

What does an AI-augmented legal and compliance department look like?

Legal and compliance department

Where Legal, Risk and Compliance is heading in the next two to three years, and what GRAIL believes it takes to get there first.

“The system watches the portfolio. People decide what the company will accept.”

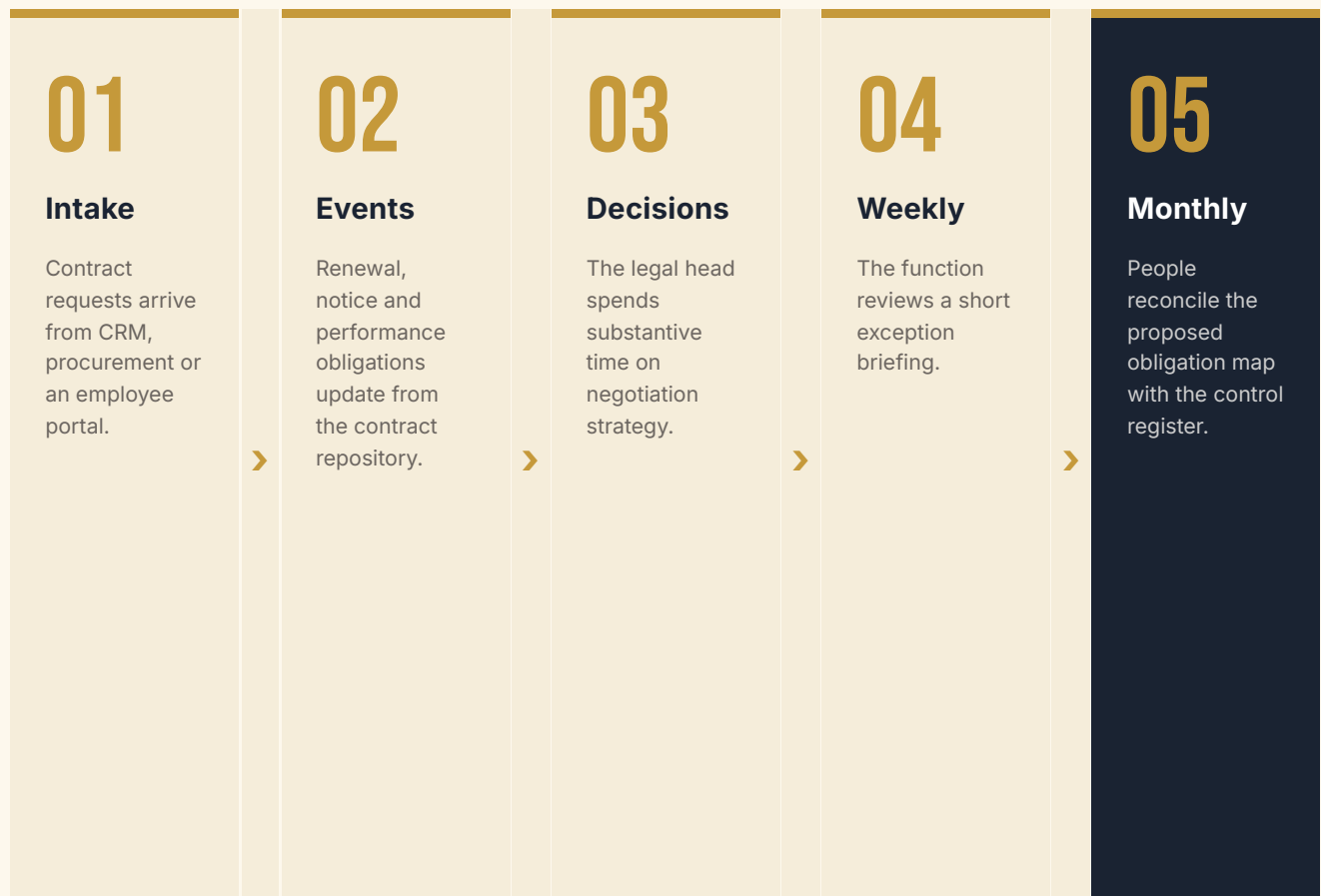
- 01 Where does your company discover risk after it has spread?
- 02 What does your company forget every time Legal approves an exception?
- 03 Which decisions are your lawyers still making without the right evidence?

