

Tool Rationalization Worksheet

Reusable LPM Knowledge Object · Platform Structure / AI Amplification

Use this worksheet to identify which tools should stay, be consolidated, governed harder, replaced, integrated, retired, or blocked from AI access. This is not a cost-cutting spreadsheet. It is an operating-model control artifact that exposes where tools create value, duplicate work, hide records, fragment ownership, weaken governance, or create risky AI access paths.

Metadata

Metadata

Value

Object type

LPM Knowledge Object

Primary LPM layers

Platform Structure, Information Ecology, Governance Architecture, AI Amplification

Connected layers

Ownership Map, Workflow Inventory, Integration Map, Source-of-Truth Map, Decision Rights Model, Evidence Checklist, Data Lineage Map

Primary use

Evaluate enterprise tools by purpose, ownership, adoption, cost, overlap, source-of-truth role, integration value, risk, lifecycle state, and AI usage boundary.

Website use

Downloadable template, workshop guide, AI readiness resource, JSON object for Lapemo ingestion, and future guided skill.

Version

1.0

Owner

LPM / Lapemo

Last reviewed

2026-06-24

Core principles

Principle

Meaning

Tool sprawl is operating-model debt

Every unmanaged tool adds hidden cost, fragmented records, duplicated workflows, inconsistent evidence, and unclear ownership.

Rationalization is not just cost reduction

A tool can be expensive and worth keeping, or cheap and operationally dangerous. Evaluate value, control, adoption, overlap, and AI exposure together.

Every tool needs a declared purpose

If teams cannot explain what a tool is for, what record it owns, and what workflow it supports, the tool is already a risk.

Source-of-truth status must be explicit

Some tools are official records, some are collaboration layers, some are reporting surfaces, and some are temporary workspaces. Confusing those creates enterprise noise.

AI changes the risk profile

Tools that were previously low-risk may become high-risk when AI can read, summarize, retrieve, update, trigger, or act through them.

Integrations increase dependency

An integrated tool is not isolated. It can move data, decisions, permissions, errors, and automation across the enterprise.

Retirement requires change management

Removing a tool without mapping workflows, evidence, integrations, owners, and user dependency creates operational disruption.

Required fields

Field

Definition

Required

Tool ID

Unique identifier for the tool, platform, application, SaaS product, internal system, plugin, bot, or AI workspace

Yes

Tool name

Common name used by business, technology, and users

Yes

Tool category

Work management, communication, document, data, BI, CRM, ERP, HR, finance, engineering, risk, AI, automation, knowledge, or shadow tool

Yes

Business purpose

What business capability, workflow, decision, information object, or control the tool supports

Yes

Primary owner

Accountable business or product owner for purpose, usage, value, and lifecycle

Yes

Technology owner

Accountable owner for architecture, security, operations, vendor, access, reliability, and integration

Yes

Data owner

Owner of critical data created, stored, transformed, or exposed by the tool

Required when data is material

Control owner

Owner of risk, compliance, security, privacy, model, audit, or policy controls attached to the tool

Required when control impact exists

User population

Teams, roles, functions, vendors, or agents using the tool

Yes

Adoption signal

Active users, frequency, workflow dependence, transaction volume, usage trend, or qualitative dependency

Yes

Cost model

License cost, consumption cost, support cost, vendor cost, implementation cost, and hidden labor cost

Yes

Value signal

Revenue, productivity, cycle time, quality, risk reduction, customer impact, decision speed, or employee experience value

Yes

Overlap / duplicate tools

Tools with similar purpose, workflow function, data object, channel, or user base

Yes

Source-of-truth role

Official record, system of entry, collaboration surface, reporting layer, temporary workspace, archive, or not a source of truth

Yes

System of record link

Where durable records, decisions, evidence, approvals, and outcomes live if not inside this tool

Yes

Workflow dependency

Workflows that start, move, approve, evidence, report, or close inside the tool

Yes

Integration dependency

Upstream and downstream systems, APIs, files, automations, webhooks, bots, agents, and data flows

