

Privacy Impact Assessment

Project context, privacy principles analysis, and the treatment actions needed before go-live.

PROJECT Kiwi Manufacturing ERP Migration	INDIVIDUALS 2500	GENERATED Assessment draft
--	----------------------------	--------------------------------------

OVERALL RISK Amber	IPP SCORE 62%	OPEN PRIVACY RISKS 3
------------------------------	-------------------------	--------------------------------

ASSESSMENT FOCUS

This Privacy Impact Assessment evaluates the privacy risks associated with Kiwi Manufacturing's planned ERP migration from MYOB to a cloud-hosted platform. The assessment identifies two high-severity risks related to cross-border data transfers and access control during migration. Overall IPP compliance sits at 62%, with IPP 11 (disclosure) and IPP 12 (overseas disclosure) requiring immediate attention.

Project description and purpose

Kiwi Manufacturing ERP Migration exists to centralise financial, hr, and production data in cloud.

Scope: All personal data processed across finance, HR, and operations

Project description: Migration from legacy MYOB to cloud-hosted ERP system

Scope and stakeholder context

Item	Detail
Project	Kiwi Manufacturing ERP Migration
Purpose	Centralise financial, HR, and production data in cloud
Scope	All personal data processed across finance, HR, and operations
Estimated people affected	2500

Data flow / lifecycle summary

The assessment reviews how personal information is collected, moved, stored, retained, and disclosed through the project lifecycle, including any cross-border flows and operational controls that matter for IPP 5, 11, and 12.

Personal information in scope

Category	Collection source	Storage	Retention	Sensitivity
Employee Records	Direct collection	Azure SQL (AU East)	7 years post-employment	high
Customer Contact Details	Direct collection	Microsoft 365 Dataverse	Duration of contract + 2 years	standard
Payroll & Banking	Direct collection	Xero Cloud (AU)	7 years per IRD requirements	high

Data sovereignty considerations

Te Mana Raraunga considerations: Kiwi Manufacturing processes data relating to Maori employees and iwi-affiliated contractors. Data sovereignty principles suggest that personal information with cultural significance should remain within Aotearoa where practicable.

IPP-by-IPP assessment

IPP	Status	Evidence	Gap / requirement
IPP 1	Compliant	Privacy notice on all collection forms	No material gap recorded
IPP 2	Compliant	Direct collection from data subjects	No material gap recorded
IPP 3	Partially Compliant	Privacy statement exists but not displayed at all...	Online forms missing privacy notice
IPP 5	Partially Compliant	Cloud storage with encryption at rest	No DLP controls on email
IPP 6	Compliant	SAR process documented and tested	No material gap recorded
IPP 11	Non Compliant	Third-party data sharing agreements incomplete	Xero data processed in Australia without adequate DPA
IPP 12	Non Compliant	Cross-border transfer assessment not completed	No assessment of AU data adequacy

Priority IPP commentary

IPP	Commentary
IPP 11	IPP 11 requires that agencies only disclose personal information in accordance with the purpose for which it was collected. Kiwi Manufacturing's data sharing with Xero for payroll processing is within purpose, but the DPA is incomplete.
IPP 12	IPP 12 governs cross-border disclosure. The transfer of employee payroll data to Xero's Australian infrastructure requires confirmation that comparable privacy protections exist under Australia's APPs framework.

Privacy risk register

Risk	Level	Score	Recommended control
Unauthorised access to employee payroll data during ERP migration	High	12	Control recommendation documented
Cross-border data transfer to AU without adequate safeguards	High	12	Control recommendation documented
Retention of legacy customer data beyond stated purpose	Medium	6	Control recommendation documented

Cross-border transfer register

Vendor	Country	DPA status	IPP 12
Xero Limited	Australia	partial	No
Microsoft Corporation	United States	executed	Yes

Recommended mitigations and treatment plan

Action	Priority	Target IPPs	Treatment outcome
Complete cross-border transfer assessment for Xero AU processing	High	11, 12	Reduce open privacy exposure before go-live
Implement DLP controls on email to prevent PI exfiltration	Medium	5	Reduce open privacy exposure before go-live

Residual risk and review checkpoints

After implementing recommended controls, residual risk for the ERP migration is expected to reduce from HIGH to MEDIUM. The primary residual risk relates to ongoing cross-border data flows to Australia, which cannot be fully eliminated while using Xero's AU-hosted payroll service.

Breach notification timeline meets 72-hour OPC requirement.

Sign-off / decision record

Reviewer	Role	Decision	Conditions
Sarah Chen	Privacy Officer	Approved with conditions	Complete cross-border assessment within 30 days