WHAT DOES AN AI-AUGMENTED **LEGAL AND COMPLIANCE DEPARTMENT** LOOK LIKE?

Where Legal, Risk and Compliance is heading in the next two to three years, and what GRAIL believes it takes to get there first.

Most legal and compliance work begins when somebody sends in a request. By then the contract is waiting, the obligation is close, or the policy is already stale. **The change that matters is that legal coverage becomes continuous, while approved judgment becomes an operating asset the whole company can use.** The decision stays with the person. The preparation starts before the request.

THE LEGAL FUNCTION'S 2028 MONTH



The system watches the portfolio. People decide what the company will accept.

GRAIL's view, from building AI-augmented work inside management functions. A position, not a survey.

A small team carries a company-wide *queue*.

A Nordic mid-market Legal, Risk and Compliance function usually has one to three core people. The in-house lawyer may also be company secretary. The compliance or quality lead may also be the Data Protection Officer. Procurement, finance, HR, IT security and external counsel supply part-time capacity.

The function protects enterprise value through risk control and affects revenue directly. Contract turnaround can delay an order. An unresolved privacy issue can block a product launch. Slow vendor review can hold up an implementation. The function sits across top-line velocity and downside protection.

Eight processes

01	Contract drafting, review and negotiation	05	Internal controls and audit support
02	Contract lifecycle and obligations	06	Incidents and whistleblowing
03	Privacy and data protection	07	Disputes, claims and insurance
04	Regulatory monitoring and policy management	08	External counsel and corporate governance

The work is measured through contract turnaround, open legal requests, agreements on approved paper, renewal notices caught, overdue obligations, DPIA cycle time, privacy-request deadlines, audit findings, policy attestations, incident closure, external counsel spend, litigation exposure and insurance recoveries.

Where the information lives is the problem. Outlook or Gmail, SharePoint or Drive, Word files, e-signature, CRM, ERP, spreadsheets and external counsel portals each hold part of the record. A CLM or privacy platform may exist. The reliable context still sits partly in people's heads.

The record can show that a control is complete while the person responsible knows it is weak.

Accepted fallback clauses, regulator history, reasons for concessions, counsel performance and prior interpretations remain personal knowledge. The function can retrieve the document without necessarily retrieving the judgment behind it.

Coverage becomes *continuous.*

The function changes in two fundamental ways.

Legal coverage moves from a request queue to continuous coverage. The current function sees a contract, regulation or control when somebody sends it in. The augmented function watches authorized information flows, detects a relevant event and prepares the response before the issue becomes urgent. Every contract can be compared with the playbook. Every renewal can be visible. Each regulatory update can arrive with a proposed map to affected policies, systems, contracts and owners.

Institutional judgment becomes an operating asset. Negotiation positions, approved exceptions, prior advice and control interpretations form a maintained context layer. The company depends less on one lawyer remembering why a concession was made years earlier. Each reviewed matter improves the next review because the approved reasoning returns to the playbook.

First-pass reading and drafting become abundant. Legal judgment, accountability and negotiation authority remain scarce.

The function can offer more predictable turnaround and continuous obligation visibility without pretending that every novel legal problem is easy. Bounded document work can become faster and more consistent. Contested interpretations, disputes and relationship-sensitive negotiations still depend on experienced people.

WHERE IT IS WEAKEST the combination is weakest when the facts are disputed, the law is unsettled, the relationship is delicate or the decision creates an irreversible commitment. Those matters stay with named people, and should.

A day, a week, a *month*.

A function that invests now still has one to three core people in many mid-market companies in 2028. Capacity has moved more often than disappeared. A fractional legal-operations or data specialist may support several control functions. External counsel handles fewer routine first drafts and more jurisdiction-specific opinions, disputes and independent review.

