

PLATFORM MAP

Reusable LPM Knowledge Object · Platform Structure / AI Amplification

Map systems -> ownership -> integrations -> truth -> controls -> AI access

Purpose

Use this template to map the enterprise platforms that shape work, decisions, information, governance, and AI. The goal is not a static application inventory. The goal is to make each platform visible as part of the operating model: what it owns, who depends on it, how it connects, what it controls, and what AI is allowed to do with it.

Metadata	Value
Object type	LPM Knowledge Object
Primary LPM layers	Platform Structure, Information Ecology, Governance Architecture, AI Amplification
Connected layers	Ownership Map, Decision Architecture, Communication Architecture, Source-of-Truth Map, Data Lineage Map
Primary use	Map the enterprise platforms, systems of record, integration paths, ownership, controls, data flows, and AI usage boundaries under one operating model.
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

1. Core principles

Principle	Meaning
Platforms are operating structures	Systems are not just tools. They shape ownership, decisions, information flow, governance, incentives, and AI behavior.
Every system needs a business owner	Technology can run the platform, but the business must own purpose, value, usage, data meaning, and adoption.
A platform without lineage is a liability	Each platform must connect to its source-of-truth objects, data lineage, evidence standards, and downstream consumers.
AI needs controlled system access	AI assistants, agents, copilots, and automations should only access systems through named permissions, review rules, and audit logs.
Shadow tools are operating-model signals	Unapproved spreadsheets, local databases, unsanctioned apps, and duplicate SaaS tools show unmet workflow, decision, or information needs.
Integration is governance	APIs, workflows, events, RPA, data pipelines, and AI actions must have owners, failure handling, controls, and observability.
Rationalization is not the first move	Do not start by killing tools. Start by mapping purpose, overlap, ownership, data criticality, and dependency risk.

2. Required fields

Field	Definition	Required
Platform ID	Unique identifier for the platform, system, application, data product, integration, or AI tool	Yes
Platform name	Common business and technical name of the platform	Yes
Platform category	Work, people, customer, finance, data/BI, governance/risk, knowledge, AI, integration, identity, or infrastructure	Yes
Business capability	The capability, process, decision, or operating need this platform supports	Yes
Primary users	Functions, roles, teams, agents, vendors, or customers who use the platform	Yes
Business owner	Accountable owner for purpose, value, adoption, operating rules, and approved use	Yes
Technical owner	Accountable owner for reliability, configuration, integrations, access, and support	Yes
Data owner / steward	Owner of the critical data objects, definitions, freshness, and quality rules in the platform	Required when data-critical
System of record status	Authoritative, consuming, reference, temporary, duplicate, shadow, retired, or disputed	Yes
Critical objects	Core records, entities, metrics, artifacts, documents, or workflows managed by the platform	Yes
Source-of-truth relationship	Whether the platform creates, masters, consumes, transforms, reports, indexes, or archives the object	Yes
Integration path	APIs, webhooks, ETL/ELT, events, file transfers, RPA, workflow automation, native connector, or manual handoff	Yes
Upstream dependencies	Systems, sources, teams, vendors, or data products required for the platform to work	Yes
Downstream consumers	Systems, reports, AI tools, workflows, controls, teams, or external parties that depend on this platform	Yes
Control requirements	Access, audit, retention, approvals, segregation, evidence, policy, compliance, or model risk requirements	Yes
AI usage boundary	Whether AI can retrieve, summarize, update, classify, recommend, create, approve, or act through the platform	Yes
Human review rule	When a human must approve a platform change, AI action, workflow step, or data update	Required when material
Adoption / value metric	Usage, cycle time, quality, cost, revenue, risk, experience, or automation metric used to assess value	Yes
Health signal	Reliability, support burden, duplicate usage, stale data, manual workaround, integration failure, or control exception	Yes
Lifecycle state	Explore, pilot, active, governed, constrained, consolidate, replace, retire, or exception	Yes
Known gaps	Missing owner, duplicate platform, weak integration, stale data, ungoverned AI access, or shadow usage	Yes
Review date	Next date to review ownership, usage, value, controls, integrations, and AI boundaries	Yes
Version	Object version, owner, last reviewed date, and change history	Yes

