

Control Map

Reusable LPM Knowledge Object for governance controls, evidence, ownership, and AI-safe operating boundaries

Use this Control Map to make enterprise controls visible, owned, testable, and connected to the operating model. The map defines what is being controlled, why the control exists, who owns it, which systems and data it depends on, what evidence proves it is working, how AI is allowed to interact with it, and what happens when the control fails. It is designed for companies scaling AI where static policy, scattered approvals, and undocumented controls cannot protect a hybrid human and machine workforce.

Built for three company profiles: 500+ employees, 5,000+ employees, and 10,000+ employees. Use it as a website artifact, workshop guide, governance control design tool, and future Lapemo guided skill.

Metadata

Metadata	Value
Object type	LPM Knowledge Object
Primary LPM layer	Governance Architecture
Connected layers	Ownership Map, Decision Architecture, Information Ecology, Platform Structure, AI Amplification
Primary use	Map enterprise controls to accountable owners, risks, evidence, systems, workflows, AI boundaries, and review rules.
Website use	Downloadable template, governance 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
Controls must be owned	Every meaningful control needs one accountable control owner and clear supporting owners across process, system, data, evidence, and AI usage.
Controls must connect to work	A control that is not connected to a workflow, decision, system, data object, or AI action boundary is only paperwork.
Evidence beats assurance language	The map must identify the exact evidence source, freshness requirement, test method, and review cadence.
AI changes the control surface	AI that retrieves, recommends, drafts, updates, triggers, executes, approves, or communicates must be tied to specific control boundaries.
Controls must have failure paths	Every control needs a defined failure condition, escalation route, remediation owner, and review or supersession rule.
Control burden must be rationalized	Controls should be right-sized. Low-risk work should not carry heavy enterprise control load, and high-risk work should not rely on informal review.
Governance must become monitorable	The control map should convert governance into measurable signals: owner coverage, evidence freshness, test outcomes, exceptions, overdue reviews, and AI boundary violations.

Required fields

Field	Definition	Required
Control ID	Unique identifier for the control, test, policy requirement, approval rule, monitoring rule, or AI boundary	Yes
Control name	Plain-language name that business, technology, governance, and audit stakeholders can understand	Yes
Control purpose	The risk, obligation, failure mode, decision quality issue, or operating-model behavior the control is designed to manage	Yes
Control category	Preventive, detective, corrective, approval, access, data quality, financial, operational, vendor, AI, model, security, privacy, compliance, or records	Yes
Risk or obligation	The policy, regulation, enterprise standard, customer risk, employee risk, operational risk, financial risk, or AI risk addressed by the control	Yes
Accountable control owner	Person or role accountable for control design, effectiveness, review, exceptions, and remediation	Yes
Process owner	Owner of the workflow, operating process, or business capability where the control is applied	Yes
System owner	Owner of the platform, application, integration, report, agent, or automation where the control is executed or evidenced	Required when systems are involved
Data owner	Owner of the data object, metric, source, knowledge object, model input, or evidence source used by the control	Required when data is involved
Evidence owner	Person or role responsible for producing, validating, storing, and refreshing control evidence	Yes
Evidence source	System of record, report, dashboard, log, ticket, approval record, decision log, lineage object, policy, test result, or audit artifact	Yes
Frequency	Real-time, event-based, daily, weekly, monthly, quarterly, annual, release-based, exception-based, or manual review	Yes
Test method	Automated check, sample review, attestation, exception report, reconciliation, approval review, log review, model validation, or control self-assessment	Yes
AI involvement	Whether AI retrieves, summarizes, drafts, recommends, updates, triggers, executes, approves, communicates, monitors, or creates evidence	Yes
AI allowed actions	Specific AI actions permitted under the control boundary	Required when AI is involved
AI blocked actions	Specific AI actions prohibited without human approval, control owner approval, or enterprise governance review	Required when AI is involved
Human review rule	Human validation, approval, override, audit, or signoff required before control-affecting action	Required when risk or AI is involved
Failure condition	What proves the control failed, became stale, was bypassed, produced weak evidence, or no longer matches operating reality	Yes
Escalation path	Route for failed control, overdue review, exception, boundary violation, unclear ownership, or material risk exposure	Yes
Remediation owner	Person or role accountable for fixing the control, process, system, evidence, data, AI boundary, or operating-model gap	Yes
Review date	Date when the control must be reviewed, retested, renewed, retired, or superseded	Yes

Control categories

Category	Purpose	Examples
Preventive control	Stops an unwanted action before it occurs	Access approval, budget threshold, release gate, AI blocked action, policy precheck
Detective control	Finds an issue after or during activity	Exception report, audit log review, quality monitor, model drift alert, data freshness check
Corrective control	Restores the operating model after failure	Rollback, remediation plan, incident response, process fix, access removal, model rollback
Approval control	Requires an authorized person or forum to approve a decision or action	Decision rights check, governance approval, risk acceptance, vendor approval
Access control	Limits who or what can see, change, trigger, or approve something	Role-based access, privileged access, agent permissions, API scope
Data quality control	Protects accuracy, completeness, timeliness, lineage, and source integrity	Reconciliation, validation rule, lineage check, source freshness threshold
AI / model control	Controls how AI can use data, create outputs, trigger work, or influence decisions	Human review, prompt boundary, retrieval scope, output validation, kill switch
Records / evidence control	Ensures the durable record exists, is reviewable, and can support audit or decision replay	Decision log, approval record, evidence package, retention rule
Vendor / integration control	Controls third-party systems, integrations, APIs, data movement, and outsourced work	Vendor review, integration owner, monitoring, SLA, data processing rule

