Service Description
Privacy Impact Assessment (Lite)

Scope

The Privacy Impact Assessment Lite (PIA Lite) service provides a focused privacy risk review for projects, systems, or service changes that handle limited or low sensitivity personal information.

It is designed to quickly assess privacy implications, confirm compliance with the OAIC's Australian Privacy Principles (APPs), and ensure that privacy by design principles are applied without the need for a complete, detailed assessment.

This streamlined assessment is ideal for:

- Minor system or process enhancements, application integrations, or low impact data and or cloud migrations.
- Incremental changes to existing data handling processes or analytics functions.
- Use of third party or SaaS tools that process small volumes of personal data.
- Verification that existing privacy notices, consent mechanisms, and data sharing arrangements remain fit for purpose.

The PIA Lite provides a fast, risk-based privacy assurance model, maintaining compliance alignment with the OAIC and NIST Privacy Framework while minimising time, documentation, and cost.

This service is ideal for privacy officers, project managers, data stewards, or system owners launching low-risk system changes, integrations, or cloud and data analytics pilots.

Where higher risk or complex processing is identified, the engagement can be uplifted into the Privacy Impact Assessment (Complete), which includes full lifecycle data mapping, detailed control validation, and comprehensive reporting.

Approach

Delivered over five practical phases, the PIA Lite service balances risk tolerance with regulatory concern and organisational requirements. Further context relating to the engagement can be found below:

Initiation & Screening

- Confirm whether the change introduces privacy implications by reviewing data types, scope, and purpose.
- Classify sensitivity and identify applicable APPs or NIST Privacy Framework categories.

Rapid Data Mapping

- Document key data elements, sources, and storage points (excludes flow and movement)
- Validate alignment with existing privacy notices, consents, and governance policies.

Risk Identification

- Identify privacy risks across collection, use, storage, disclosure, and retention.
- Assess their likelihood and impact using organisational risk matrices.

Mitigation Recommendations

- Recommend proportionate safeguards - technical, procedural, or contractual, to reduce residual risk.
- Confirm that implemented security measures uphold confidentiality, integrity, and availability.

Summary Reporting

- Produce a concise Privacy Impact Summary outlining key risks, mitigations, and next steps.
- Provide a clear endorsement for Privacy Officer or Project Sponsor sign off.

Value

- Faster delivery enables privacy assurance for smaller or agile projects without delaying implementation.
- Compliance confidence demonstrates alignment with OAIC APPs, the NIST Privacy Framework, and internal governance expectations.
- Risk visibility identifies emerging privacy risks early, allowing proactive remediation.
- Scalable governance reinforces privacy by design across IT and business functions in a repeatable, lightweight format.
- Cost efficiency reduces administrative effort compared to the Privacy Impact Assessment (Complete) while maintaining assurance and accountability.

Benefits

These are the key advantages of undertaking this service offering:

- Maintains compliance confidence for low-risk projects through proportional governance.
- Reduces the need for extensive documentation while preserving visibility of key privacy impacts.
- Supports faster decision making and project approvals.
- Provides a pathway to uplift into the Privacy Impact Assessment (Complete) when material privacy or regulatory risks are detected.

Outputs

These outputs are delivered to support implementation and forward planning.

- PIA Lite Summary Report Concise overview of identified risks, mitigations, and sign off status.
- Risk and Recommendation Matrix Summary table of risks, ratings, and recommended actions.
- Executive Summary & sign off record for the Privacy Officer or Project Owner.