Yes

Data sensitivity

Public, internal, confidential, regulated, customer, employee, financial, model, legal, or executive-sensitive

Yes

Access model

Who can access, approve access, change permissions, export data, connect integrations, and grant AI/tool access

Yes

AI usage boundary

Whether AI can retrieve, summarize, draft, recommend, update, trigger, execute, approve, or be blocked from this tool

Yes

Human review rule

When a person must validate AI output, approve tool actions, review evidence, or accept risk

Required when AI touches the tool

Risk / control profile

Security, privacy, compliance, audit, retention, operational, financial, model, vendor, or resiliency risk

Yes

Lifecycle state

Keep, govern harder, consolidate, replace, integrate, archive, retire, exception, or block

Yes

Rationalization decision

Decision made, decision owner, evidence used, tradeoffs, timing, and review date

Yes

Retirement / migration path

Plan for records, users, workflows, integrations, controls, evidence, communications, and cutover

Required for consolidate, replace, archive, or retire

Review cadence

Monthly, quarterly, semiannual, annual, event-driven, or continuous monitoring

Yes

Version

Object version, owner, last reviewed date, and change history

Yes

Tool categories

Category

Examples

What to evaluate

Common risk

Work management

Jira, Asana, Monday, ServiceNow, Azure DevOps

Workflow ownership, status record, decision capture, dependencies

Multiple backlogs and conflicting status

Communication

Teams, Slack, email, Zoom, Google Chat

Channel purpose, decision communication, retention, AI summaries

Decisions live only in chat or meetings

Document / knowledge

SharePoint, Confluence, Notion, Google Drive, Box

Source-of-truth role, freshness, permissions, ownership

Stale knowledge becomes AI retrieval source

Data / BI

Tableau, Power BI, Looker, data catalogs, warehouses

Metric ownership, lineage, freshness, access, dashboard duplication

Competing metrics and low-confidence evidence

CRM / customer

Salesforce, HubSpot, Zendesk, Gainsight

Customer record, workflow dependency, automation, access

AI acts on customer data without review

HR / people

Workday, Greenhouse, payroll, LMS

Employee data, access control, policy, workflow evidence

Sensitive data exposure and unclear ownership

Finance / ERP

SAP, Oracle, NetSuite, Coupa

Financial control, approval, audit, integration, reporting

Tool changes create control exceptions

Engineering / DevOps

GitHub, GitLab, CI/CD, monitoring, feature flags

Code ownership, deployment control, AI coding access, logs

AI-assisted change without decision rights

Governance / risk

GRC, audit, policy, access review, legal tools

Control evidence, issue ownership, risk acceptance, retention

Governance detached from real workflows

AI / automation

Copilot, ChatGPT Enterprise, agents, RPA, Zapier, n8n

Source access, action boundary, logs, review, model risk

AI reads or acts across tools without control

Shadow / local tools

Spreadsheets, personal databases, unapproved SaaS, rogue bots

Business dependency, data sensitivity, replacement path

Critical work hidden outside governed platforms

Rationalization stages

Stage

What happens

Evidence

Key fields

Common risk

1. Inventory

List active tools, shadow tools, AI tools, integrations, owner candidates, and major users.

Procurement data, SSO logs, expense reports, browser extensions, interviews, workflow scans

Tool ID, name, category, user population

Missing shadow tools and team-specific SaaS

2. Classify

Group tools by capability, workflow, data object, source-of-truth role, risk profile, and AI exposure.

Platform map, workflow inventory, source-of-truth map, data lineage

Tool category, purpose, source role, risk

Classifying by vendor instead of operating role

3. Evaluate

Score value, adoption, cost, overlap, control strength, integration dependency, and AI readiness.

Usage logs, cost data, user feedback, incident history, audit findings

Adoption, cost, value, overlap, AI boundary

Keeping tools because of politics or sunk cost

4. Decide

Choose keep, govern harder, consolidate, replace, integrate, archive, retire, exception, or block.

Decision log, evidence checklist, owner review, control review

Lifecycle state, decision owner, rationale

Decisions made without migration or control plan

5. Migrate

Move users, records, workflows, integrations, permissions, evidence, and AI access safely.

