compensating controls and/or ensure controls are cost-effective and functioning in light of the business requirements. Examples of partial compliance would be if policy does not exist, however is informally communicated and is in practice or policy exists and is not approved or communicated to the management	Action plan to be implemented. Expected to be implemented in no later than 1 month.
Compliant	Controls are operating effectively and can reliably support the achievement of management's business objectives.	No action plan is needed.

7.2 Compliance Review Scoring

The following scoring criteria may be used to determine the “Report Rating” when presenting the report to the top management:

Score	
Non-Complaint	**0**
Partially Compliant	**0.5**
Compliant	**1**

8. Overall Report Rating

Following are the criteria of report rating that may be used by the auditor for the classification of the report in accordance with the risk score performed in the light of the aforementioned "**Compliance Review Criteria".**

Rating of the Report	Compliance Summary	Rating Explanation – Criteria	Risk Score
Unsatisfactory	Non-Compliant deficiencies were noted in the CTDISR Compliance Review. Immediate corrective action required	Controls evaluated are not adequate, appropriate, or effective to provide reasonable assurance that compliance is being managed and objectives are met. Resolution of the weakness(s) would help to avoid a potentially critical negative impact involving loss of material assets, customers' relationships, reputation, critical financial information, or ability to comply with the most important laws, policies, or procedures. In case, if at-least 6 major non-compliances are issued by the auditor. The rating will drop to "Unsatisfactory" in spite of the accumulative score percentage.	Between 50 to 60%
Needs Significant Improvements	Partially Compliant deficiencies are noted in the CTDISR Compliance Review. Timely corrective action is required.	High residual risk exists in a major scope or risk area. The controls evaluated are unlikely to provide reasonable assurance that risks are being managed and objectives met. In case, if maximum number of non-compliance issued by the auditor are between the range of 3 to 5. The rating would drop to "Unsatisfactory" category in spite of the accumulative score percentage.	Between 60% to 75%
Needs Minor Improvements	Adequate System of CTDISR Compliance Review. One or more Partially Compliant observations were noted.	Generally, controls evaluated are adequate, appropriate, and effective to provide reasonable assurance that risks are being managed and objectives should be met. One or more moderate risk observations were noted, with no major impact on the overall system of internal controls. Recommended control enhancements would improve the reliability of controls to support the achievement of management's business objectives. In case, if maximum number of non-compliance issued by the auditor are between the range of 1 to	Between 75 – 90% with at least one major non-compliance.

		2. The rating would drop to “Needs Minor Improvement” category.	
Satisfactory	Satisfactory Controls implemented.	Controls are operating effectively and can reliably support the achievement of management's business objectives. In case if, no major non-compliances are observed. The licensee would fall under the “Satisfactory” category provided that the accumulative score after Partial non-compliances remain above 90%.	90% above with no major non-compliance.

4. Cybersecurity Framework

Controls	Control Level	CTDISR Control Description	Interpretation	Compensating Control	Supporting Documents
4.1	CL1	Licensee shall constitute steering. the committee comprising of high-level representation from key operational areas, to govern and ensure the implementation of Cybersecurity initiatives	The auditor should determine the presence of the steering committee and assess action items proposed by the committee and its current status, as well as the effectiveness of the steering committee in terms of timely approval of IS policies.		Approved organogram, Approved IS Policies Steering committee Minutes of Meeting
4.2	CL1	Keeping in view the requirements of these regulations, necessary policies shall be defined, approved, and communicated by the licensee to its employees and other stakeholders such as partners, contractors, and any other entity having an interface with its telecom data/infrastructure to ensure compliance with these regulations.	he auditor should determine if the following is present: i. Organization-level security policy should be formulated and implemented. ii. The scope of security policy should explicitly cover Critical Telecom Infrastructure and related components, people, and processes. iii. Organization-level and system-level security documentation should be created where required. e.g., system plans, system configurations, network plans, SOPs, etc. iv. The organization-level security policy should be approved by the Board (Senior Management).		Approved IS Policies Steering committee Meeting evidence

			v. Organization-level security documentation should be approved by the CISO/Head of Department. vi. Security policies and documentation, including notification of subsequent changes, should be communicated to all stakeholders on time.		
4.3	CL1	The policies mentioned in point 4(2) shall be regularly reviewed by the licensee at planned intervals or upon any significant change/event	Auditors should assess if the policies are reviewed at planned intervals and are periodically updated in the light of the organization's internal "Information Security Policy". The auditor should also review if the criteria of the policy review have been clearly defined in the document.		Evidence of Policy Review Information Security Policy
4.4	CL1	Roles and responsibilities for cybersecurity shall be clearly defined and allocated by the licensee	The auditor should inspect the Roles and responsibilities matrix (R&R) or RACI and if the same has been communicated and approved by the senior management.		Approved R&R matrix. RACI Chart
4.5	CL1	Critical data and Infrastructure shall be identified and designated by the licensee for ensuring cybersecurity	Auditor should assess if the Licensee has performed asset discovery/service-based classification to identify critical data and infrastructure. The definitions of CTI/CTD has been provided in the definitions section.		Asset inventory Information Classification Policy Information Classification Document

4.6	CL1	Licensee shall maintain appropriate contact with relevant stakeholders to ensure cybersecurity	Auditor should inspect if a designated role is assigned to an individual or group of individuals in the organization who will liaison with the regulator, industry, and other relevant entities on matters of cyber security on behalf of the organization. An auditor should also check for proper documentation and authorization of the job has been assigned. Furthermore, Auditors must ensure that: i. All relevant Telecom stakeholder groups should be identified along with documented applicable cyber security requirements and expectations. This may include but is not limited to Employees, Contractors, Customers, Subscribers, LDIs, Call Centers, Franchises, Telecom Digital Service Providers, including technical and non-technical staff. ii. All relevant Telecom stakeholder groups should be made aware of their cyber security		R&R Matrix Approved JD of Individuals

			responsibilities, due diligence, and due care in the protection of critical assets.		
4.7	CL1	Employees and contractors shall be contractually bound by the licensee to relevant cybersecurity requirements with a formal and communicated disciplinary process in place for compliance	The auditor should assess if a formal sign-off and undertaking from the contractor is documented and has been communicated to the management.		Third-party Contract NDA Vendor or third-party Policy Vendor onboarding documentation/policy
4.8	CL1	To ensure proper implementation of security measures, employees including relevant contractors/partners shall be made aware by the licensee of the security policies and requirements through awareness sessions, education, and training	The auditor should determine that the activities in the awareness program should be scheduled at planned intervals in light of the organization's information security policy so that the activities are repeated and cover new employees and contractors' employees on the client site. The program should be updated regularly so it stays in line with organizational policies and procedures and should be built on the basis of lessons learned from information security incidents. Auditor should also inspect if Phishing simulation exercise has been carried out and actions that have been executed on the basis of the results obtained from the exercise.		Evidence of advisories and Cybersecurity awareness campaigns for employees/contractors/partners