3. Platform categories

Category	Examples	Operating role	Primary owners	Common risk
Work systems	Jira, Asana, Monday, Azure DevOps, ServiceNow, Linear	Intake, planning, delivery, dependencies, blockers, outcomes	Product / PMO owner, work system owner	Hidden work, status theater, duplicate backlogs
People systems	Workday, SuccessFactors, ADP, Greenhouse, Lattice	Org structure, roles, skills, capacity, performance, incentives	People owner, HRIS owner, identity owner	Bad org data, unclear roles, AI workforce routing errors
Customer / revenue systems	Salesforce, HubSpot, Gainsight, Zendesk, Intercom	Customer records, pipeline, support, success, renewal, experience	Revenue owner, CX owner, CRM owner	Duplicate customer truth, weak handoffs, AI outreach risk
Finance / resource systems	ERP, FP&A, procurement, billing, planning tools	Budget, cost, vendor spend, resource allocation, benefits tracking	Finance owner, ERP owner, budget owner	Untracked AI cost, benefit leakage, vendor sprawl
Data and BI systems	Snowflake, Databricks, Power BI, Tableau, Looker, dbt	Metrics, analytics, data products, semantic models, dashboards	Data owner, analytics owner, BI owner	Competing dashboards, stale metrics, weak lineage
Knowledge systems	Confluence, SharePoint, Notion, Google Drive, wikis	Policies, SOPs, playbooks, templates, decisions, knowledge objects	Knowledge owner, content steward, platform owner	Stale content becomes AI memory

Category	Examples	Operating role	Primary owners	Common risk
Governance and risk systems	GRC, IAM, legal, privacy, audit, policy platforms	Controls, policies, exceptions, access, risk, compliance evidence	Risk owner, control owner, GRC owner	Controls disconnected from work and AI actions
Integration and automation systems	Mulesoft, Workato, Zapier, n8n, APIs, event streams, RPA	Data movement, workflow automation, handoffs, system actions	Integration owner, platform owner, automation owner	Brittle automations, no failure path, no audit trail
AI systems	Copilot, ChatGPT Enterprise, Claude, agent platforms, vector DBs, model registry	Retrieval, summarization, recommendation, generation, automation, agents	AI owner, model owner, data owner, governance owner	Agents act without authority, source, or review

4. Platform map stages

Stage	What happens	Evidence	Key fields	Common risk
1. Identify	Catalog the platform, category, users, owner, capability, and lifecycle state.	Platform register, app inventory, owner list	Platform ID, business owner, technical owner	No named owner or unknown usage
2. Classify	Determine whether the platform creates, masters, consumes, reports, indexes, or automates enterprise objects.	Source-of-truth map, data catalog, process map	System-of-record status, critical objects	Duplicate truth or disputed source
3. Connect	Map integrations, upstream dependencies, downstream consumers, workflows, and AI access paths.	Integration catalog, API list, data lineage map	Integration path, dependencies, consumers	Manual handoffs or invisible automation
4. Govern	Attach access, control, retention, evidence, review, and escalation rules.	GRC records, access model, audit logs	Control requirements, review rule, evidence link	Platform action without policy or control
5. Measure	Track adoption, value, reliability, risk, cost, and support burden.	Usage metrics, cost data, tickets, SLA, value score	Adoption metric, health signal, value metric	Shelfware, redundant spend, low-trust system
6. Optimize	Decide whether to standardize, consolidate, integrate, replace, constrain, or retire.	Rationalization plan, roadmap, exception list	Lifecycle state, known gaps, next action	Tool sprawl and unmanaged shadow systems
7. AI-enable safely	Define whether AI can retrieve, summarize, recommend, update, approve, or act through the platform.	AI policy, model registry, agent logs, permission model	AI boundary, human review, audit trail	AI reaches into systems without authority

5. Platform archetypes

Archetype	Definition	Examples	Governance requirement
System of record	Authoritative platform where a critical object is created or mastered	HRIS for employee record, CRM for account record	Must have business owner, data steward, access rule, lineage, and evidence standard
System of work	Platform where teams plan, execute, track, or coordinate work	Jira, ServiceNow, Azure DevOps, Asana	Must connect to decision logs, ownership, delivery metrics, and escalation path
System of intelligence	Platform that analyzes, reports, predicts, or recommends	BI tools, analytics layers, AI assistants, model platforms	Must reference approved sources, confidence, freshness, and review rules
System of control	Platform that enforces risk, access, policy, approvals, or compliance	IAM, GRC, policy, audit, legal, privacy platforms	Must connect to evidence, exceptions, ownership, and automated control checks
System of integration	Platform that moves data or executes workflow across systems	API gateway, iPaaS, event platform, RPA, workflow automation	Must have failure handling, ownership, observability, and audit trail
Knowledge system	Platform that stores reusable human and AI-readable knowledge	SharePoint, Confluence, Notion, knowledge bases, prompt libraries	Must have content ownership, freshness review, versioning, and AI retrieval boundary
Shadow system	Unapproved or unmanaged tool used because official systems do not meet the need	Spreadsheets, local databases, rogue SaaS, personal AI tools	Must be evaluated for unmet need, risk, value, and replacement path