Migration plan, communication plan, cutover checklist, access review

Retirement path, system of record, controls

Tool is turned off before work is moved

6. Govern

Monitor ownership, usage, cost, controls, integrations, data, and AI access over time.

Dashboards, access logs, audit evidence, vendor reviews, AI logs

Review cadence, health signals, exceptions

Rationalization becomes a one-time cleanup

7. Reassess

Reopen decisions when company structure, AI use, regulation, cost, vendor risk, or workflow needs change.

Freshness review, renewal dates, incident reports, new AI use cases

Version, review date, change trigger

Old tool decisions survive new realities

Rationalization decision options

Decision

Meaning

When to use

Required control

Keep

Tool has clear purpose, owner, value, adoption, controls, and AI boundary

High-value, well-governed, low-overlap tools

Review cadence and owner confirmation

Govern harder

Tool is valuable but has weak ownership, evidence, access, controls, or AI exposure

Necessary but under-governed systems

Control plan, access review, AI boundary, evidence owner

Consolidate

Multiple tools serve similar purpose and should move to a smaller set

Duplicative channels, backlogs, dashboards, knowledge stores

Migration path and source-of-truth decision

Replace

Tool is valuable, but vendor, cost, capability, architecture, or risk is no longer acceptable

Weak platform fit, aging tech, failed adoption, high risk

Replacement plan, workflow migration, control continuity

Integrate

Tool should remain but must connect to official records, workflows, identity, or reporting

Valuable isolated tool that creates manual handoffs

Integration owner, lineage, monitoring, fallback

Archive

Tool no longer supports active work but contains records that must be retained

Historical records, legal hold, audit needs

Retention rule, access control, retrieval process

Retire

Tool should be decommissioned after users, records, workflows, and integrations move

Low value, duplicated, unsupported, or risky tools

Retirement checklist and communication plan

Exception

Tool violates standard but is temporarily approved because the business need is real

Regulatory, customer, vendor, M&A, regional, or time-bound need

Exception owner, expiry date, risk acceptance, review

Block

Tool should not be used or accessed by AI because risk, policy, ownership, or source trust is unacceptable

Rogue SaaS, unsafe AI plugins, unknown data exposure

Block rule, communication, monitoring, alternative path

Worksheet template

Field

Entry

Notes

Tool ID

[Unique ID]

Use consistent naming across platform, procurement, SSO, and architecture records

Tool name

[Tool name]

Include vendor and internal nickname if different

Tool category

[Category]

Work management, communication, data, AI, automation, etc.

Business purpose

[Purpose]

What capability, workflow, decision, or control this tool supports

Primary owner

[Name / role]

Owns value, purpose, adoption, and lifecycle

Technology owner

[Name / role]

Owns architecture, security, support, vendor, reliability

Data owner

[Name / role]

Required for material data

Control owner

[Name / role]

Required for regulated, sensitive, or control-impacting tools

User population

[Teams / roles / vendors / agents]

Include AI agents or automations if applicable

Adoption signal

[Usage data]

Active users, transactions, frequency, trend

Cost model

[License / support / hidden cost]

Include renewal date and contract owner when available

Value signal

[Value evidence]

Productivity, revenue, quality, risk, cycle time, decision speed

Overlap / duplicate tools

[Tool names]

Include same-purpose tools and same-record tools

Source-of-truth role

[Official record / collaboration / reporting / temporary / none]

Must align with Source-of-Truth Map

System of record link

[System / URL / owner]

Where durable records live

Workflow dependency

[Workflow names]

Use Workflow Inventory references

Integration dependency

[Upstream / downstream]

APIs, files, bots, webhooks, automations, agents

Data sensitivity

[Sensitivity level]

Internal, confidential, regulated, customer, employee, financial, legal

Access model

[Access rule]

Who grants, changes, exports, integrates, and audits access

AI usage boundary

[Retrieve / summarize / draft / recommend / update / execute / blocked]

Be explicit about allowed and blocked AI actions

Human review rule

[Review requirement]

