

LPM Reusable Escalation Map

A versioned knowledge object for surfacing blocked ownership, decision conflict, risk, and AI escalation paths.

Field	Value
Object type	LPM Knowledge Object
Primary LPM layers	Governance Architecture, Decision Architecture, Ownership Map, Communication Architecture, AI Amplification
Connected layers	Identity & Incentives, Information Ecology, Platform Structure
Primary use	Define when issues, decisions, dependencies, risks, exceptions, and AI events must escalate, who owns the path, and how resolution is tracked.
Website use	Downloadable template, executive guide, operating model reference, JSON object for Lapemo ingestion, and future guided skill.
Version	1.0
Owner	LPM / Lapemo
Last reviewed	2026-06-24

An Escalation Map defines how the enterprise moves from signal to owner, owner to decision, decision to resolution, and resolution to operating memory. It prevents important issues from disappearing inside meetings, channels, side conversations, or informal executive access.

The object is reusable across three company profiles: 500+, 5,000+, and 10,000+ employees.

1. Knowledge object model

This knowledge object is designed to be used as both a downloadable artifact and a future reusable Lapemo skill.

- Human guide - plain-language escalation guidance for executives, transformation leaders, operations, product, technology, risk, governance, data, and AI teams.
- Template artifact - a downloadable map teams can use to define escalation paths before work, systems, or AI autonomy scale.
- Machine-readable schema - fields, scoring logic, validation rules, mappings, prompts, review triggers, and version metadata.
- Guided skill - an AI-assisted workflow that classifies escalation type, severity, owner path, evidence quality, AI boundary risk, and required follow-up object updates.

2. Why this matters for AI scaling

AI will speed up routing, summarization, recommendations, and execution. If escalation paths are unclear, AI will move issues faster through the wrong owners or escalate noise while missing true risk. The map makes escalation explicit, tiered, owner-based, and auditable.

3. Core principles

Principle	Meaning
Escalation is a designed path	Escalation should not depend on who knows whom, who is loudest, or who has executive access.
Escalate by consequence	The trigger should be tied to customer, employee, financial, regulatory, platform, governance, or AI impact.
One owner per escalation	Every open escalation has one accountable escalation owner and one resolution owner.
Speed is tiered	Low-risk issues resolve locally. Material issues move quickly to the right authority tier.
Evidence travels with the escalation	Escalations must include the decision, dependency, risk, evidence, impact, options, and recommended path.
Escalation creates memory	Resolved escalations should feed the Decision Log, Ownership Map, risk register, backlog, control library, or AI governance record when material.
AI events have stop paths	AI-enabled workflows need human override, incident response, boundary owner, and stop-control paths before autonomy scales.

4. Canonical fields

Field	What it captures	Required?
Escalation ID	Unique identifier for the escalation, issue, exception, conflict, risk, or AI event	Yes
Escalation category	Decision conflict, ownership gap, dependency, delivery risk, platform risk, data risk, governance exception, AI event, customer impact, financial impact, people impact, security, privacy, legal, or regulatory issue	Yes
Trigger condition	What caused the escalation and what threshold was breached	Yes
Severity tier	Tier 0 local, Tier 1 functional, Tier 2 cross-functional, Tier 3 executive, Tier 4 enterprise control, or Tier 5 board/regulator/external	Yes
Business impact	Impact on customer, revenue, cost, employee experience, operations, risk, compliance, strategy, or execution	Yes
Affected decision	Decision or decision right connected to the escalation	Required when decision-related
Affected owner	Accountable owner, process owner, system owner, data owner, control owner, or AI boundary owner	Yes
Escalation owner	One person or role accountable for moving the escalation to resolution	Yes
Resolution owner	Person or role accountable for fixing the issue, decision, dependency, control, or workflow	Yes

