

PRODUCT WORKFLOW STUDY

From isolated machine records to permissioned access and shared service continuity

An asset-sharing workflow showing how Corexa can let owners, operators and service providers access the same machine history while controlling who can view or change it.

Evidence level stated clearly throughout

Repository-reviewed

Capability basis

Permissioned access

Control model

Persistent history

Asset value

Pilot required

Outcome standard



THE CHALLENGE

Why the existing process breaks down

A coffee machine can be owned by one party, operated at another site and serviced by several technicians over its life. Each participant may hold part of the history. When access is informal, the machine accumulates duplicate records or loses continuity whenever a person, provider or location changes.

01

Each party keeps a separate record

Owner, venue and technician may all describe the same machine differently and store different service evidence.

02

History depends on one provider

Changing service business can mean starting again without previous parts, faults or recommendations.

03

Access is too broad or too narrow

A user may receive full account access when they only need one machine, or no access to information required for service.

04

Machine movement breaks context

A machine moved to another site can be re-created instead of retaining its original lifecycle record.

05

Revocation is unclear

Former staff or providers may retain access because nobody can see or manage the sharing relationship.

06

Duplicate assets weaken reporting

Multiple records split jobs, health, parts and costs across what is physically one machine.

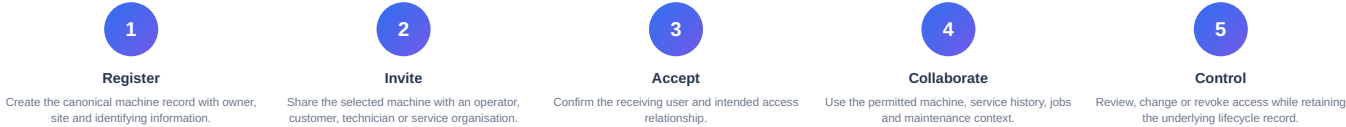
The central risk

The machine changes hands or service relationships, but its operational history cannot move safely with it.

THE OPERATING MODEL

A connected workflow around the machine

Corexa can preserve one persistent machine record while granting selected users a defined relationship to it. Sharing can be accepted, reviewed, adjusted or revoked without copying the asset and its history into another disconnected account.



COREXA CAPABILITY	OPERATIONAL CHANGE	WHY IT MATTERS
Shared-machine dashboard	Presents machines shared with the signed-in user separately from directly owned assets.	The receiving user can find the asset without duplicating it.
Invite and acceptance flow	Creates an explicit sharing relationship between users and the machine.	Access is traceable rather than communicated only through account credentials.
Machine-level scope	Limits the relationship to selected equipment and related information.	Users can collaborate without receiving unnecessary business-wide access.
Customer and site hierarchy	Keeps the shared machine connected to its operational location and customer context.	Service activity remains understandable even when ownership and operation differ.
Access adjustment	Allows the sharing party to review, change or revoke permissions.	Former participants do not need to retain indefinite access.
Persistent service history	Retains jobs, parts, maintenance and evidence against the original machine.	The asset history can survive changes in staff, site or service relationship.

CREDIBILITY STANDARD

What is supported - and what is not yet claimed

A credible case study distinguishes repository evidence, real workflow scope and future outcome hypotheses. The evidence level below is deliberately explicit.

✓ Repository capability

The dashboard code includes shared-machine retrieval and the product contains invitation, customer, site and machine account concepts.

✓ Asset-centred model

The design treats sharing as access to an existing machine record, not a second copy of the machine.

✓ Credible limitation

Permission design must be tested carefully. This study does not claim that every data field and role boundary has completed a formal security audit.

✓ Pilot requirement

A controlled pilot should test invitations, visibility, revocation and service continuity across at least two user roles.

Not yet claimed: this case study does not present a measured productivity, revenue, accuracy or customer-satisfaction improvement. A controlled baseline and participant-approved result are required before those claims are published.

Measurement plan for the publishable version

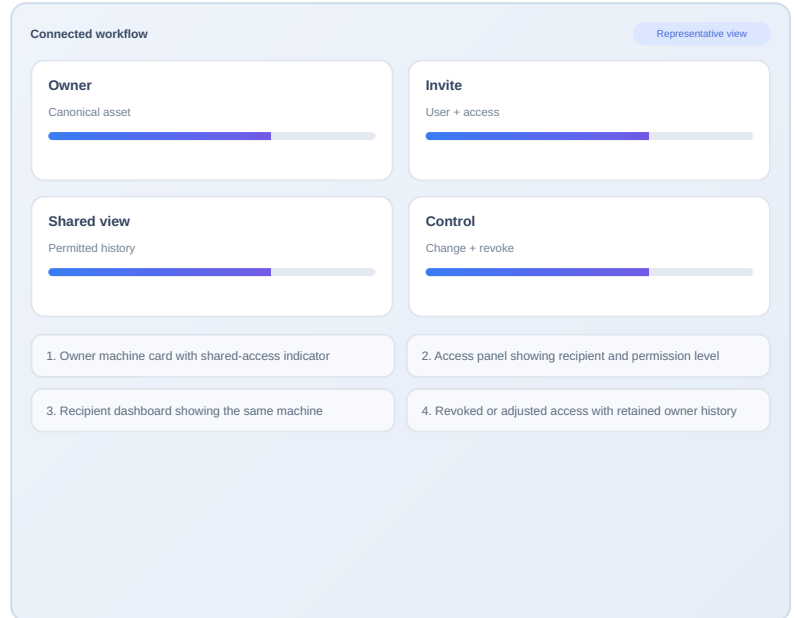
MEASURE	EVIDENCE SOURCE	CREDIBLE REPORTING
Invite acceptance	Sharing records	Accepted invitations as a percentage of valid invitations sent.
Access setup time	Invite and acceptance timestamps	Median time to give the intended user usable machine access.
Duplicate asset rate	Machine identity audit	Duplicate records found for machines participating in the pilot.
Revocation completion	Access logs	Time from revocation request to confirmed loss of access.
History continuity	Machine service audit	Percentage of visits recorded against the canonical machine through role or site changes.
Permission exceptions	Support and security review	Cases where a user saw too much, too little or stale information.

"The machine should keep one history while the people allowed to see and contribute to that history can change safely over time."

MAKE THE STORY TANGIBLE

Show one machine from the owner and shared-user perspectives

Use the same real asset in both accounts. Show the share control, accepted relationship, permitted history and revocation or access change so the audience can understand the boundary.



Recommended evidence-building sequence

Phase 1 - Permission map

Define exactly what each pilot role should see and change for one machine.

Phase 2 - Controlled sharing

Run invite, acceptance, service update and access change with test participants.

Phase 3 - Security evidence

Document visibility checks, exceptions, duplicate prevention and approved participant feedback.

Build the publishable proof layer

Replace representative views with dated interface screenshots, a defined baseline, system-derived measures and an approved participant quotation.

corexa.com.au
sales@corexa.com.au

Publication note: capability descriptions are based on the Corexa repository supplied in July 2026. Confirm the deployed workflow, permissions, integrations and data quality before presenting a capability as a completed customer outcome.