6. Template: platform map

Map element	Entry	Guidance
Platform ID	[PLAT-001]	Unique platform or system object ID
Platform name	[Name]	Business and technical name
Platform category	[Work / People / Customer / Finance / Data / Knowledge / GRC / Integration / AI]	Used for routing and architecture review
Business capability	[Capability supported]	Why the platform exists

Map element	Entry	Guidance
Primary users	[Roles / teams / agents / vendors]	Who depends on it
Business owner	[Name / role]	Owns purpose, value, adoption, and business rules
Technical owner	[Name / role]	Owns configuration, reliability, access, support, and integrations
System-of-record status	[Authoritative / consuming / duplicate / shadow / disputed]	Defines truth status
Critical objects	[Records, metrics, workflows, documents, actions]	What the platform manages
Integration path	[API / webhook / ETL / event / RPA / manual]	How data or work moves
Upstream dependencies	[Systems / vendors / data sources]	What this platform relies on
Downstream consumers	[Systems / dashboards / AI tools / teams]	Who relies on this platform
Control requirements	[Access / approval / retention / audit / evidence]	Governance and compliance rules
AI usage boundary	[Retrieve / summarize / recommend / update / act / blocked]	Defines what AI can do
Adoption / value metric	[Usage, cost, cycle time, risk, quality, revenue]	How value is measured
Known gaps	[Owner gap, duplicate system, weak integration, shadow usage]	Exception list
Lifecycle state	[Pilot / active / governed / consolidate / replace / retire]	Current operating status
Review date	[Date]	Next review date

7. Version for 500+ employee company

Dimension	Recommended pattern
Design intent	Create basic platform visibility before systems, spreadsheets, AI tools, and ownerless workflows multiply.
Minimum scope	Map the top 20 to 40 platforms across work, people, customer, finance, data, knowledge, governance, integration, and AI.
Operating pattern	Monthly platform review led by technology, transformation, and business owners with a simple lifecycle status.
AI focus	Block AI access to unowned or disputed systems. Allow summary and retrieval only from named sources with human review.
Governance need	Name owners, define source-of-truth status, list integrations, and identify shadow tools before rationalizing.
Red flags	No platform owner, duplicate customer or employee truth, manual exports, AI pilots using local files, and unclear usage metrics.

- Start with platforms that run revenue, delivery, finance, people, knowledge, customer support, and active AI initiatives.
- Name business and technical owners before documenting every edge case.
- Treat shadow tools as signals of unmet process, reporting, or decision needs.

8. Version for 5,000+ employee company

Dimension	Recommended pattern
Design intent	Move from tool inventory to capability-owned platform architecture that supports cross-functional execution and governed AI.
Minimum scope	Map enterprise platforms, critical integrations, domain systems of record, BI layers, GRC systems, and AI platforms.
Operating pattern	Quarterly platform governance by domain with lifecycle decisions, adoption metrics, control status, and integration health.
AI focus	Define AI usage boundaries by platform: retrieve, summarize, recommend, update, create, approve, or act.
Governance need	Connect each platform to owners, data objects, access rules, evidence standards, lineage, and escalation paths.
Red flags	Business units buying duplicate SaaS, integration debt, BI sprawl, ungoverned copilots, and automation without audit trail.

- Organize platform ownership by business capability and domain, not just IT application inventory.
- Connect systems of record to source-of-truth maps, data lineage maps, and AI usage boundaries.
- Use platform health, duplication, integration risk, and adoption signals to drive rationalization.

