ACCREDITATION CRITERIA FOR CLOUD SERVICE PROVIDERS

Ministry of Information Technology
& Telecommunication

DIGITAL PAKISTAN

Contents

1 Introduction:

Pakistan Cloud First Policy (PFCP) was approved by the Government of Pakistan in February 2022. (available at https://moitt.gov.pk/SiteImage/Misc/files/Pakistan%20Cloud%20First%20Policy-Final25-02-2022.pdf) which envisions digital transformation of Pakistan by optimized ICT spending and efficient utilization of latest cloud-based technologies. The policy mainly applies to all Public Sector Entities (PSE) intended to procure Cloud based services from Cloud Service Providers (CSPs)

A Cloud Office has been established under the Ministry of Information Technology and Telecommunication (MoIT&T) to facilitate and supervise the matters related to PCFP. Besides other implementation measures, Cloud Office has formulated Accreditation Criteria for Cloud Service Providers (CSPs) which will help to ensure that CSPs have the necessary security and compliance control to protect Government Data.

The Criteria is formulated for CSPs opting to provide services to PSEs. The criteria are based on international benchmarks such as security, reliability, cost, interoperability, availability, and any other established parameters

This document provides the general and certification requirements along with the list of artifacts required from CSPs. The accreditation procedure, audit process and suspension / termination clauses are also included in this document.

CSPs will be required to meet the requirements to get the accreditation from Cloud Office. PSE will be required to provision services from accredited list of CSP only. The Cloud Office will maintain an accredited list of CSP for PSE and will have the authority to revoke the accreditation of CSP in case of non-compliance.

2 Accreditation Criteria

2.1 General Requirements

1. CSP shall be any Public Sector or Private Sector Organization.
2. CSP shall abide by all relevant policies and legal requirements issued by Government of Pakistan as may be amended or revised from time to time.
3. CSP must fulfil contractual requirements as mentioned in Section 10.2 of PCFP that is Service Level Agreements (SLA), Interoperability Requirement, Migration between CSPs and Data Ownership.
4. CSP shall offer Cloud Services by choosing a model from the Cloud Deployment Models (Public Cloud, Government Cloud, Private Cloud, and Hybrid Cloud) [As specified in Section 7 of PCFP].
5. CSP shall adhere to the shared responsibility matrix referred in Annex C of PCFP or as agreed in SLA between CSP and PSE.
6. There should be sufficient capacity offered by CSP at an overall level in the compute, network and storage etc. to swiftly provision new resources in response to unanticipated additional / reduced requirement from PSE (as per the SLA between CSP and PSE)
7. The PSE shall be provided by CSPs with access rights (including the underlying secure connection) to the user administration / portal of cloud services (availed by PSE) to have visibility into the dashboard, SLAs, management reports, etc.

8. The PSE shall also be provided with the visibility of where its data is stored i.e.; geolocation of the data center as well as the accessibility matrix (who can view or process the data including the 3rd party partners of CSPs).
9. The PSE requiring Enhanced and Highest levels of security shall also be provided with the option to allocate personnel with CSP for stationing in data center that is hosting the data of the PSE.
10. CSP shall make the services available online, on-demand and dynamically scalable up or down as per request for service from PSE with multi-factor authentication via appropriately secure connection i.e. TLS.
11. CSP shall have ability to integrate and comply with the requirements laid down by existing legislation (Acts, Rules, Regulations and Polices) and relevant agencies of Pakistan.
12. CSP shall adhere to the relevant standards published (or to be published) by Cloud Office or any standards body setup / recognized by Federal Government and notified to the CSP by Cloud Office as a mandatory standard.
13. CSP shall be responsible for all costs associated with implementing, assessing, documenting and maintaining the accreditation process including audit cost wherever required.
14. The CSPs shall have provision to configure, schedule and manage backups of all the data including but not limited to files, folders, images, system state, databases and applications as per requirement of PSE or as per the policy defined by the cloud office.
15. The data center facilities and the physical and virtual assets should be secure, shall cater for the space, power, physical infrastructure requirement and must be located within Pakistan and ensure that all data functions and processing are performed within Pakistan except for data classified as Open / Public Data under Data Classification Guideline (Annex D of PCFP)
16. No data should be shared with any third party without explicit approval by the PSE, unless legally required by the relevant agencies / courts of Pakistan upon official request.
17. The CSP shall ensure that their incident response and handling policies are rigorously designed against industry best practices & standards to facilitate swift detection, immediate response, clear communication, and timely alerting in the event of any security or data breach.

2.2 Certifications

1. A CSP seeking to get accredited shall have the certifications listed under this section.
2. The certificates should have been issued in the name of the CSP for the relevant facility.
3. A CSP shall renew all applicable certifications 30 days prior to the date of expiry and submit a copy of the renewed certification of compliance (with applicable ISO Standards issued by a certification body accredited by Assurance Services International) to Cloud Office.
4. A CSP shall maintain a list of certified staff as required in relevant certification.
5. All certifications provided by the CSP for accreditation are subject to verification/confirmation by the auditors registered with Cloud Office. CSP will arrange for such verification to be done by the registered auditors.