4.9	CL1	Where applicable the licensee shall also provide Cybersecurity awareness to its customers/subscribers for safeguarding against security threats and incidents	The auditor should assess, if Licensee, periodically disseminates security advisories/security alerts via its communication channels such as email/SMS/social media platforms for providing Security awareness to customers/subscribers as defined Information Security Strategy document or relevant policy document. Licensee should also communicate to subscriber/customer if a security breach has taken place affecting subscriber/customers data. The licensee should maintain evidence of such communications.		Evidence of advisories and Cybersecurity awareness campaigns for customers. Information Security Strategy document Evidence of communication regarding the security breach for that particular customer

5. Physical and Environmental Security

Controls	Control Level	CTDISR Control Description	Interpretation	Compensating Control	Supporting Documents
5.1	CL1	Physical security for secure 'areas shall be designed and implemented by the licensee	Auditor to assess, List of authorized users and asset in/out details should be maintained.		Approved List of authorized users for visiting secured areas. Gate pass inventory. Automated/manual log registry Datacenter policy
5.2	CL1	Security perimeters shall be defined by the licensee for secure areas	Security perimeters should be defined and used to protect areas that contain either sensitive or critical information and information processing facilities		Approved Data center policy
5.3	CL1	Physical access to assets in secure areas shall be managed and protected by the licensee	The licensee should have oversight of the physical security. Even in case, if the access to the secure areas is outsourced to a third party. Representatives of the Licensee should be available on-site for an oversight.	Approved JD of employee overseeing third-party vendor managing secured areas. OR RFID entry/exit to be mapped with SIEM and use cases should be formulated for anomaly detection.	NDA Risk acceptance document
5.4	CL1	Only authorized personnel shall be provided access to secure areas	The list of authorized users should be displayed on the entrance duly signed and reviewed/inspected on regular basis as per the		Approved List of authorized users for visiting secured areas Approval emails of vendor visits Log of all personnel entering the secure areas along with the purpose of the visit

			organization's internal security policy. Server rooms are properly locked, and all RFID is functioning well.		
5.5	CL2	Licensee shall ensure that access points where unauthorized persons can enter the secure area are be controlled and if possible isolated from CTI	The CTI systems must be locked in server farms and separated from other servers. In case of shared data centers, (systems of several organizations are sited in the same data center as telecommunications facilities), the Licensees should implement appropriate measures to protect customers' information stored in their systems. Such systems should have additional security in place, e.g., by being located in a separate secured area and appropriate physical security controls		Electronic/physical logging CCTV coverage of secure area without blind spots
5.6	CL1	A physical log book or electronic audit trail shall be maintained and monitored by the licensee for personnel accessing secure areas	Details of the logbook should be reconciled, mapped with work orders, and frequently audited. Moreover, a data retention policy should be developed for the		Electronic/physical logging. Policy for authorized users accessing CTI / secured areas

			retention of logbooks in both physical/electronic forms.		
5.7	CL2	The physical environment of secure areas shall have monitoring/ surveillance by the licensee to prevent and respond to a cybersecurity incident	The auditor should inspect the oversight mechanism by the licensee for monitoring/surveillance of the physical environment even in the case of the licensee has outsourced the physical security to a third party. Find answers to the following: 1) Can the Detective Controls resources detect without being detected? 2) Can Detective controls identify an intrusion coming from a distance? 3) When is monitoring active (time/ duration)? 4) Where and how are records kept and analyzed?	2x representatives of the licensee to be present on-site for oversight can be accepted as compensating control.	Automated/manual log registry. Review of 360 Degree CCTV coverage Review of blind spots, Piggy backing threat, etc.
5.8	CL1	Procedures for working in secure areas shall be designed and implemented to safeguard against cybersecurity incidents	The auditor should assess if staff/vendors accessing CTI, or working on details in the data center are formally informed and approved by the management.		Approved documented procedure for accessing the CTI.

5.9	CL2	Physical protection against natural disasters, hazards, malicious attacks, or accidents shall be designed and applied by the licensee for secure areas	Power generation should be above ground level to avoid uncertainty from the natural disaster. The auditor should review that the power supply facilities in isolated areas, such as mobile base stations, should preferably provide an uninterruptible power supply with capacity for complete load and capable of withstanding primary power supply failures for the duration of likely outages. If that is impossible, a mechanism to provide uninterruptible power to critical equipment should be installed. Batteries may need to be augmented with a private electric generator, especially in isolated areas. Any equipment room should have adequate heating, ventilation, and air conditioning (HVAC) services to ensure that external environmental conditions do not result in equipment operating		A maintenance agreement with a third party. Last data center review report performed by operator IS department.

			outside manufacturers' guidelines.		
5.10.	CL1	Secure areas shall be protected from power failures and other disruptions caused by failures in supporting utilities	Auditors should ensure that supporting utilities be appraised regularly for their capacity to meet business growth and interactions with other utilities. All supporting utilities should be inspected and tested regularly to ensure their proper functioning. Maintenance schedules/records must be reviewed. Interviews with people who performed these tasks - to see their knowledge of the specific hazards and issues. Fire-fighting provision - Enough/Appropriate and what are the Alternate? HVAC controls should be connected to an uninterruptable power supply to ensure that the loss of power does not impact the operating environment.		Generator/UPS service documents Maintenance schedules Records of maintenance/qualification / capabilities of the staff

5.11	CL1	Power and telecommunication cabling for CTI shall be protected from interception, interference, or damage	Power and Telecommunication cabling must be structured, server racks must be locked to protect from interception, interference, or damage. Cabling should be implemented in such a way that it ensures that wire-tapping and eavesdropping devices or any alteration to the cabling can be detected either using active means or regular audits of access points.		A maintenance agreement with a third party. Last data center assessment report performed by operator's internal audit/security team or third party.
5.12	CL1	Maintenance for Equipment in secure areas shall be correctly carried out by the licensee for its availability and integrity.	The auditor must ensure that equipment should be maintained in accordance with the supplier's recommended service intervals and specifications		A maintenance agreement with a third party. Gate pass inventory. Automated/manual log registry.
5.13	CL1	Appropriate protection shall be applied by the licensee at secure areas for unattended equipment to safeguard against unauthorized access	The auditor must ensure that an appropriate locking mechanism is in place, e.g., a password-protected screen saver; log–off from application or network services when no longer needed.		Automated/manual log registry.
5.14	CL1	Assets pertaining to CTI shall not be taken off-site without proper authorization	The licensee must record the assets entry and exit, and maintain the gate pass record.		Gate pass inventory. Approval against each gate passes entry.