Required before action, external communication, approval, or record change

Risk / control profile

[Risks and controls]

Security, privacy, compliance, audit, retention, vendor, resiliency

Lifecycle state

[Keep / govern harder / consolidate / replace / integrate / archive / retire / exception / block]

Current rationalization decision

Rationalization decision

[Decision and rationale]

Include decision owner and evidence used

Retirement / migration path

[Plan]

Required when consolidating, replacing, archiving, or retiring

Review cadence

[Cadence]

Monthly, quarterly, annual, event-driven, continuous

Version for 500+ employee company

Dimension

Recommended pattern

Design intent

Create visibility into tool sprawl before it becomes enterprise drag. Focus on tools used for coordination, knowledge, work management, customer operations, finance, HR, data, and AI.

Minimum scope

Inventory the top 50 to 100 tools, all AI tools, all tools with customer or employee data, and any tool used as a de facto system of record.

Operating pattern

Quarterly tool review led by business operations, technology, security, finance, and transformation owners.

AI focus

Block unmanaged AI access to sensitive tools. Allow AI retrieval and summarization only where source, owner, and review rules are clear.

Governance need

Name owners, confirm purpose, identify duplicate tools, define source-of-truth roles, and clean up obvious shadow systems.

Red flags

Tool bought by one team now runs critical work, AI browser plugins touching sensitive apps, spreadsheet databases, duplicate project tools, and no renewal owner.

Version for 5,000+ employee company

Dimension

Recommended pattern

Design intent

Move from tool inventory to capability-based platform governance across functions, business units, and shared services.

Minimum scope

Inventory enterprise platforms, departmental SaaS, AI tools, automation tools, critical spreadsheets, integrations, reporting tools, and systems touching regulated data.

Operating pattern

Quarterly platform rationalization council with domain owners, architecture, procurement, security, data, risk, finance, and AI governance.

AI focus

Classify every AI-accessible tool by permitted actions: retrieve, summarize, draft, recommend, update, execute, or blocked.

Governance need

Connect tool records to workflow inventory, source-of-truth map, integration map, data lineage, access model, and control ownership.

Red flags

Department-specific tools duplicate enterprise platforms, renewal decisions happen without usage evidence, AI tools bypass systems of record, and integrations are undocumented.

Version for 10,000+ employee company

Dimension

Recommended pattern

Design intent

Create enterprise tool control across business units, geographies, regulated functions, vendors, BPO partners, AI agents, and critical systems of record.

Minimum scope

Maintain a governed tool registry with Tier 1, Tier 2, high-risk, AI-connected, regulated, externally facing, and shadow-tool populations.

Operating pattern

Enterprise platform governance with domain councils, automated discovery, renewal controls, continuous access monitoring, AI tool-use logs, and exception governance.

AI focus

AI action through tools requires permission boundaries, source lineage, data classification, tool-use audit logs, human override, exception handling, and kill-switch rules.

Governance need

Link rationalization to architecture standards, data governance, model risk, privacy, security, procurement, finance, legal, compliance, records retention, and executive decision forums.

Red flags

Business units run local variants of enterprise systems, AI agents cross tool boundaries, vendors operate unmanaged tools, and tool retirement breaks controls or records retention.

Scoring logic

Dimension

Score

What good looks like

Purpose clarity

0-5

Tool has a clear business purpose, supported capability, user population, and workflow role.

Ownership clarity

0-5

Business, technology, data, control, vendor, and AI owners are named where relevant.

Adoption strength

0-5

Usage evidence shows real adoption, not only licenses purchased or executive sponsorship.

Value evidence

0-5

Tool value is tied to productivity, revenue, quality, risk, cycle time, customer impact, or decision speed.

Cost transparency

0-5

License, consumption, support, vendor, implementation, renewal, and hidden labor costs are visible.

Overlap control

0-5

Duplicate tools and overlapping functions are known, justified, consolidated, or retired.

Source-of-truth discipline

0-5

Tool role is clear: official record, entry layer, collaboration surface, reporting layer, archive, or temporary workspace.