Field	What it captures	Required?
Control owner	Risk, compliance, legal, privacy, security, audit, finance, or model-risk owner	Required for material risk
AI boundary owner	Human owner accountable for AI override, monitoring, stop control, and incident path	Required when AI involved
Evidence attached	Facts, metrics, decision record, dependency map, policy, system evidence, AI output, audit evidence, or impact analysis	Yes
SLA / response time	Expected first response, decision time, resolution time, and review cadence by severity tier	Yes
Communication path	Where escalation status is communicated and who is informed	Yes
Decision log link	Link to decision record when escalation results in a material decision	Required if material
Status	Open, triaged, escalated, decision pending, resolving, blocked, resolved, superseded, or closed	Yes
Review date	Date when escalation, root cause, and operating-model correction are reviewed	Yes
Version	Artifact version, owner, last reviewed date, and change history	Yes

5. Escalation scoring logic

Score	Meaning
0	Escalation paths are informal, political, meeting-driven, or dependent on personal relationships.
1	Escalation paths exist but are inconsistent, slow, undocumented, or disconnected from owners and decision rights.
2	Escalation tiers are defined, but evidence standards, SLAs, AI triggers, control owners, or closure rules are weak.
3	Escalation paths are clear, owner-based, severity-tiered, evidence-backed, and connected to decisions, risks, and execution.
4	Escalation is federated, auditable, AI-aware, monitored, tied to operating-model corrections, and continuously improved.

Escalation health score: average of path clarity, owner clarity, severity accuracy, evidence quality, SLA discipline, control coverage, AI boundary clarity, communication quality, and closure discipline.

High-risk flag: any escalation with no owner, no resolution owner, missing control owner for material risk, AI involvement without a boundary owner, unresolved SLA breach, or material decision not logged.

6. Severity tiers

Tier	When used	Typical owner	First response	Logging standard
Tier 0 - Local	Small issue inside one team or workflow	Team lead, product owner, process owner, or domain operator	Same day or next business day	No enterprise log unless recurring
Tier 1 - Functional	Issue within one function, product, platform, or process	Functional owner or delegated accountable owner	1-2 business days	Log if tied to roadmap, people, budget, platform, or AI
Tier 2 - Cross-functional	Multiple teams, systems, data flows, dependencies, customers, or controls affected	Named cross-functional escalation owner	24-48 hours	Escalation record and decision log if material
Tier 3 - Executive	Funding, strategy, portfolio, operating model, vendor, major customer, delivery, or control tradeoff	Executive sponsor or executive forum with named owner	24 hours	Decision log and evidence pack required
Tier 4 - Enterprise control	Security, privacy, legal, regulatory, model risk, enterprise platform, data governance, or AI boundary breach	Enterprise control owner and accountable executive	Immediate to 24 hours	Formal record, control owner, and review trigger required
Tier 5 - Board / regulator / external	Material external commitment, regulator exposure, public incident, legal entity impact, or board-level risk	Board-facing executive or formally delegated authority	Immediate	Formal evidence pack and audit trail required

7. Escalation triggers

Trigger	What it means	Primary LPM mapping
Ownership gap	No clear owner for decision, workflow, control, platform, data, or AI boundary	Ownership Map and Decision Rights Model
Decision conflict	Two active owners or forums claim authority over the same decision	Decision Rights Matrix and Decision Log
Dependency stall	Work is blocked by another team, system, vendor, policy, or data dependency	Platform Structure and Communication Architecture
Control exception	Required control, approval, evidence, policy, or audit step is missing or bypassed	Governance Architecture
AI boundary event	AI output, agent action, automation, model, or prompt workflow crosses approved scope	AI Amplification and Governance Architecture
Data integrity issue	Source data, lineage, quality, access, or definition is disputed or stale	Information Ecology
Customer or employee impact	Issue affects external customers, internal workforce, service continuity, or experience quality	Identity & Incentives and Communication Architecture
Material value risk	Value realization, cost, revenue, strategic benefit, or transformation outcome is at risk	Ownership Map and Decision Architecture