5.15	CL2	Appropriate security shall be applied by the licensee to off-site CTI assets taking into account risks outside the licensee's premises.	The licensee must oversee and maintain all assets entry and exit record. The record may be integrated with Security monitoring solution for a holistic view.		Gate pass inventory. Approval against each gate passes entry.
5.16	CL1	Clear desk policy for papers and removable storage media and clear screen policy for critical data processing facilities shall be adopted by the licensee	Auditors must ensure that sensitive and critical business information e.g., on paper or electronic storage media, should be locked away (ideally in a safe or cabinet or other forms of security furniture) when not required, especially when the office is vacated, unattended documents on shared printers to be shred.		Emails on security awareness for clear desk, removable storage, and clear screen policy. Spot Check Records etc.

6. Monitoring

Controls	Control Level	CTDISR Control Description	Interpretation	Compensating Control	Supporting Documents
6.1	CL1	Automated network monitoring systems shall be put in place by the licensee to detect unauthorized/malicious users, connections, devices, and software with preventive action	Ensure the critical infrastructure is integrated with the SIEM solution, Anomaly detection systems, Advanced Persistent Threat detection, Endpoint detection solutions, etc. The auditor should assess if security controls/solutions are integrated with SIEM for centralized monitoring and a holistic view. Correlation rules should be built to identify intrusions and incidents across different security solutions. This would also prevent alert fatigue where-by security analysts have to manually review output from each security		License agreements of relevant security controls deployed by the licensee. Walkthrough of security controls and SIEM solution

			control/solution and manually correlate them for incidents.		
6.2	CL1	Authority may issue guidelines/specifications for deployment, operations, management, and access to information/logs of said Monitoring Systems	The auditor should assess if organization's log retention policies are in line with the PECA 2016 section 32 Retention of Traffic, License conditions, or directions issued by the Authority, in case where the authority has not issued specific guidelines for retention of data, alignment with the organization's; internal policy should be assessed.		IAM matrix for log Storage. Logging policy, Operational manual Review of record maintenance in secure rooms
6.3	CL2	CTI shall be monitored to identify and prevent eavesdropping', unauthorized access, and cyber threats	The auditor should assess the following: i. A dedicated and secure facility (SOC) should be designed for centralized security logging and monitoring operations. ii. A secure centralized logging platform (SIEM) should be	SMEs who cannot manage a dedicated facility may opt for managed services and other cost-effective solutions as per the organization's budget. The Authority's directions and support be acquired from time to time. In this regard,	Document for security logging and monitoring. Identity Access management document. Review of SIEM, DLP, and Firewalls

			implemented and CTI systems should be configured to save event logs to the facility as soon as possible after each event occurs.	Authority may provide hand-holding and capacity building for its licensees. Opensource, customized indigenous tools may be used for the implementation of a centralized platform.	
6.4	CL2	Licensee shall ensure that event logs for user activities, exceptions, faults, and cybersecurity incidents are produced, stored, and regularly reviewed to identify and mitigate security threats and incidents	Auditor to assess if events/logs of all critical systems are properly recorded and integrity of the same is protected. Auditor may also assess log levels being recorded that would provide assistance when investigating security incidents.		IAM matrix for log Storage. Data retention policy Incident handling and management policy
6.5	CL2	Event logs shall include the following when relevant: - User IDs - Successful and rejected system access attempts - System activities. - Use of system utilities and applications - Records of any transactions executed by users - Data files accessed and kind of	Auditor to assess if events/logs of all critical systems defined as per organizations information security policy/Log retention policy are properly recorded. In case, where-by a device does not support		Evidence for alert and integration with SIEM solution. Evidence of actions taken/reviewed List of exceptions to be documented.

		access - Timestamp and details of key events - Identity of device - Location - Records of successful and rejected data and other resource access attempts - System configuration changes - Network addresses and protocols - Alarms raised by the access control system - Activation and de-activation of protection systems such as Anti-Virus and Intrusion detection systems	logging of certain events due to technical limitations. In that case, exceptions should be properly documented. Auditor should also ensure 360-degree coverage of Critical Systems and various types of logs, NetFlow traffic, IP Traffic etc. required for incident handling purposes.		
6.6	CL2	Logging facilities and log information shall be protected by the licensee against tampering and unauthorized access	Ensure that sensitive commands allowing users to modify or delete logging are disabled by default. Administrator access should be properly logged and recorded and duly integrated with a security incident and event Management (SIEM) solution.	Real-time backups of logs at the alternative site. OR Privileged Access Management (PAM)	Access control policy Logs retention policy
6.7	CL3	Logs from multiple sensors and sources shall be aggregated and Correlated by the licensee to understand attack targets and methods	Auditors should assess that a centralized platform should support event log aggregation, correlation, analytics, human-readable and understandable dashboards,		Evidence of integration with SIEM. Custom alerts and rules on SIEM

			notification, and alerting from multiple sensors and sources to establish real-time security context, prioritize audits, and focus investigations.		
6.8	CL2	System administrators shall not have permission to erase or deactivate logs of their activities and controls shall be in place to audit their activities	Audit logs for system administrator activity should be monitored by a separate function with logging to be duly integrated with SIEM or anomaly detection solution. The principle of least privilege should be applied whereas, access to logs should be restricted to Need to know basis. PAM solution may be configured to prevent system administrators from deleting audit logs.	In case, if audit logs are being retained with Syslog servers, SIEMs, log aggregators, ELK stack etc. It may be treated as a compensating control.	Alert on SIEM against log deletions. Log retention policy.

6.9	CL1	Clock synchronization shall be performed to ensure that clocks within an organization are synchronized to a single reference time.	The auditor should assess if the NTP protocol has been configured and appropriated to keep all servers in synchronization with the master clock.		Evidence of NTP configuration and information security policy.
6.10.	CL1	Vulnerability scans shall be carried out by the licensee to perform countermeasures against vulnerabilities.	The auditor should assess if vulnerability assessment is being performed across the organization's critical assets at least once annually or in accordance with the organization's internal policy. The auditor should also assess if the identified vulnerabilities were reported to the management and action plan to resolve the identified vulnerabilities was communicated and acted upon. The auditor should also assess if all critical assets have received sufficient coverage.		Vulnerability Assessment Policy Vulnerability Assessment Report Vulnerability Assessment tracking sheet Management Action Plan against the identified vulnerabilities

