LPM REUSABLE KNOWLEDGE OBJECT

Information Ownership Register

A reusable template for assigning ownership, stewardship, evidence, lifecycle, and AI usage rules to critical information assets.

Use this object to make information ownership visible before AI scales stale documents, weak metrics, unofficial knowledge, and unmanaged context across the enterprise.

Field	Value
Object type	LPM Knowledge Object
Primary LPM layers	Information Ecology, Ownership Map, Governance Architecture, AI Amplification
Connected layers	Decision Architecture, Communication Architecture, Platform Structure, Identity & Incentives
Primary use	Assign accountable ownership to critical information assets, knowledge objects, records, metrics, policies, evidence, and AI-accessible content.
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. Purpose

The Information Ownership Register assigns accountable ownership and stewardship to the information assets that shape decisions, work, governance, metrics, knowledge, and AI behavior. It prevents important information from becoming orphaned, stale, duplicated, overtrusted, or unsafe for AI retrieval.

In LPM terms, this object strengthens Information Ecology by connecting information to ownership, source-of-truth discipline, governance, communication, platform structure, decision rights, and AI amplification.

2. Core principles

Principle	What it means
Information without ownership decays	Every durable information asset needs a named accountable business owner and a steward responsible for hygiene, review, and change control.
Ownership is not authorship	The person who created a document, dashboard, or data product is not automatically accountable for its accuracy, usage, or lifecycle.
AI expands the blast radius	Unowned documents, stale pages, weak metrics, and duplicate records become more dangerous when AI can retrieve, summarize, or act on them.
Stewardship needs operating rules	Owners need review windows, evidence standards, access rules, quality thresholds, and escalation paths.
Truth must be maintained	Important information should have a source, owner, status, version, confidence rating, and supersession rule.
Ownership must map to use	The owner must understand who consumes the information, what decisions depend on it, and what risks emerge if it is wrong.
Retirement matters	Old artifacts, abandoned dashboards, stale policies, and obsolete AI context should be archived or marked as superseded.

3. Required fields

Use these fields to build an information ownership object that can be completed manually, rendered as a website artifact, imported into Lapemo, or used as a guided skill.

Field	Definition	Required
Information asset ID	Unique identifier for the document, record, data object, dashboard, metric, policy, evidence set, knowledge object, prompt, model context, or AI-readable asset	Yes
Information asset name	Plain-language name of the asset being governed	Yes
Asset type	Document, dashboard, metric, data product, policy, control evidence, decision record, knowledge object, process guide, prompt, dataset, model output, or system record	Yes
Business domain	Function, product, region, capability, operating layer, or enterprise system category the asset supports	Yes
Primary LPM layer	The LPM layer most affected by the asset	Yes
Purpose / business use	What the information exists to support, explain, decide, measure, control, or automate	Yes
System / repository	Where the asset currently lives: SharePoint, Confluence, Jira, ServiceNow, BI tool, CRM, HRIS, data catalog, GRC, Lapemo, etc.	Yes
Source of truth link	Authoritative location for the current approved version or record	Yes
Accountable business owner	Role accountable for accuracy, relevance, use, lifecycle, and dispute resolution	Yes
Information steward	Role responsible for metadata, freshness, formatting, quality checks, review hygiene, and update coordination	Yes
Technical owner	Role responsible for platform, permissions, integrations, automation, and reliability when system-backed	Required when system-backed
Data owner / content owner	Role that governs definitions, data quality, content standards, and downstream usage	Required when applicable
Primary consumers	Roles, teams, workflows, dashboards, AI agents, vendors, controls, or decisions that depend on the asset	Yes
Decision dependency	Decisions, approvals, risk events, customer commitments, or operating reviews that rely on this asset	Required when material
AI access rule	Whether AI can retrieve, summarize, classify, recommend, update, or act on this asset	Yes
Human review rule	When a person must validate the asset before use, publication, decisioning, or AI action	Yes
Freshness window	How current the information must be to remain usable	Yes
Review cadence	Monthly, quarterly, semiannual, annual, event-triggered, or retired	Yes
Confidence state	High, medium, low, provisional, stale, disputed, superseded, or retired	Yes
Sensitivity / classification	Public, internal, confidential, restricted, regulated, customer-sensitive, employee-sensitive, legal-sensitive, or security-sensitive	Yes
Access rule	Who can view, edit, approve, export, automate, train on, or supersede the asset	Yes
Evidence standard	Proof required to treat the asset as decision-grade, audit-grade, or AI-usable	Yes
Lineage / dependencies	Upstream sources, linked records, dashboards, integrations, approvals, transformations, and downstream consumers	Yes
Exception path	Where conflicts, stale information, missing owners, or unauthorized use should escalate	Yes
Supersession rule	How prior versions are replaced, retired, archived, or marked obsolete	Yes
Last reviewed date	Date of last human review	Yes
Next review date	Date or trigger for next review	Yes
Change history	What changed, who approved it, and why	Yes