8. Role model

Role	Accountability	Posture
Issue reporter	Raises the escalation with trigger, evidence, severity, impact, and recommended path	Initiates
Escalation owner	Owens movement from triage to decision, resolution, communication, and closure	Accountable
Resolution owner	Fixes the underlying issue, dependency, decision, workflow, control, or system condition	Executes
Decision owner	Owens the decision connected to the escalation and records it when material	Decides or owns decision memory
Control owner	Reviews risk, compliance, legal, privacy, security, audit, finance, or model-risk exposure	Controls
Communication owner	Ensures the right stakeholders are informed without turning escalation into noise	Communicates
Executive sponsor	Breaks high-impact deadlocks, tradeoffs, or resource conflicts	Escalates authority
AI boundary owner	Owens AI override, stop-control, monitoring, incident path, and post-event review	Controls AI

9. SLA and response model

Tier	First response	Resolution expectation	Auto-escalate when
Tier 0	Same day or next business day	Within team rhythm	If recurring three times or unresolved after agreed window
Tier 1	1-2 business days	Within sprint, planning cycle, or function SLA	If dependency, funding, control, or cross-functional conflict appears
Tier 2	24-48 hours	Within 5-10 business days or next governance checkpoint	If customer, platform, regulatory, AI, or executive tradeoff appears
Tier 3	24 hours	Executive decision window defined by impact	If enterprise policy, major risk, or resource conflict remains unresolved
Tier 4	Immediate to 24 hours	Formal remediation plan with control owner	If breach, incident, regulator exposure, or AI stop-control event occurs
Tier 5	Immediate	Formal board/regulator/external path	Handled under formal governance, legal, audit, or crisis protocols

10. Version A - 500+ employee company

A 500+ company needs a simple escalation map that reduces founder/executive dependency without introducing corporate theater.

Design area	500+ version	Minimum standard
Primary problem	Escalation still moves through founders, executives, strong operators, Slack/Teams, and informal urgency	Create a simple escalation ladder before work becomes personality-driven
Authority model	Three-tier path: team, functional/cross-functional owner, executive sponsor	Keep it light but explicit
Owner standard	Every escalation has a reporter, escalation owner, resolution owner, and decision owner if a decision is needed	One owner per path
Evidence standard	Short issue brief: trigger, impact, owner, blocker, options, and recommendation	No escalation without facts
Communication path	Single escalation channel or page connected to work system and leadership rhythm	Avoid side-channel chaos
AI trigger	Any AI pilot touching customers, employees, data, controls, or external commitments escalates to named owner	AI must not bypass ownership

500+ design principle: make escalation visible without creating bureaucracy. The goal is one clear path from issue to owner to decision.

11. Version B - 5,000+ employee company

A 5,000+ company needs escalation paths that cross functions, platforms, products, vendors, data teams, and governance forums without losing accountability.

Design area	5,000+ version	Minimum standard
Primary problem	Escalations cross functions, platforms, products, vendors, data teams, and governance forums	Separate delivery escalation from authority escalation
Authority model	Five-tier model: team, function, cross-functional, executive, enterprise control	Map escalation to decision rights and materiality
Owner standard	Escalation owner, resolution owner, decision owner, control owner, communication owner, and AI boundary owner where needed	Role separation reduces noise and drift
Evidence standard	Structured escalation record with dependency map, impact analysis, decision needed, options, control review, and SLA	Escalations must be reviewable
Communication path	Escalation register connected to Jira, ServiceNow, Teams/Slack, governance forums, and decision log	Status must not live in meetings only
AI trigger	AI routing, recommendation, automation, or agent action requires severity path, override path, and control owner	AI escalation becomes part of operating control

5,000+ design principle: separate delivery escalation from authority escalation and connect both to decision rights, controls, and AI boundaries.