7. Malware Protection

Controls	Control Level	CTDISR Control Description	Interpretation	Compensating Control	Supporting Documents
7.1	CL2	Critical telecom infrastructure shall be protected against malware by the licensee	Ensure that antivirus and other security tools are implemented to protect the organization from malware. Coverage of the antivirus/antimalware/Advanced Persistent Threat Protection solution should be extended to all systems including endpoints, servers and network devices, as one weak link can be a potential entry point to the critical telecom infrastructure. Review the awareness activities that are being done to make people aware of how to protect themselves from malicious activity, cybercrime, malware, and sophisticated cyber threats. Auditor should map asset list with Antivirus/EDR to assess coverage across assets.		The license agreements of antivirus/EDR and other anti-malware security tools. Patch management tools
7.2	CL2	Automated malware protection shall be applied by the licensee to identify and	The auditor should assess that a malware protection solution for Endpoints and Network Traffic is present.		AV policies. EDR policy. Evidence of review of the logs

		eliminate malicious software activity	The auditor should also ensure that the Malware protection solution is being regularly updated and relevant endpoints are being scanned on regular basis. The scan must include but should not be limited to any files received over networks or via any storage medium; email attachments and web pages. The auditor should also assess if sufficient coverage across CTI is present. Specific responsibilities for the proper maintenance of these tools – must be reviewed (as in many cases the logs are not reviewed by the orchestrator and many systems remains unpatched / non-updated, etc.		Review of Anti-malware updates regularly
7.3	CL1	A policy shall be formulated and enforced by the licensee to prohibit the use of unlicensed 'and unauthorized software.	The auditor should assess if a documented policy is in place that prevents and prohibits the use of unlicensed/unauthorized software without prior initiation of the management. The auditor should also review if there is a mechanism in place that periodically analyzes systems for unauthorized software or	Application whitelisting Solutions may also be treated as compensating control.	List of approved Whitelist and backlists software. The policy of blocking Potentially Unwanted applications (PUA).

			a preventative control that prevents users from installing unauthorized/unlicensed software.		
7.4	CL2	A vulnerability management plan shall be developed and implemented by the licensee	Ensure the vulnerability assessment plan is available and approved by the management. Review the assessment results and actions taken/implemented for effectiveness		Vulnerability assessment plan Vulnerability assessment tracker Records of assessment results
7.5	CL2	For systems and software being used by the licensee, exploitation of related technical vulnerabilities shall be avoided by obtaining their information in a timely fashion and taking appropriate measures to address associated risks	The auditor should assess if the organization has an internal Incident Response Team that is in sync with PTA CERT. The team should periodically review and assess threats against the systems and software being used by the licensee. Furthermore, the auditor should also assess if the organization maintains a list of software being used and if the list of periodically updated.	Subscription to any Open-source or Commercial Threat Intelligence Platform	Vulnerability assessment plan Vulnerability assessment tracker follow-up and closure of findings
7.6	CL1	A formal policy shall be formulated and enforced by the licensee to protect against risks associated with data and software obtained from external networks or any other medium	A formal policy should be in place to prohibit the use of unauthorized software. Appropriate controls must be in place to prevent and detect the use of unauthorized software (e.g., application whitelisting)		List of whitelisted software Software installation process/record of approvals

7.7	CL2	Employees shall be made aware through training and awareness sessions by the licensee to safeguard against malware distributed using the internet.	Auditors should assess the presence of an internal security awareness program and the content encompasses sufficient coverage of common types of social engineering tricks to lure the victim into installing malicious software. Auditors should also assess, the percentage of employees that have gone through security awareness sessions and ensure that maximum coverage has been conducted.		Evidence of Cyber security Seminar/Training/awareness sessions including press releases, internal emails, or pictures. Licensee's policies/procedures etc. for raising security awareness.
7.8	CL1	Procedures and responsibilities shall be defined by the licensee to deal with malware protection on CTI as well as carrying out required training.	The auditor should assess if the information management/response policy contains an R&R matrix or RACI Chart which documents the procedures, roles, and responsibilities of the licensee to deal with malware/APTs. The auditor should assess if a security training program exists for employees and the coverage Awareness activities to protect communications service users from unsolicited communications, cybercrime, malware, and similar.		Incident Management/Response policy Evidence of security training and awareness conducted internally or from external third parties.

7.9	CL3	An appropriate business continuity plan shall be prepared by the licensee for recovering from malware attacks including necessary data/software backup and recovery arrangements	Auditors should assess if the organization has a BCP plan which should also include playbooks that could help the organization from recovering from malware attacks. Review the business impact analysis used for identifying the critical activities/services/systems / applications etc. The BCP should be reviewed to ensure that for graceful degradation of service with priority given to emergency services and the least critical services being degraded or stopped in priority order. The business continuity plan should contain a provision for information security continuity to protect the information in various forms. In developing and implementing the business continuity plan, licensees should consider the inclusion of a disaster recovery plan (DRP) for telecommunications services and ensure the essential communications of telecommunications service customers.	For SMEs the runbooks, disaster recovery planning, and incident response plan – can be created to ensure the following: 1) Critical activities / data / applications / systems / hardware etc. are identified 2) The impacts of – these if not available - for a certain period – on the provision of services to the customers 3) The define prioritized period for recovery - in case of disaster/disruption 4) The steps to be followed for the recovery within that period.	Approved BCP plan Data retention policy.

8 Data Protection

Controls	Control Level	CTDISR Control Description	Interpretation	Compensating Control	Supporting Documents
8.1	CL1	Privacy shall be ensured for critical telecom data stored by the licensee and it shall only be used for the purpose for which it was obtained from customers/users	The auditor should assess if the licensee has published a privacy policy and if it the same been explicitly communicated to customers. Privacy policy should be communicated at the time of onboarding of customers such as issuance of SIM card, Internet connection, enrolling corporate customers etc. Whereas, for all customers that have already been onboarded without privacy policy, the same should be disseminated to every customer through SMS, Email, Phone etc. Privacy policy should state the type of data to be collected, why it is being collected, the retention policy and how it will be used. Similarly, any change in privacy policy should be communicated to all the customers.	If the licensee has communicated privacy policy through alternative channels such as IVR on the customer support helpline, website or email and has not incorporated it as a part of onboarding process or has not explicitly communicated privacy policy to all customers, it can qualify as compensating control.	Privacy Policy Evidence of Privacy Policy being communicated to customers.
8.2	CL2	Data shall be protected from unauthorized disclosure, modification, loss, and destruction	The auditor should assess if the approved Identity access management (IAM) matrix is in		Access Control policy/guidelines for CTI User onboarding Document

			place to prevent unauthorized disclosure, modifications, and loss.		
8.3	CL1	Licensed data retention timeframes shall be observed and where required clarity shall be sought from the Authority for the retention timeframe of any data for which a retention timeframe is not mentioned in the license	The auditor should assess if Data Retention timelines are in accordance with the Licensee conditions. Where-by Licensee conditions or Authority Guidelines do not specify data retention timelines for specific systems such as SIEM, EDR, etc., in that case, alignment with the Organization internal policy should be assessed.		Approved data retention policy.
8.4	CL1	Data shall be appropriately classified by the licensee to ensure that personal and critical telecom data receive the appropriate level of protection	The auditor should assess if the asset/information classification policy is in place and if the licensee has already performed classification of CTI (Critical Telecom Infrastructure) and CTD (Critical Telecom Data).		Approved Data classification document Asset/Information Classification Policy
8.5	CL2	Consideration shall be given to the possibility of deterioration of storage media, and data handling procedures shall be made accordingly to avoid data loss	The auditor should assess if special consideration is being given to factors that can deteriorate or reduce the effectiveness of restoration of storage media. This can include Environmental factors or physical damage to the storage media. The auditor should also assess if storage media equipment is being inspected and tested on regular basis.		Email Policy for data protection Data storage policy and procedure