The day

INTAKE

Contract requests arrive from CRM, procurement or an employee portal. The workflow identifies the agreement type, compares incoming language with approved positions, explains deviations and prepares tracked changes. Low-risk company templates follow predefined approval paths. The lawyer reviews material departures and negotiates the commercial risk with the business owner.

EVENTS

Renewal, notice and performance obligations update from the contract repository. A new vendor, processing activity, product feature or employee system prompts the relevant privacy or compliance work. Incident files receive a chronology and deadline checklist inside restricted matter spaces.

DECISIONS

The legal head spends substantive time on negotiation strategy, contested risk, product and market choices, management advice and the company's agent portfolio. Playbook changes receive the care once reserved for individual agreements because one approved change can shape hundreds of later decisions.

THE WEEK The function reviews a short exception briefing. It covers deals outside policy, obligations approaching breach, regulatory changes with likely impact, control failures and matters exceeding budget. Sales, procurement, HR and IT join for decisions assigned to them. The meeting is about trade-offs, not collecting status.

THE MONTH People reconcile the proposed obligation map with the control register. Policy owners receive cited changes and impact explanations. The contract portfolio is reviewed for concentration, unusual liabilities, renewal exposure and commitments that do not match invoices or operating performance. The board sees changes in exposure, open decisions and assurance quality.

Whole-portfolio review, continuous obligation visibility and preserved reasoning used to be episodic. They become the normal operating rhythm.

What runs, and what stays with the *person*.

PROCESS	WHAT THE AGENT DOES	WHAT STAYS WITH THE PERSON
Contract drafting, review and negotiation	Identifies the agreement type, compares language with the playbook, explains deviations, proposes tracked changes and drafts the negotiation brief	Acceptable risk, commercial context, material negotiation and approval of departures
Contract lifecycle and obligations	Extracts parties, dates, notice rules, prices and obligations; maintains the register; prepares owner briefings and recommends renewal or termination steps	Approval of notices, commitments and commercial action
Privacy and data protection	Pre-populates assessments, finds missing facts, maps risks to prior controls and locates candidate records for a request	The DPO challenges the business owner; people verify identity, scope, exemptions, redactions and the conclusion
Regulatory monitoring and policy management	Monitors approved official sources, summarizes cited changes, proposes obligation mappings and drafts affected policy sections	Counsel decides applicability; policy owners approve changes and assigned actions
Internal controls and audit support	Prepares test plans, gathers evidence and flags missing or inconsistent support across connected records	Control owners explain exceptions; compliance and internal audit judge sufficiency and close findings
Incidents and whistleblowing	Preserves the original report, prepares a summary and chronology, checks deadlines and tracks remediation inside a restricted workspace	Named investigators decide credibility, scope, interviews, findings and employment consequences
Disputes, claims and insurance	Deduplicates documents, proposes relevance categories, builds cited chronologies and compares claims with policy language	Lawyers validate samples and privilege calls; coverage, settlement and litigation strategy stay human
External counsel and corporate governance	Prepares matter instructions, compares invoices with billing rules, summarizes advice and drafts director briefs and minutes	Counsel selection, acceptance of advice, board judgment and final minutes remain human decisions

Look hardest at the right-hand column. Each line contains accountability, interpretation or authority. The left-hand column exists to give those decisions better evidence, stronger memory and more of the team's attention.

Five stages across *The Access Ladder.*

A realistic path has five stages. They map onto the rungs of The Access Ladder. The sequence matters because legal context becomes more sensitive as live data and action enter the workflow.