4. Information asset types

Asset type	Examples	Typical owner roles	Failure risk
Strategic artifact	Strategy memo, roadmap, operating model, annual plan	Executive, transformation, product, finance	Outdated strategic context drives wrong prioritization
Decision record	Decision log entry, approval record, governance outcome	Decision owner, governance lead, portfolio leader	People reinterpret old decisions or ignore supersession
Metric / KPI	Dashboard, metric registry item, BI semantic definition	Business owner, data owner, BI steward	Competing definitions create false performance views
Policy / control	Policy, standard, control, exception, audit evidence	Control owner, risk owner, legal/compliance	Old controls get reused by AI or bypassed by teams
Knowledge object	LPM artifact, playbook, SOP, onboarding guide, framework asset	Artifact owner, steward, methodology owner	Stale guidance becomes institutional memory
Data product	Curated dataset, data contract, data mart, semantic layer	Data product owner, domain owner, platform owner	AI and dashboards rely on weak lineage
Process artifact	Process map, workflow guide, operating procedure	Process owner, function leader, system owner	Teams follow unofficial process variants
Customer / employee record	CRM record, HRIS profile, entitlement record, account file	Domain owner, data steward, system owner	Wrong routing, access, commitments, or personalization
AI context asset	Prompt, retrieval corpus, model card, evaluation set, agent memory	AI product owner, risk owner, content steward	AI produces confident output from unapproved context
Evidence pack	Source extract, audit proof, validation log, risk assessment	Evidence owner, control owner, reviewer	Decision or audit cannot be defended

5. Owner roles

Information ownership is role-based. One person may fill multiple roles in smaller companies, but the accountability boundaries should still be explicit.

Role	Owns	Accountable for
Accountable business owner	Owns business accuracy, relevance, lifecycle, and risk acceptance	Approves use, resolves disputes, sets review expectations, accepts consequences if wrong
Information steward	Maintains asset hygiene and review discipline	Tracks metadata, freshness, links, formatting, versioning, and owner follow-up
Technical owner	Owns platform reliability, integrations, access, and automation boundaries	Manages repository, permissions, APIs, retention, and technical controls
Data / content owner	Owns definitions, data quality, content quality, and approved usage	Validates quality, resolves definition conflicts, reviews downstream dependencies
Risk / control owner	Owns policy, compliance, audit, and exception requirements	Defines evidence standard, control needs, review checkpoints, and escalation triggers
AI usage owner	Owns how AI is allowed to read, summarize, recommend, or act on the asset	Defines retrieval rules, human review rules, prohibited uses, and evaluation expectations

6. 500+ employee company version

Category	Guidance
Design intent	Create visible ownership before knowledge becomes scattered across documents, chat, spreadsheets, and founder memory.
Minimum register	Track critical documents, dashboards, decision records, policies, process guides, customer records, and AI initiative artifacts.
Biggest risk	Useful information exists, but no one owns keeping it current, trusted, or safe for AI retrieval.
Ownership pattern	One business owner and one steward per critical asset. Technical owner added when the asset lives in a managed system.
Review cadence	Quarterly for core assets, monthly for AI-accessible or customer-impacting assets, event-triggered for major org or system changes.
AI focus	Do not let AI retrieve from unowned repositories, stale playbooks, or duplicate documents without review and confidence labels.
Operating rule	If an asset influences decisions, customers, employees, controls, or AI, it must be in the register.