8.6	CL2	Storage media shall be stored in a safe and secure environment in line with relevant manufacturer requirements	The auditor should assess if the storage and handling of assets associated with data are in line with the manufacturer's requirements. This may include protecting storage media from environmental factors (Moisture, heat, electromagnetic fields) or physical damage during transit which may reduce the likelihood of restoring the storage media.		Ensure Storage media is physically secure. Physical security policy
8.7	CL2	Storage media shall be disposed of securely to avoid any unauthorized release of data.	Auditors should assess if storage media when deleted or disposed of, are handled securely and removed from the asset inventory. All items of equipment containing storage media should be verified to ensure that any sensitive data and licensed software have been removed or securely overwritten Auditors should also assess if regular reviews of asset inventory are being conducted and if the process of installing and removing assets is automatically enforced.		Storage media disposal policy or guidelines Evidence and record of disposed/sanitized media Sample review of the storage location of (to be disposed-off) media – review/test if it was adequately sanitized (e.g., connect and test for data, etc.)
8.8	CL2	Data breaches shall be avoided during the physical transfer of storage media	Auditors should assess if information transfer rules, procedures or agreements are in place for transferring data within facilities and across any external entities.		Data storage and media Chain of Custody forms for transfer of physical media Policy for acceptable use of information transfer facilities

			The auditor should assess if the controls are in place to ensure traceability and if the Chain of Custody was being maintained during the transfer of Physical media. If responsibilities and liabilities are documented in an event of loss of Physical storage media or data transfer.		Check that mobile and removable media devices are protected with cryptographic controls using strong algorithms and sufficient key length etc.
8.9	CL2	A policy shall be made and enforced to protect critical data access, process or store at teleworking sites	Auditors should assess if a policy is in place and enforced to protect information that is being accessed by employees remotely. Auditors should also assess if appropriate controls are in place to identify, detect and prevent unauthorized access through identity theft.		Teleworking policy
8.10.	CL3	Privacy and protection of personal and critical telecom data, either at rest or in transit shall be ensured and the licensee may use encryption to avoid any data breach	For this clause to be compliant, Personal and critical telecom data should either be encrypted in transit or at rest. In case, if either is true, the auditor should treat it as compliant. information consists of data transmitted between any two points in an electronic formation as well as metadata of each transmission, e.g., positioning data of sender and receiver. Regardless of how the information is transmitted and whether it is cached or stored during		Evidence of all data at rest or in transit is encrypted.

			transmission, information should always be appropriately protected.		
8.11	CL1	An organization-wide data policy shall be prepared and implemented by the licensee to ensure the protection and privacy of personal and critical data and prevent its unauthorized release/access.	Auditors should assess if the organization has issued a policy for preventing data from unauthorized access, destruction, and unauthorized release. The auditor should also assess if guidelines have been issued for disposal of personal or critical data handling, the chain of custody, secure disposal, and preventing manipulation of records.		Data protection policy document.
8.12	CL1	No Data shall be stored beyond the country's geographical boundaries without the approval of the Authority	"Data" refers to the personal data of Citizens or Customers/users data or any data related to Critical Infrastructure classified in accordance with the organization's internal information classification policy. Auditors should closely review if any data is being shared/handled by the outsourcing partners (of the licensee). In case if the data is being hosted on the Cloud or by a third party vendor/supplier etc. Auditor will review, if the Licensee has a clear policy communicated on geographical locations and ensure		Data Protection Policy document mandating data localization for Critical Telecom Data. Approval of authority of data stored outside geographical boundaries (if any) Signed Undertaking document indicating that no CTD has been stored outside the geographical boundaries.

			that partner/vendor can provide sufficient evidence of data storage – in compliance to this requirement. Auditor should assess if the licensee has submitted undertaking before the authority ensuring that Critical Telecom Data (CTD) will not be stored outside of geographical boundaries of Pakistan.		

9. Critical Telecom Infrastructure Management

Controls	Control Level	CTDISR Control Description	Interpretation	Compensating Control	Supporting Documents
9.1	CL1	Assets shall be classified by the licensee to ensure that Critical Telecom Infrastructure receives the appropriate level of protection	The auditor should assess if the asset/information classification policy is in place and if the licensee has already performed classification of CTI (Critical Telecom Infrastructure) and CTD (Critical Telecom Data). The auditor should also assess if appropriate security controls are in place for CTI.		Asset inventory Asset Classification Policy Asset Classification Document Evidence of CTI integration with Syslog servers, SIEMs, log aggregators, ELK stacks, etc.
9.2	CL2	Licensee shall ensure that Assets associated with Critical Telecom Infrastructure are inventoried with responsibility assigned to either an individual or a designated entity to ensure that associated cyber threats such as technical vulnerabilities are effectively managed	In accordance to organization internal policy, the auditor should assess if an inventory of assets part of Critical Telecom Infrastructure is being maintained and periodically updated. Auditors should ensure that regular reviews are being conducted to ensure consistency of the data. Inventory updates are automatically enforced in case of deployment, modification, and removal of an asset belonging to Critical Telecom Infrastructure.		Internal/External VAPT report Action plan on findings Implementation review update reports etc.
9.3	CL1	Rules shall be documented and implemented by the licensee for acceptable use, transfer, removal, and disposition of assets	The auditor should ensure that all assets being transferred, removed, or disposed of are not without the approval of the	.	Access control policy. Asset disposal policy