12. Version C - 10,000+ employee company

A 10,000+ company needs federated escalation paths that preserve local speed while centralizing memory, controls, auditability, and AI boundary enforcement.

Design area	10,000+ version	Minimum standard
Primary problem	Escalation fragments by BU, region, legal entity, platform, risk type, governance forum, and executive structure	Federate escalation locally while centralizing memory, controls, and AI boundaries
Authority model	Six-tier model including enterprise reserved, board, regulator, and external commitment paths	Support local speed and enterprise control
Owner standard	Escalation owner, resolution owner, decision owner, control owner, executive sponsor, legal/entity owner, communication owner, AI boundary owner, and value owner where needed	Complexity requires formal role separation

Design area	10,000+ version	Minimum standard
Evidence standard	Formal evidence pack for regulated, customer-impacting, employee-impacting, platform, data, model, or AI-autonomous events	Replayable evidence is mandatory
Communication path	Enterprise escalation registry with links to decision memory, risk system, audit evidence, operating model map, and incident record	No hidden executive escalation paths
AI trigger	Autonomous or semi-autonomous AI events require stop control, incident path, governance review, and supersession of failed authority logic	AI authority must be explicit and revocable

10,000+ design principle: federate escalation paths locally while centralizing memory, controls, and AI boundary enforcement.

13. Escalation map template

Use this template to create a reusable escalation path for a decision, workflow, platform, control, AI initiative, or operating-model domain.

Field	Value	Instruction
Escalation ID		Unique identifier for the escalation record
Category		Decision conflict, ownership gap, dependency, control exception, AI event, customer impact, platform risk, data risk
Trigger condition		What threshold, policy, decision, dependency, or boundary was breached?
Severity tier		Tier 0 through Tier 5
Business impact		Customer, employee, revenue, cost, regulatory, platform, data, or AI impact
Affected decision / owner		Decision, owner, system, process, data object, or AI workflow affected
Escalation owner		One accountable owner for movement to resolution
Resolution owner		Who fixes the issue or implements the decision?

Field	Value	Instruction
Control owner		Required for material risk, security, privacy, legal, model risk, audit, or compliance exposure
AI boundary owner		Required when AI is involved
Evidence attached		Facts, metrics, logs, screenshots, decision record, policy, data lineage, AI output, or impact analysis
SLA / response time		First response, decision time, resolution time, and review cadence
Communication path		Where status is posted and who must be informed
Decision log link		Required when escalation creates, changes, or supersedes a material decision
Status		Open, triaged, escalated, decision pending, resolving, blocked, resolved, superseded, or closed
Review date		When root cause and operating-model correction will be reviewed

14. AI escalation boundary levels

Level	Escalation rule	Human accountability
Level 0 - No AI	Normal escalation rules apply	No AI-specific boundary owner required
Level 1 - AI drafts or summarizes	Escalate if AI output changes meaning, omits material evidence, or creates decision confusion	Decision owner validates final record
Level 2 - AI recommends	Escalate if recommendation conflicts with policy, evidence, owner authority, or risk tier	Decider and control owner review when material
Level 3 - AI routes or triggers workflow	Escalate if routing logic misclassifies severity, owner, system, dependency, or audience	Process owner and AI boundary owner approve changes
Level 4 - AI executes with approval	Escalate if approval path is bypassed, evidence is weak, or action creates downstream risk	AI boundary owner and control owner own stop path
Level 5 - Autonomous AI	Immediate escalation for unexpected action, boundary breach, customer impact, regulated exposure, or control failure	Executive owner, AI boundary owner, and control owner accountable