7. 5,000+ employee company version

Category	Guidance
Design intent	Create cross-functional stewardship across functions, shared platforms, data domains, governance forums, and AI programs.
Minimum register	Track enterprise knowledge objects, metric definitions, policies, controls, data products, process artifacts, decision records, and AI context assets.
Biggest risk	Each function manages its own information standards, producing conflicting truths and inconsistent AI outputs.
Ownership pattern	Business owner, steward, data/content owner, technical owner, and risk/control owner assigned by domain and asset class.
Review cadence	Quarterly domain reviews, monthly AI/risk asset reviews, and automated stale-asset alerts through platform metadata.
AI focus	AI retrieval and agent workflows must use registered assets with owner, freshness, confidence, sensitivity, and allowed-use metadata.
Operating rule	High-use assets and AI-accessible assets require owner validation, source-of-truth mapping, and evidence standards.

8. 10,000+ employee company version

Category	Guidance
Design intent	Operate information ownership as an enterprise control layer across regions, business units, platforms, vendors, and AI agents.
Minimum register	Maintain enterprise asset classes for data, knowledge, policy, control, metric, decision, model, agent, vendor, and regulated information.
Biggest risk	AI scales stale or conflicting institutional knowledge across thousands of employees, systems, and automated workflows.
Ownership pattern	Federated domain ownership with enterprise metadata standards, stewardship councils, data governance, model governance, and audit traceability.
Review cadence	Risk-tiered review: monthly for regulated/AI/customer/employee-impacting assets, quarterly for operational assets, annual for stable reference assets.
AI focus	AI systems must check ownership, classification, confidence, lineage, and review status before retrieving, summarizing, recommending, or acting.
Operating rule	Unowned, stale, disputed, or superseded assets are blocked from decision-grade use and flagged for governance action.

9. Confidence states

State	Definition	Use rule
High	Owner confirmed, source mapped, review current, lineage visible, evidence standard met	Can support decisions and approved AI retrieval within defined boundaries
Medium	Owner known, source usable, minor gaps in lineage, evidence, or freshness	Can support operational use with caution and owner review for high-impact decisions
Low	Owner unclear, stale metadata, weak evidence, or unresolved definition issues	Cannot support critical decisions or AI action without review
Provisional	New asset not fully governed yet	Time-boxed use only; owner and review rules required
Stale	Freshness window missed	Flag for review; do not use for AI outputs or executive decisions until refreshed
Disputed	Conflicting owners, sources, definitions, or interpretations	Escalate through information governance or decision rights path
Superseded	Replaced by a newer source, artifact, metric, or policy	Archive or redirect users and AI to the current source
Retired	No longer active or approved for use	Remove from active workflows and AI retrieval scope

10. Workshop flow

Step	Instruction
1. Inventory	List critical information assets by domain, system, workflow, decision, metric, policy, and AI use case.
2. Classify	Assign asset type, sensitivity, business domain, LPM layer, and primary consumers.
3. Assign ownership	Name the accountable business owner, steward, technical owner, data/content owner, and risk/control owner where applicable.
4. Map source and lineage	Identify authoritative location, upstream dependencies, downstream consumers, and related decision/evidence objects.
5. Define AI rules	Specify whether AI can retrieve, summarize, recommend, update, train on, or act on the asset.
6. Set review rules	Define freshness window, review cadence, human validation trigger, and supersession rule.
7. Score confidence	Rate ownership clarity, freshness, evidence, lineage, sensitivity, AI readiness, and lifecycle control.
8. Resolve gaps	Create actions for missing owners, stale records, duplicate assets, unauthorized channels, or AI exposure issues.
9. Publish register	Store the approved register in a durable system and link it to the source-of-truth map, decision log, and evidence checklist.
10. Operate as living object	Review when systems, owners, policies, workflows, metrics, or AI use cases change.