			management as defined under the organization's asset disposal policy.		
9.4	CL1	Employees or external users having access to assets related to critical infrastructure, shall be made aware by the licensee of their Cybersecurity requirements	Ensure the cybersecurity requirements are duly communicated and signoff by the employees/external user having logical/physical access to CTI is documented and regularly updated.		Approved Data Center Personnel access list. Access control policy
9.5	CL1	An access control policy shall be established, documented, and enforced by the licensee to prevent unauthorized access to CTI.	Ensure that appropriate access controls are implemented/deployed to prevent unauthorized access.		Access control policy Access Control Matrix Physical inspection Access logs
9.6	CL1	A policy shall be formulated and enforced by the licensee to enable only authorized access to Network, and Network services	Auditor should inspect if the security policy is formulated and enforced to enable authorized users to log into CTI. Security protocols such as TACACS, TACACS+ should be used for providing centralized authentication to the users attempting to gain access to CTI. Logical and physical segregation of the network should performed to prevent lateral movement in case of unauthorized access.	If the licensee has enabled Multi-factor authentication for all devices part of CTI, it can be treated as a compensating control.	BYOD policy (if applicable) Evidence for Physical/Logical network segregation Access logs Security logs
9.7	CL3	A user access mechanism shall be implemented by the licensee to enable the assignment of user	Auditors should assess if user access roles are in-line with the business requirements while	If the licensee has enabled Multi-factor	

		rights and access privileges for systems and services.	giving due consideration to the Need to know and segregation of duties principle. Access rights are periodically reviewed, updated, and modified in accordance with the organization's access control policy. Similarly, auditor should inspect if Security protocols such as TACACS, TACACS+ are implemented used for providing centralized authentication to the users attempting to gain access to CTI. Auditor should also assess if the same has been integrated with any Security Monitoring solution. Furthermore to this, if correlation rules have been formulated to monitor sensitive commands such as drop commands, log removal etc.	authentication for all devices part of CTI, it can be treated as a compensating control.	
9.8	CL1	A password management mechanism shall be put in place by the licensee to ensure quality passwords	"Quality Passwords" refers to a strong password, the definition of a strong password should be treated in accordance with NIST 800-63b or ZXCVN entropy.	Password less authentication includes Biometric fingerprints, Facial Recognition, Token based authentication, etc.	Password Policy Inspection of Password Manager (if any)

9.9	CL1	Employees shall be made accountable for protecting their secret authenticated information	"Secret authenticated information" refers to any data that an organization treats as confidential, sensitive, etc. as per their information classification policy or data related to customer/user and critical telecom infrastructure.		Copy of Non-Disclosure Agreements on sampling basis.
9.10.	CL2	It shall be ensured by the licensee that Critical Telecom Infrastructure shall not be compromised to prevent unauthorized access to critical telecom data including real-time data /voice connections	The auditor should assess if the licensee has taken necessary steps to prevent unauthorized access to critical telecom data including real-time data/voice connections. In addition to it, the auditor should also assess Telecom Network to ensure that licensee has taken adequate safeguards for securing SS7, Diameter, GTP, SIP or H.323 protocols. The network should be assessed in accordance with the following standards: FS.07 SS7 and SIGTRAN Network Security FS 11 SS7 Filtering and Monitoring FS.19 Diameter Interconnect Security IR.77 Inter-Operator IP Backbone security requirements, IR.82 (SS7) GSMA interconnection security and relevant GSMA standards.		

9.11	CL3	Licensee shall ensure that patches for Critical vulnerabilities are applied and verified within 72 hours	Subject to reasonable/legitimate technical or documented business constraints, all systems with critical vulnerabilities. The definition of Critical vulnerabilities should be determined in accordance with the CVSS score (ref) or the organization's internal risk scoring criteria.	If an unpatched system with Critical vulnerabilities is to be segregated in a manner that they are not exposed to the internet, it may be accepted as compensating control.	Patch Management Policy List of risks accepted by the management due to subject to reasonable/legitimate technical or documented business constraints. Risk acceptance criteria
9.12	CL2	Licensee shall only use Vendor-supported software versions for systems and applications that store Critical Data	The auditor should assess any End-of-life software that is not in use within the organization. The auditor should also assess if the organization has an asset discovery mechanism in place to automatically identify the end-of-life systems and end-of-life software running on these systems. Similarly, if an internal audit team or security team has documented end-of-life systems as a risk.	End-of-life system isolated from the network can be treated as compensating control.	Asset discovery document Repository of software Walkthrough of asset management tool (if any)
9.13	CL3	The licensee shall validate and audit all the privileged accounts on an annual or more frequent basis	The auditor should ensure that all privileged accounts are being monitored at least on an annual basis or frequently in accordance with the organization's internal security policy. The auditor should assess if privileged access rights for each system or process are based		Policy document Evidence for Access control Review record of PAM or tools Review Audit Trails for the privileged accounts Review log management system and Log files

			upon the Need to know and least-privileged principle. Auditors should assess the need for privileged access on a need basis and an event-by-event basis. The auditor should assess if the organization's policy covers requirements for expiration/revocation of privileged access rights. Similarly, revocation of privileged access is automatically enforced as soon as an employee leaves the organization. Similarly, the auditor should determine if logging of all privileged access to the system for audit purposes is enabled.		
9.14	CL3	Multi-factor authentication shall be implemented for all users accessing any part of Critical Telecom Infrastructure	The auditor should assess all critical systems not limited to telecom are being accessed through multi-factor authentication both externally and internally.		

10. Backup

Controls	Control Level	CTDISR Control Description	Interpretation	Compensating Control	Supporting Documents
10.1	CL2	Backup copies of data, relevant software, and system images related to critical data and CTI, shall be taken and tested regularly and upon any significant change by the licensee	"Backup copies" is only relevant to the critical infrastructure and Telecom data and user/customer data and hence the same has to be verified by the auditor. Backups should be conducted frequently and should also be included as a part of the policy. The policy/procedure should be clearly defining the below: a) Scope and schedule of backups; b) Backup methods and data formats, including encryption, if relevant; c) Retention periods for backup data; d) Process for verifying the integrity of backup data; e) Process and timescales involved in restoring data from backup;		Physical inspection of the end-to-end backup process Approved Change request forms. Review of asset classification identifying CTI assets. Backup Policy/Procedures Backup Testing & restoration results

			f) Back up testing process capabilities. g) The storage location of backups.		
10.2	CL2	The backup shall be stored by the licensee at a remote site located at a suitable distance from the primary site	Full Back up of critical data should be stored in a remote location, not within the radius of 100KM of the primary backup site.		Backup Policy/Procedures
10.3	CL2	A copy of backups must be disconnected from computers and networks and shall be placed in a non-rewritable and non-erasable manner	The auditor should inspect if the Critical data has backed up Offline storage in a non-rewritable and non-erasable manner. Backup storage device should be immutable, in which the data cannot be altered and that stores the data in a write once, read many (WORM) state.	If backups for Critical data are Physically and logically segregated from the network, however they are not disconnected from the network, they may be accepted as a compensating control. Critical data backup on an external storage device/ drive with strong encryption, as per international standards (NIST SP 800-175B, FIPS approved) may also be accepted as compensating control.	End to end walk through the backup process Backup Testing & restoration results