Control map template

Map area	Question	Mapping guidance
Control object	What is being controlled?	Name the risk, behavior, workflow, decision, data object, system action, or AI action boundary.
Owner model	Who owns design, execution, evidence, and remediation?	Separate control owner, process owner, system owner, data owner, evidence owner, and remediation owner.
Evidence model	What proves the control is working?	Identify the evidence source, freshness window, test method, confidence level, and storage location.
System and data dependency	Where does the control live or depend?	Map systems, integrations, data objects, dashboards, logs, reports, agents, and workflow tools.
AI boundary	What can AI do and not do?	Document allowed actions, blocked actions, retrieval scope, human review, logging, and kill switch.
Failure and escalation	What happens when it fails?	Define failure signals, escalation route, remediation owner, SLA, review date, and supersession rule.

Workflow

Step	Action
1. Identify control population	List controls from policies, audit findings, governance forums, system permissions, workflows, dashboards, AI use cases, vendor obligations, and key decisions.
2. Classify control type	Classify each control as preventive, detective, corrective, approval, access, data quality, AI/model, vendor, records, financial, operational, security, privacy, or compliance.
3. Assign ownership	Assign accountable control owner plus process, system, data, evidence, remediation, and AI boundary owners where relevant.
4. Map evidence	Define the evidence source, system of record, freshness window, confidence rating, test method, and storage location.
5. Map dependencies	Connect each control to workflows, decisions, platforms, integrations, data lineage, source-of-truth objects, and AI initiatives.
6. Define AI boundary	Document AI allowed actions, blocked actions, human review rules, logs, override path, and kill switch.
7. Set failure path	Define failure condition, escalation route, remediation owner, target resolution time, and review or supersession trigger.
8. Score and improve	Score control health, fix weak ownership and evidence, retire duplicate controls, and create Lapemo control objects for ongoing monitoring.

Version for 500+ employee company

Dimension	Recommended pattern
Design intent	Create practical control visibility without building a heavy committee model. Focus on material risks, AI initiatives, core systems, customer/employee impact, and key evidence sources.
Minimum scope	Map top 25 to 75 controls across finance, people, customer, product, security, data, platform, AI pilots, and executive decisions.
Operating pattern	Monthly control review with named owners, simple evidence links, clear exception path, and light AI boundary classification.
AI focus	Every AI pilot or automation must identify accountable owner, source data, human review rule, blocked actions, and control evidence.
Governance need	Prevent founder-led or function-led exceptions from becoming hidden operating risk as systems and AI usage scale.
Red flags	Controls live in policy documents only, evidence is manual screenshots, AI pilots have no control owner, and exceptions are handled through informal leadership channels.

Version for 5,000+ employee company

Dimension	Recommended pattern
Design intent	Standardize control ownership and evidence across domains, platforms, data products, workflows, vendors, and AI-enabled work.
Minimum scope	Map material controls by business domain, platform, data source, integration, AI initiative, governance forum, and risk/control obligation.
Operating pattern	Quarterly control owner review, automated evidence where possible, exception management, issue remediation, and governance route alignment.
AI focus	AI controls must include retrieval boundaries, approval boundaries, output review, tool/action permissions, audit logs, and escalation path.
Governance need	Connect control maps to decision logs, evidence checklists, platform maps, integration maps, workflow inventory, and source-of-truth map.
Red flags	Control ownership is split across functions, dashboards conflict with audit evidence, AI agents use uncontrolled data, and duplicate tools create duplicate controls.

Version for 10,000+ employee company

Dimension	Recommended pattern
Design intent	Create enterprise-grade control lineage across business units, regions, regulated functions, shared services, vendors, BPO partners, AI agents, and critical systems.
Minimum scope	Map enterprise control inventory, control objectives, risk domains, evidence sources, issue workflows, model/AI controls, data lineage, integration controls, and policy obligations.
Operating pattern	Automated control monitoring with control owner dashboards, evidence freshness signals, exception routing, remediation SLAs, AI boundary monitoring, and audit-ready lineage.
AI focus	AI tools and agents must have permission scopes, evidence requirements, source lineage, human override, action logs, review cadence, incident path, and kill-switch ownership.
Governance need	Integrate with risk, compliance, internal audit, legal, privacy, security, architecture, data governance, model risk, finance, procurement, and executive governance.
Red flags	Multiple control taxonomies conflict, local AI tools bypass enterprise controls, evidence cannot be traced to source, and exceptions never expire or trigger remediation.