11. Validation rules

Condition	Rule
No owner assigned	Asset is not decision-grade, audit-grade, or AI-usable until an accountable business owner is assigned.
No steward assigned	Asset may exist, but hygiene and review accountability are incomplete.
No source-of-truth link	Asset cannot be treated as authoritative.
Stale review date	Asset must be flagged and removed from AI retrieval for critical use until refreshed.
AI access enabled without rule	Block AI use until retrieval, summarization, update, and human review boundaries are defined.
Sensitive asset without access rule	Escalate to technical owner, risk owner, or data governance.
Decision dependency without evidence standard	Require evidence checklist completion before the asset supports critical decisions.
Duplicate asset found	Assign one source of truth and mark duplicates as copies, references, or superseded assets.
Disputed owner or definition	Escalate through decision rights model and information governance path.
Retired or superseded asset still in use	Redirect users and AI to current source and log the supersession.

12. Scoring model

Dimension	Score	Question
Ownership clarity	0-5	Is there a named accountable business owner and steward?
Source clarity	0-5	Is the authoritative source location known and linked?
Freshness control	0-5	Does the asset have a review date, freshness window, and stale-state handling?
Evidence strength	0-5	Can the asset support decisions with traceable evidence?
Lineage visibility	0-5	Are upstream sources and downstream consumers known?
Access governance	0-5	Are sensitivity, permissions, export, and edit rules defined?
AI use readiness	0-5	Are AI retrieval, summarization, and action boundaries defined?

Dimension	Score	Question
Lifecycle discipline	0-5	Is there a supersession, archive, retirement, and change-history rule?

13. AI prompts

Prompt	Instruction
Classify information asset	Classify this asset by type, LPM layer, sensitivity, business domain, primary consumers, and likely owner roles.
Detect missing ownership	Review this register and identify assets missing accountable owners, stewards, technical owners, or risk owners.
Score AI readiness	Score each asset for AI retrieval readiness using ownership, source clarity, freshness, sensitivity, evidence, and human review rules.
Find duplicate truths	Identify assets that appear to govern the same object, metric, policy, decision, or process and recommend one source-of-truth path.
Generate review actions	Create prioritized actions for stale, disputed, unowned, sensitive, or AI-exposed assets.
Create source-of-truth mapping	Map each information asset to its authoritative source, system role, owner, evidence standard, and AI usage rule.
Draft owner outreach	Draft a short message asking an accountable owner to confirm accuracy, allowed use, freshness, and AI access rules for this asset.

14. Example information ownership register

ID	Asset	Type	Domain	Owner	Steward	Source	AI rule	Confidence
IOR-001	AI sales enablement playbook	Knowledge object	Sales	VP Sales Ops	RevOps steward	Confluence	Summarize only; no autonomous send	Medium
IOR-002	Customer health metric	Metric	Customer Success	Chief Customer Officer	BI steward	Metric registry	Allowed for insight; human validates action	High
IOR-003	Employee access policy	Policy/control	IT / HR	CISO	Policy steward	GRC	Retrieve only; no policy interpretation without reviewer	High
IOR-004	Product roadmap	Strategic artifact	Product	CPO	Portfolio steward	Portfolio tool	Summaries require owner-approved version	Medium
IOR-005	Legacy process spreadsheet	Process artifact	Operations	Unknown	None	SharePoint	Blocked until owner assigned	Low
IOR-006	AI agent prompt library	AI context asset	AI Platform	Head of AI Product	AI steward	Model registry	Use only in approved agent workflows	Provisional

15. How this becomes reusable

- Website artifact: publish the Markdown as the educational page and offer the DOCX and PDF as downloads.
- Workshop asset: use the DOCX to inventory information assets, assign ownership, and surface stale or unowned information.
- Lapemo ingestion object: convert completed rows into structured information objects tied to owners, sources, decisions, evidence, systems, and AI workflows.
- AI skill: use the JSON schema and prompts to classify assets, detect missing owners, score AI readiness, and recommend governance actions.
- Living object: review and update when systems, owners, processes, policies, metrics, AI workflows, or business domains change.