10.4	CL3	Backup arrangements shall cover all system information, applications, and data necessary for recovery to ensure business and service continuity	Backup is relevant to the critical infrastructure and Telecom data and user/customer data and hence the same has to be verified by the auditor.		DR Drill document. Logs of testing BCP Testing reports
10.5	CL1	Appropriate retention timeframe for critical data shall be defined keeping in view the relevant regulatory requirements	The auditor should assess if Data Retention timelines are in accordance with the Licensee conditions. Where-by Licensee conditions or Authority Guidelines do not specify data retention timelines for specific systems such as SIEM, EDR, or any other security controls, in that case, alignment with the Organization internal policy should be assessed.		Data retention policy Dispositions method
10.6	CL3	Encryption shall be applied to safeguard backup data from unauthorized access.	Ensure data kept at rest must be encrypted and only approved/authorized users can access it.		Access control policy. Evidence of data encryption. IAM matrix
10.7	CL1	A backup policy shall be formulated and enforced to ensure compliance.	Ensure the compliance of the data backup policy is maintained or reviewed. Ensure that the audit is conducted against the backup policy.		Compliance review report of backup policy.

10.8	CL3	Full recovery of backups must be tested at least once annually and upon a fundamental infrastructure change	The auditor should inspect the end-to-end process of backups and their recovery. The auditor should also inspect if a full recovery test of backups is part of the backup policy of the organization. In case of any exception due to technical limitations and business constraints, a formal exception process should be devised and necessary compensating controls should be put in place.		Testing results of previous full recovery backup. Post testing actions Investigation of failures.

11. Cybersecurity Incident Management

Controls	Control Level	CTDISR Control Description	Interpretation	Compensating Control	Supporting Documents
11.1	CL3	A Computer Emergency Response Team (CERT) shall be established by the licensee to ensure a quick, effective and orderly response to Cybersecurity incidents	Ensure that the internal incident response team is available round the clock (24/7) to serve and respond to cybersecurity incidents. (refer to Annexure C)	Incident Response Retainers with strict SLA of the response team to be physically available on-site within 6 hours may be accepted as compensating control.	Incident Management Policy Incident Response Team organogram Review of IR Team Job description
11.2	CL2	CERT shall be capable of Planning, detection, initiation, response, Recovery, and Post-incident analysis having well-defined functions and communicated processes in place which shall be tested periodically	Ensure the CERT has well-defined rules which would assist at the end to end of the investigation. Also, ensure all the events are properly configured and tested periodically.		Incident response playbook Incident Management Policy
11.3	CL3	CERT shall have established and designated communication and reporting channels to enable internal and external users including subscribers and other sources to report Cybersecurity events as quickly as possible.	Ensure the CERT portal or reporting channel is communicated to all internal and external users.	.	Review of end-to-end incident response process
11.4	CL2	Reported and monitored Cybersecurity events shall be	Ensure the Incident management process is		Incident management policy

		assessed and accordingly classified as Cybersecurity incidents	available with the appropriate classification policy.		
11.5	CL1	All Cybersecurity incidents shall be formally recorded and a post-incident review report of all the incidents must be maintained	Ensure all the incident reports are formally informed to management Ensure that a process is in place to report security incidents to PTA.		Post-Breach Analysis reports. Actions taken evidence
11.6	CL2	Incidents shall be responded to achieve a normal security level and initiate necessary recovery to resume business continuity	The auditor should review the Incident response report of previously identified incidents and assess if the recovery time has been in conformance with the timelines provided in the incident management policy or Incident response SLAs in case of Incident response retainer.		Incident response SLA's Incident Management Policy
11.7	CL1	Procedures shall be defined and applied to identify, collect and preserve information related to a Cybersecurity incident that can serve as evidence	The auditor should assess if procedures are in place to ensure that the integrity of the evidence is not compromised during the incident response phase. The auditor should review if the Chain of Custody for handling evidence is being maintained.		Incident management policy Incident reporting process. Incident response playbook

11.8	CL1	Cybersecurity incidents shall be analyzed to reduce the likelihood of their future occurrence and resolve any identified security weaknesses	The auditor should inspect post-breach analysis reports (if any) and analyze if the recommendations have been implemented by the management.		Inspection of Post-Breach analysis reports. Preventive Actions taken
11.9	CL3	Licensee shall establish processes for collecting, analyzing, and responding to cyber threat intelligence information collected from internal and external sources. The licensee shall share threat feeds with PTA	Ensure the information received from Threat feeds, phishing emails, APT, etc. are being duly reported to PTA within 72 hours.		Evidence of reporting cyber threats via the PTA CERT portal or by email.
11.10.	CL1	To safeguard the Telecom Sector as a whole, licensee CERT shall be in contact with Telecom sector CERT established by PTA as well as other licensees CERTs to share security alerts/advisories/events/incidents information in a timely fashion	The auditor should assess, if incident report root causes analysis including and not limited to artifacts, IOC, etc. have been shared with PTA via CERT portal or email or via any other medium.		Evidence of reporting cyber threats via the PTA CERT portal or by email.

12. Service and Cybersecurity Continuity Management

Controls	Control Level	CTDISR Control Description	Interpretation	Compensating Control	Supporting Documents
12.1	CL1	The licensee shall ensure that during all situations, Service and Cybersecurity continuity shall be ensured to ensure the provision of licensed services and safeguard the integrity, availability, and confidentiality of CTI and critical data	Arrangements for redundancies must be ensured for Telecom CTD&I and cybersecurity systems.		Redundancy and backup of devices/systems/database/ applications are made. Data backup and data retention policy.
12.2	CL1	Formal processes and procedures shall be formulated, documented, and implemented by the licensee to ensure the required level of continuity for Services and Cybersecurity during adverse situations	The auditor should assess if, procedures for review and verification of such arrangements should be defined, enforced and Audited at regular intervals. For SMEs the runbooks, disaster recovery, and incident response plans – can be created to ensure the following: 1) Critical activities / data / applications / systems / hardware etc. are identified 2) The impacts of – these if not available - for a certain period – on the provision of services to the customers 3) The defined prioritized period for recovery - in case of disaster/disruption The steps to be followed for the recovery within that period.		Third-party SLA's BCM policy

12.3	CL2	Redundancies shall be arranged by the licensee for CTI and Cybersecurity systems and said arrangements shall be verified at regular intervals to ensure their efficacy	Ensure DR and BCP drills are performed for at least a year or as per the approved internal policy.		BCP drills / Testing results DR policy Post Drill Actions taken