Scoring logic

Dimension	Score	What good looks like
Ownership clarity	0-5	Control owner, process owner, system owner, data owner, evidence owner, AI boundary owner, and remediation owner are clear where relevant.
Control purpose clarity	0-5	The risk, obligation, behavior, decision, workflow, or AI boundary being controlled is explicit.
Evidence strength	0-5	Evidence is current, sourced, owned, durable, testable, and stored in a known system of record.
System and data lineage	0-5	The control is connected to platforms, integrations, data objects, reports, logs, workflows, and source-of-truth objects.
Testability	0-5	The control has a defined test method, frequency, sample or automation rule, and pass/fail criteria.
AI boundary clarity	0-5	AI allowed actions, blocked actions, review rules, logs, retrieval limits, and kill switch are documented.
Exception handling	0-5	Exceptions have owner, rationale, expiration date, evidence, escalation route, and remediation path.
Failure response	0-5	Failure condition, escalation path, remediation owner, SLA, and review trigger are defined.
Control rationalization	0-5	Duplicate, stale, manual, low-value, or policy-only controls are identified for retirement or redesign.
Governance readiness	0-5	Controls are connected to governance routes, decision logs, evidence checklists, platform maps, workflow inventory, and AI initiatives.

Suggested readiness score: average the ten scores, then classify 0-1.9 as Fragmented control environment, 2.0-3.4 as Mapped but weakly monitored controls, 3.5-4.4 as Governed control layer, and 4.5-5.0 as AI-ready control architecture.

AI prompts

- Given this control, classify the control category, risk or obligation, accountable owners, evidence source, test method, AI involvement, and recommended governance route.
- Identify missing control owners, weak evidence, stale review dates, unclear AI boundaries, source-of-truth gaps, data lineage gaps, and missing failure paths.
- Determine whether this control should be preventive, detective, corrective, approval-based, automated, manual, retired, redesigned, or escalated.
- Score the control from 0 to 5 across ownership clarity, control purpose clarity, evidence strength, system and data lineage, testability, AI boundary clarity, exception handling, failure response, control rationalization, and governance readiness.
- Generate the minimum evidence package required to prove this control is operating effectively.
- Draft a remediation plan for a failed or stale control, including owner, failure condition, fix, evidence, escalation path, and review date.
- Create a Lapemo ingestion plan that turns this control map into control, owner, evidence, system, data, AI boundary, exception, issue, and governance route objects.

Validation rules

- Every control must have one accountable control owner.
- Every control must state the risk, obligation, behavior, workflow, decision, or AI boundary it controls.
- Every control must identify evidence source, evidence owner, test method, frequency, and review date.
- Every control touching a system must name the system owner and system of record or execution environment.
- Every control touching data must name the data owner, source of truth, lineage dependency, sensitivity, and freshness rule.
- Every AI-involved control must define allowed AI actions, blocked AI actions, human review rule, logging rule, and kill-switch or escalation path.
- Every failed control must have a failure condition, escalation route, remediation owner, and target resolution time.
- Every exception must have an owner, rationale, approval authority, expiration date, evidence requirement, and review date.
- A control cannot be considered active if ownership is unclear, evidence is missing, review date is stale, or test method is undefined.
- Status must never be encoded only by color. Use labels such as active, stale, failed, exception, retired, redesign, AI-sensitive, or escalated.

Lapemo ingestion mapping

Lapemo object	Fields / entities	Use
Knowledge object	Control Map	Canonical reusable artifact for governance-layer control ownership and monitoring.
Control object	Control ID, name, purpose, category, risk, frequency, test method, status	Creates structured controls that can be monitored and reviewed.
Ownership object	Control owner, process owner, system owner, data owner, evidence owner, remediation owner	Connects controls to accountable roles across the operating model.
Evidence object	Evidence source, evidence owner, freshness, confidence, storage location, test result	Turns control assurance into inspectable proof.
Platform object	System owner, execution system, system of record, logs, integrations, access model	Connects controls to tools, systems, and integration points.
Data object	Data source, data owner, lineage, sensitivity, freshness, downstream use	Connects controls to data lineage and source-of-truth rules.
AI boundary object	AI involvement, allowed actions, blocked actions, human review, logs, kill switch	Controls AI usage inside governance-sensitive workflows.
Exception object	Exception owner, rationale, approval, expiration, remediation, review date	Tracks temporary deviations and prevents permanent shadow governance.
Issue / escalation object	Failure condition, escalation route, remediation owner, SLA, outcome	Moves failed or stale controls into formal resolution.

Website positioning

Use this artifact as a downloadable governance-layer control template and as a future guided skill inside Lapemo. The website version should explain that controls are not just audit artifacts. They are operating-model boundaries that connect ownership, evidence, systems, data, AI behavior, risk, and escalation.

Reusable knowledge object structure

Layer	Reusable asset
Human guide	Plain-English explanation, control categories, map template, workflow, and scale-specific versions.
Downloadable template	DOCX and PDF for workshops, governance design, executive briefings, and website downloads.
Machine-readable schema	JSON object with required fields, scoring logic, prompts, validation rules, and Lapemo mappings.
Guided skill	Future Lapemo workflow that asks control-mapping questions, scores control health, validates evidence, and recommends remediation or escalation.