9. Version for 10,000+ employee company

Dimension	Recommended pattern
Design intent	Create enterprise platform control across business units, shared services, data domains, AI agents, risk, and regulatory obligations.
Minimum scope	Map Tier 1 and Tier 2 platforms, systems of record, high-risk integrations, AI-critical data paths, control systems, and external data sharing.
Operating pattern	Enterprise platform council, domain architecture boards, automated dependency tracking, evidence packs, and lifecycle governance.
AI focus	AI agents require platform permission boundaries, tool-use logs, source lineage, model risk tiering, human review, and kill-switch rules.
Governance need	Connect platform changes to access, data, risk, policy, architecture, procurement, security, and audit review.
Red flags	Federated sprawl, business-unit-specific truth, unmanaged vendor platforms, silent API dependencies, and AI acting across systems without decision rights.

- Treat the platform map as an enterprise control layer across systems, integrations, data, risk, AI agents, and decision rights.
- Automate dependency discovery where possible, but keep ownership and decision rights human-approved.
- Connect platform change to architecture, security, procurement, GRC, data, model risk, and executive governance.

10. Scoring logic

Dimension	Score	What good looks like
Ownership clarity	0-5	Business, technical, data, control, and AI owners are named for critical platforms.
Purpose clarity	0-5	Each platform has a clear capability, user group, value metric, and lifecycle state.
Source-of-truth clarity	0-5	Critical objects have authoritative system status and known consumers.
Integration visibility	0-5	Upstream and downstream dependencies are mapped with owners and failure paths.
Governance strength	0-5	Access, retention, controls, evidence, policy, and escalation rules are defined.
AI boundary clarity	0-5	AI retrieval, recommendation, update, action, and review boundaries are explicit.
Health visibility	0-5	Usage, reliability, support burden, cost, adoption, and risk signals are monitored.
Lifecycle discipline	0-5	Platforms are actively governed as pilot, active, consolidate, replace, retire, or exception.

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

11. AI prompts

- Given this platform inventory, classify each system by category, lifecycle state, source-of-truth status, and AI usage boundary.
- Identify duplicate platforms, shadow tools, weak ownership, risky integrations, stale data paths, and ungoverned AI access.
- Score each platform from 0 to 5 across ownership clarity, purpose clarity, source-of-truth clarity, integration visibility, governance strength, AI boundary clarity, health visibility, and lifecycle discipline.
- Generate a platform dependency map showing upstream systems, downstream consumers, critical objects, integrations, AI consumers, and control evidence.
- Recommend whether each platform should be standardized, integrated, governed harder, consolidated, replaced, retired, or accepted as an exception.

- Create a Lapemo ingestion plan that converts this platform map into platform objects, ownership objects, integration objects, data objects, control objects, and AI boundary rules.

12. Validation rules

- Every critical platform must have a business owner and technical owner.
- Every system of record must identify the critical objects it masters and the downstream systems that consume them.
- Every integration must have an owner, purpose, failure path, observability signal, and review date.
- Every platform used by AI must have an approved AI usage boundary and human review rule.
- No AI tool should retrieve, update, approve, or act through a platform unless access, source, lineage, and decision rights are defined.
- Shadow systems must be flagged as unmet-need signals, not ignored or instantly removed.
- A platform cannot be classified as authoritative if ownership, freshness, access rules, and evidence links are missing.
- Status must never be encoded only by color; use labels such as authoritative, consuming, duplicate, shadow, disputed, active, governed, constrained, retire, or exception.

13. Lapemo ingestion mapping

Lapemo object	Fields / entities	Use
Knowledge object	Platform Map	Canonical reusable artifact for platform control and AI-safe system access.
Platform object	Platform ID, category, lifecycle, capability, source-of-truth status	Creates the enterprise platform inventory and control layer.
Ownership object	Business owner, technical owner, data owner, control owner, AI owner	Connects systems to accountable humans.
Integration object	Upstream dependencies, downstream consumers, API/event/file/RPA/workflow paths	Shows how systems connect and where risk travels.
Information object	Critical objects, source-of-truth relationship, lineage, freshness, evidence	Links platform structure to enterprise truth.
Governance object	Access, control, retention, policy, exception, review date	Links systems to operating controls and auditability.
AI object	AI usage boundary, permissions, review rule, logs, agent tool use	Defines what AI can safely do across platforms.

14. Reusable knowledge-object model

This artifact should exist in four synchronized forms: a human-readable guide, a downloadable template, 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 missing platform owners, duplicate systems, stale integrations, ungoverned AI access, shadow tools, and high-risk dependency changes for human approval.