CONTINUAL IMPROVEMENT

13. Cybersecurity Reviews

Controls	Control Level	CTDISR Control Description	Interpretation	Compensating Control	Supporting Documents
13.1	CL3	Licensee shall carry out quarterly periodic reviews of Cybersecurity measures for analysis and improvement of Cybersecurity measures.	The auditor should assess if quarterly reviews for analyzing and improving the overall cyber security posture are being conducted. The auditor should also assess, the action items that have been agreed upon as a result of the quarterly periodic reviews and the action item for their execution and see if management has any oversight/strategy to eradicate delays that might halt the progress of the agreed action items.		Ensure all Information security policies and processes are formally approved and reviewed. Evidence of quarterly reviews of Cyber Security measures conducted including Minutes of Meeting (MOM) and review of progress on action items.
13.2	CL2	At least once a year or upon a significant change/event, the licensee shall carry out an independent review from a third party after getting due approval from PTA, of its Cybersecurity measures and	Licensee should render services of PTA's approved Cyber Security Audit firms. List of which is in the Cyber Security section on PTA's official website.		Significant change approvals from PTA, Change request forms and approved process.

		implement required corrective actions.			
13.3	CL3	Technical compliance reviews for CTI such as vulnerability assessment and penetration testing shall be regularly carried out by the licensee at least once every six (6) months to identify and rectify vulnerabilities and security weaknesses.	This refers to internal VAPT exercises conducted by the internal security team. The auditor should assess if the vulnerabilities identified during internal VAPT have been duly rectified in accordance with the internal security policy. The auditor should also review vulnerabilities that have been accepted by the management and the rationale behind the acceptance.	External pen testing/audit reports with coverage of Critical Infrastructure may be accepted as a compensating control	Internal VAPT assessment reports Closure of Internal/external VAPT assessment reports Review of Risk Register and Risk acceptance Form
13.4	CL1	The licensee shall assist the Authority or its designated personnel in carrying out the audit of its Cybersecurity capabilities with the implementation of any identified shortcomings within the recommended timeframe.	The auditor should assess if a process is in place where-by the roles and responsibilities of individuals responsible for assisting authority or its designated personnel are documented and are reviewed at least once annually.		

MISCELLANEOUS

14. Breach of Conditions of Regulations

Controls	Control Level	CTDISR Control Description	Interpretation	Compensating Control	Supporting Documents
14.1	CL1	In case of non-compliance of any procedure specified in these regulations and as directed by the Authority from time to time, or upon receipt of information from any source of non-compliance of these regulations and directions of the Authority, the Authority or an authorized officer of the Authority not below the rank of Director, may initiate action against the offender.	The auditor should assess if CTDISR and regulatory obligations have been communicated to the management.		Evidence of CTDISR policy communicated to Board/Management.

15. Directions of the Authority

Controls	Control Level	CTDISR Control Description	Interpretation	Compensating Control	Supporting Documents
15.1	CL1	All directives, notifications, standard operating procedures and orders issued by the Authority from time to time on or before notification of these Regulations shall be binding and applicable on the Licensees.	The auditor will review all Policy Directives, Guidelines, SOP, etc. related to Cyber Security issued by PTA and will assess compliance against them.		Validate that operator has a PTA CERT portal account and compliance has been given against each advisory issued by PTA.

16. Consumer Education & Awareness

Controls	Control Level	CTDISR Control Description	Interpretation	Compensating Control	Supporting Documents
16.1	CL1	All licensees shall take necessary steps for the awareness of consumers to safeguard against cyber threats.	The auditor would ensure that security awareness, and capacity building program has been established within the organization. Auditor will also assess if information security awareness sessions are being conducted periodically at least once annually, or in line with the organization's policy. The organization's security awareness programs should		Approved Policy which covers Security awareness of the consumer. Delivery methodology Post awareness/ training session feedback Review of the feedback/ actions taken

			be tailored to the audience. Ideally, inputs from Security incidents should be made part of these programs.		

17. Inspection

Controls	Control Level	CTDISR Control Description	Interpretation	Compensating Control	Supporting Documents
17.1	CL1	To ensure compliance with these Regulations, the Authority through its authorized officer(s) may inspect the premises and records maintained by the Licensee(s) at any time	The auditor should assess if the same has been communicated to the senior management and has been made part of the Cyber Security Policy.		Evidence of CTDISR policy communicated to Board/Management.
17.2	CL1	The concerned Licensee(s) shall provide all the information and shall extend all possible assistance to the authorized officer(s) or representative of the Authority to inspect the records.	The auditor should assess if the same has been communicated to the senior management and has been made part of the Cyber Security Policy.		Evidence of CTDISR policy communicated to Board/Management.

18. Reporting Requirements

Controls	Control Level	CTDISR Control Description	Interpretation	Compensating Control	Supporting Documents
18.1	CL1	Reports mentioned in the regulations such as security policies, incident reports, BCP drills/ testing reports, security reviews, etc. shall be submitted to PTA upon conclusion of an activity /event or, as and when required by the Authority	Ensure all policies and procedures mentioned in the regulation are available and approved by management, and are readily available to be shared with PTA.		Approved security policies, incident reports, security reviews, etc. policies are available.
18.2	CL1	In case of a data breach or damage to CTI or critical data, the licensee shall duly inform the Authority within 72 hours of the discovery of the incident.	The auditor should inspect if reporting Data breaches or damage to CTI or Critical data to the authority is part of the organization's incident management/response policy. Also, how it is being reported / details provided and responsibilities etc.		Incident management process.
18.3	CL1	Access to reports and logs of security monitoring systems shall be provided to the Authority as per its defined guidelines.	The auditor should assess if the authority has provided directives or guidelines for access to the reports of security monitoring systems, in that case, Compliance against the directive/guidelines should be assessed.		

19. Confidentiality of-Information

Controls	Control Level	CTDISR Control Description	Interpretation	Compensating Control	Required Documents
19.1	CL1	Without prejudice to the provisions of any law for the time being in force, every Licensee shall ensure the confidentiality of all information disclosed by the subscribers under the provisions of these Regulations.	Auditors should inspect security controls implemented by the licensee to ensure confidentiality of all the information disclosed by the subscribers. The auditor can suggest additional security controls to protect the confidentiality, in case the current security controls do not seem to be sufficient. Auditor will also assess if the Need-to-know principle is being followed for accessing subscriber data/information.		Walkthrough of Security controls implemented by the Licensee.

Annexures

Annexure	Title	URL
Annexure A	Critical Telecom Data and Infrastructure Security Regulations, 2020	https://www.pta.gov.pk/assets/media/critical_telecom_data_reg_20112020.zip
Annexure B	Security Audit Firms Categorization	https://www.pta.gov.pk/en/security-audit-firms-categorization-220722
Annexure C	Security Audit Firms Criteria	https://www.pta.gov.pk/assets/media/cs_security_audit_reg_criteria_06-06-2022.pdf