2.2.1 Security

S No	Levels	International Standards / Guidelines
1	Baseline	• ISO/IEC 27001:2013 or 27001:2022

2	Intermediate	• ISO/IEC 27001:2013 or 27001:2022 • ISO/IEC 27017:2015
3	Enhanced	• ISO/IEC 27001:2013 or 27001:2022 • ISO/IEC 27017:2015 • ISO/IEC 27005:2022
4	Highest	• ISO/IEC 27001:2013 or 27001:2022 • ISO/IEC 27017:2015 • ISO/IEC 27005:2022 • ISO/IEC 27070:2021 • CSA STAR Certification • SOC2 (Managing Customer Data) • Relevant Sector Specific Standards

- *ISO/IEC 27001:2013 or 27001:2022 Information Security Managements*
- *ISO/IEC 27017:2015 Information technology — Security techniques — Code of practice for information security controls based on ISO/IEC 27002 for cloud services.*
- *ISO/IEC 27005:2022 — Information security, cybersecurity and privacy protection — Guidance on managing information security risks*
- *ISO/IEC 27070:2021 — Information technology — Security techniques — Requirements for establishing virtualized roots of trust*
- *CSA STAR Certification - (Global Cloud Security Alliance) - For Security, Trust, Assurance and Risk, CSA is standard for global cloud services providers*
- *SOC – 1, 2 & 3 Reports – AICPA – (Service Organization Control) - Frame work for managing and securing info. Reports used by svc orgs incl. cloud industry to demo security, availability, integrity, confidentiality & privacy*

Note: ISO/IEC 27001:2013 will be applicable till termination period (i.e. end of life by the Principal/ISO).

Security levels will allow PSEs to select CSP according to classification of their data [As specified in Section 16 of PCFP]

2.2.2 Privacy

1. For Baseline Level - ISO/IEC 27018:2019 Information technology — Security techniques — Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors.
2. For Intermediate, Enhanced and Highest levels - Sector specific HIPAA (Health Insurance Portability and Accountability Act) - Requirement for cloud services handling healthcare-related information to maintain confidentiality, integrity, and availability of electronic protected health information (ePHI), with stringent controls on data access and transfer.
3. For Intermediate, Enhanced and Highest levels - Sector specific PCI DSS (Payment Card Industry Data Security Standard) - Standard that requires cloud providers processing, storing, or transmitting credit card information to adhere to rigorous security measures, ensuring the protection of cardholder's data against breaches and fraud.

2.2.3 Service and Quality Management

1. ISO/IEC 20000-1:2018 Information technology — Service management — Part 1: Service management system requirements
2. ISO 9000 Family – Quality Management

Note: for Intermediate, Enhanced and Highest level only.

2.2.4 Data Centre

1. Tier II (for Baseline level)
2. Tier III Data Centre facility certified via TIA-942, Uptime Institute or equivalent (for Intermediate, Enhanced and Highest level).

2.3 Required Documentation

1. Copy of the certificate of incorporation, Memorandum of Association, Articles of Association and Company Profile issued by the Securities and Exchange Commission of Pakistan (SECP).
2. Certificate of Origin (including parent company).
3. 3rd Party Partners list which are necessary to provide the cloud services to PSE.
4. Certificate of Not-Blacklisted and Non-Bankruptcy.
5. Proof of financial strength/stability and guarantee to continue its business in Pakistan at least for next 10 years.
6. Copy of license and annual tax returns from the FBR or concerned revenue body. In case of registration to provide services for Open Data only and when the CSP is a foreign company or foreign body corporate not registered in Pakistan, a copy of the charter, statute, memorandum, articles or other instrument, constituting or defining the constitution of the foreign company or a foreign body corporate issued in its country of incorporation.
7. Certification of compliance with all the required standards of the Cloud Office issued by an auditing body designated by the Cloud Office.
8. List of relevant required human resources handling data or services of PSEs requiring Intermediate, Enhanced and Highest levels of Security. Screening of HR, as per ISO-27001, verified by the Auditors registered with the Cloud Office.
9. Any other document as required by the Cloud Office.

3 Accreditation Procedure

3.1 Accreditation Certificate

1. A CSP interested in getting accredited to provide services to PSEs in Pakistan will submit an application to the Cloud Office (via online application form or physical letter) with all the required documentation.
2. The Cloud Office will intimate the CSP about the start of review process.
3. The Cloud Office will review the submitted documentation.
4. The Cloud Office may ask the CSP to provide any clarification on the information submitted or to submit any missing documentation.
5. The Cloud Office will issue accreditation certificate to CSP that meet all the requirements.

6. This accreditation will be time bound and subject to terms and conditions.
7. The Cloud Office will publish a list of accredited CSP on its website.
8. Accreditation validity period will be 1 year.
9. Initially there will be accreditation fee exemption for the period of three years.

4 Audits of CSP

1. All the accredited CSP are subject to comply to ICT audits requirements mandated by PCFP.
2. Audits can either be carried out at regular intervals or on as the need be.
3. The Cloud Office will publish a list of designated auditing bodies on its website.
4. CSP to ensure that their audit is done by an auditor registered with the Cloud Office.
5. If required, the Cloud Office will designate any auditing body to carry out the audits based on the criteria outlined by the Cloud Office.
6. CSPs will be required to share the internal audit report as well as the 3rd party audit report with the Cloud Office within one month of the receipt of these reports from the audit department / firm.

5 Suspension and Termination of Accreditation of CSP

1. Cloud Acquisition Office (CAO) or PSE can submit complaints to the Cloud Office regarding accredited CSP.
2. Upon receiving a complaint from CAO or PSE or on its own motion, the Cloud Office may issue a show cause notice to the CSP identifying non-compliance with a contractual obligation or a term of its accreditation, asking for written explanation.
3. Cloud Office will carry out initial conflict resolution through direct negotiation, mediation and or arbitration.
4.
5. If Cloud Office finds the CSP in violation of any requirement, it may:
    a. Issue warnings and impose financial penalties
    b. Suspend some of the services being provided by the CSP
    c. Suspend all the services being provided by the CSP
    d. Terminate the accreditation of the CSP