15. Validation rules

Validation condition	System response	Reason
No escalation owner	Block escalation record approval	Escalation without ownership becomes noise
No resolution owner	Flag unresolved issue risk	Escalation must lead to a fix, decision, or closure
Severity tier missing	Require classification	Response path depends on consequence
Material escalation without control owner	Escalate to governance/control path	Risk-bearing issues need control ownership
AI involved but no AI boundary owner	Block AI workflow or escalate immediately	AI authority must have a human accountable owner
No evidence attached	Return to submitter	Escalations need facts, not opinions
Escalation open past SLA	Auto-escalate to next tier	Stale escalation creates operating drag
Decision created but not logged	Require Decision Log entry	Material decisions must become operating memory
Same issue recurs repeatedly	Create operating-model correction	Repeated escalation indicates structural failure

16. Mapping rules

Connected LPM object	Escalation Map mapping
Ownership Map	Affected owner, escalation owner, resolution owner, control owner, and AI boundary owner must map to named ownership.
Decision Rights Model	Severity tier and authority path must match decision materiality and rights.
Decision Rights Matrix	Escalated decision must map to decider, recommender, consulted, informed, implementation owner, and control owner.
Decision Log	Material escalations that create, change, or supersede decisions must be logged.
AI Initiative Owner Register	AI-related escalations map to initiative owner, value owner, control owner, and AI boundary owner.

Connected LPM object	Escalation Map mapping
Incentive Alignment Checklist	Recurring escalations may reveal incentives that reward local optimization, delay, risk hiding, or unclear ownership.
Information Ecology	Escalations tied to bad data, missing lineage, stale evidence, or conflicting definitions map to information health.
Platform Structure	System, workflow, integration, and vendor escalations map to platform owners and operational controls.
Governance Architecture	Control exceptions, audit exposure, regulatory paths, policy violations, and risk decisions map to governance owners.

17. AI prompts for the guided skill

- Classify this escalation by category, severity tier, affected LPM layer, owner gap, evidence quality, and decision path.
- Identify whether this issue should stay local, move to a functional owner, escalate cross-functionally, or become an executive or enterprise-control decision.
- Detect missing roles: escalation owner, resolution owner, decision owner, control owner, communication owner, and AI boundary owner.
- Determine whether this escalation requires a Decision Log entry, Ownership Map update, risk record, AI initiative update, or governance review.
- Summarize the escalation into an executive-ready brief with trigger, impact, options, recommendation, owner, SLA, and next decision needed.
- Identify repeated escalations that indicate a structural operating-model failure rather than a one-off delivery issue.
- Generate the correct escalation map version for a 500+, 5,000+, or 10,000+ employee company.

18. Render outputs

Output	Use
Word document	Workshop, consulting, operating-model design, internal enablement, website download
PDF guide	Executive education, briefing, governance design, AI readiness
Website page	Downloadable resource and educational landing page
Interactive form	Guided escalation intake and triage
CSV import	Bulk import of escalation paths, triggers, and SLAs
JSON object	Lapemo ingestion, scoring, validation, and automation rules
In-app workflow	Live escalation routing, escalation health, AI event triage, and operating-model correction

19. Review and update triggers

- Company crosses a major scale threshold, such as 500, 5,000, or 10,000+ employees.
- Escalations repeatedly bypass formal paths and move through executive side channels.
- An AI workflow, automation, or agent creates a decision, routing, customer, employee, regulatory, or control event.
- A major platform, system of record, vendor, data domain, or governance forum changes.
- A material incident, audit finding, regulatory issue, customer impact, or operating-model failure occurs.
- Escalation SLAs are repeatedly missed or decisions repeatedly stall.
- Ownership, decision rights, or incentives are restructured.

20. Website positioning copy

Escalation Map

A reusable LPM method for defining when issues, risks, decisions, dependencies, and AI events move from local resolution to cross-functional, executive, enterprise-control, or external escalation. Use it to reduce hidden blockers, side-channel escalation, unclear ownership, and unmanaged AI risk.

21. Practical guidance

Do not make every problem an escalation. Escalation is for blocked ownership, material risk, decision conflict, unresolved dependency, AI boundary events, or repeated operating-model failure. The goal is not more meetings. The goal is faster resolution with clearer accountability.