Integration visibility

0-5

Upstream/downstream systems, APIs, files, automations, bots, and dependencies are mapped.

Governance strength

0-5

Access, controls, risk, retention, audit, vendor, and exception rules are defined.

AI boundary clarity

0-5

AI retrieval, summarization, recommendation, update, execution, review, and blocked actions are explicit.

Suggested readiness score: average the ten scores, then classify 0-1.9 as Fragmented, 2.0-3.4 as Rationalized, 3.5-4.4 as Governed, and 4.5-5.0 as AI-ready.

AI prompts

Given this tool inventory, classify each tool by category, business purpose, source-of-truth role, user population, owner, risk profile, integration dependency, and AI exposure.

Identify duplicate tools, overlapping capabilities, shadow systems, high-cost low-adoption tools, unmanaged AI tools, and tools without a named owner.

Score each tool from 0 to 5 across purpose clarity, ownership clarity, adoption strength, value evidence, cost transparency, overlap control, source-of-truth discipline, integration visibility, governance strength, and AI boundary clarity.

Recommend whether each tool should be kept, governed harder, consolidated, replaced, integrated, archived, retired, excepted, or blocked.

Generate a migration risk list for every tool marked consolidate, replace, archive, or retire, including workflow impact, data impact, integration impact, control impact, and communication need.

Create a Lapemo ingestion plan that converts this worksheet into tool objects, platform objects, ownership objects, workflow objects, information objects, integration objects, governance objects, and AI boundary rules.

Validation rules

Every tool must have a named business owner and technology owner.

Every tool with material data must have a named data owner and sensitivity classification.

Every tool used as an official record must be listed in the Source-of-Truth Map.

Every tool involved in recurring work must link to at least one Workflow Inventory object.

Every integrated tool must link to an Integration Map record and identify upstream and downstream dependencies.

Every tool with AI access must define allowed AI actions, blocked actions, human review rules, and audit logging requirements.

A tool cannot be marked Keep if ownership, purpose, cost, adoption, and risk are unknown.

A tool cannot be retired until records, workflows, integrations, access, evidence, and users have a migration or archive path.

A tool cannot be marked AI-ready if source-of-truth role, data sensitivity, access model, human review, and tool-use logging are unclear.

Status must never be encoded only by color. Use labels such as keep, govern harder, consolidate, replace, integrate, archive, retire, exception, or block.

Lapemo ingestion mapping

Lapemo object

Fields / entities

Use

Knowledge object

Tool Rationalization Worksheet

Canonical reusable artifact for platform simplification and AI-safe tool governance.

Tool object

Tool ID, name, category, purpose, lifecycle state, rationalization decision

Reusable artifact package: DOCX · PDF · Markdown · JSON skill schema

Creates governed tool records inside the control layer.

Ownership object

Primary owner, technology owner, data owner, control owner, vendor owner, AI owner

Connects tool lifecycle to accountable humans.

Platform object

System role, source-of-truth status, users, workflows, architecture, lifecycle

Links tools to platform structure and enterprise capability.

Workflow object

Workflow dependency, entry channel, system of record, decision points, outputs

Shows where tools participate in recurring work.

Information object

Data sensitivity, evidence, source role, freshness, lineage, records

Connects tool records to information ecology.

Integration object

Upstream systems, downstream systems, APIs, files, bots, automations, agents

Maps dependencies and failure paths.

Governance object

Access, controls, privacy, retention, risk, audit, vendor, exception, review cadence

Links tools to enterprise control requirements.

AI object

AI usage boundary, human review, permissions, tool-use logs, blocked actions, rollback

Defines what AI can safely do with or through each tool.

Reusable knowledge-object model

This artifact should exist in four synchronized forms: a human-readable guide, a downloadable worksheet, a machine-readable JSON object, and a guided Lapemo skill. The knowledge object should be versioned, reviewed, scored, and connected to system data over time. It should not auto-update silently. Lapemo should flag unowned tools, high-cost low-adoption tools, duplicate tools, shadow systems, weak source-of-truth roles, undocumented integrations, stale access, unresolved renewal decisions, and risky AI action boundaries for human approval.