- 01 Documents only · Rung: Curated Knowledge**
Approved templates, playbooks, policies and prior advice sit in a permission-controlled SharePoint or Drive location. Drafting, comparison and research begin here. The agent reads. A person supplies matter context and approves every output.
- 02 Read access · Rung: Connected Context**
CLM and e-signature data create a live contract register and reliable lifecycle events. The agent can see signed language, status, renewals and notice dates. The system of record remains authoritative.
- 03 Cross-system read access · Rung: Connected Context**
CRM and ERP add deal value, customer, supplier, invoice and performance data. Legal terms can be read against their business consequence. A warehouse becomes necessary when the question depends on cross-system history rather than a current lookup.
- 04 Read and act with approval · Rung: Controlled Action**
The agent prepares drafts, updates metadata and launches approval workflows. External sends, signature, acceptance, legal advice and contractual commitments retain named human approval.
- 05 Purpose-specific access · Rung: Bounded Action**
Privacy, HR and whistleblowing connect last. Access is narrow, identifiable case content is isolated, and action expands only where it is reversible and exception rates are measured.

The system landscape in September 2026

Microsoft 365	Graph supports production reads and writes to SharePoint files and lists, with site-scoped permissions. Federated connectors support real-time retrieval, while custom connectors remain read-only. Action needs a separate approved surface.
Google Workspace	Drive and Gmail APIs are mature. Remote MCP servers for Gmail, Drive, Docs and Calendar were in developer preview in August 2026. They inherit user permissions and can act, which makes instruction integrity and approval boundaries material.
Oneflow	REST APIs and webhooks support contract creation, reading, updates, publishing, approvals, lifecycle events and signatures. No first-party MCP server was documented.
Juro and Ironclad	Juro released a Claude MCP connection in June 2026. Ironclad supports permission-aware contract search and, with the relevant add-on, obligation operations. Both also provide APIs or webhooks.
Docusign and Adobe Acrobat Sign	Both have mature APIs and webhooks. Docusign's MCP server supports agreement search and workflow action in open beta. No first-party Acrobat Sign MCP was verified.
Privacy and GRC	OneTrust exposes APIs across inventories, DPIAs, data requests, incidents, policies and AI-governance assessments. Its public MCP endpoint supports developers, not a verified operational connection to a customer tenant.
CRM and ERP	HubSpot and Salesforce had generally available hosted MCP servers by April 2026. Business Central has mature REST APIs. Fortnox combines read and write scopes, so monitoring is better placed behind a read-only proxy.

Point connections stop being enough when obligations must be compared with invoices, incidents with control failures, vendor terms with service performance, or policy changes with historical evidence.

A headless legal stack keeps CLM, e-signature and GRC as systems of record. Staff begin work through Teams, email or a controlled conversation layer. Every action records the requesting user, retrieved sources, instruction version, model version, proposed output, human approval, resulting change and any rollback.

Six things we believe, from building *this*.

Legal, Risk and Compliance cannot become AI-native by adding a drafting assistant to the request queue. The operating model has to change. Six beliefs define that change.

01 **The queue is the symptom. Late visibility is the problem.**

A faster first draft helps after a matter has reached Legal. Continuous coverage matters more because it detects the contract event, policy change, control failure or renewal before urgency removes the good choices.

02 **The playbook is not a document. It is the function's memory.**

Approved positions, exceptions and reasoning have to return to a maintained context layer. If the company stores the final contract but loses why it accepted the clause, the next review begins from memory again.

03 **Abundant first-pass work raises the value of scarce judgment.**

Reading, comparison, evidence gathering and draft preparation can cover far more of the portfolio. The return is not fewer people. It is more attention on negotiation strategy, product choices, contested risk and board advice.

04 **An obligation only matters when it reaches an owner and a control.**

Regulatory summaries are easy to produce and easy to ignore. The useful chain connects the rule to the policy, system, contract, control, evidence and accountable owner, then returns the approved interpretation to the record.

05 **Augment the judgment. Never automate the authority.**

Contract acceptance, external legal communications, investigation findings, privacy disclosures, legal advice, coverage and settlement decisions stay with named people. The agent prepares the evidence and proposed action. The person carries the accountability.

06 **Legal leadership becomes the designer of decision systems.**

The in-house lawyer remains senior risk counselor, but also owns how approved judgment travels through work. The compliance lead or DPO becomes an obligation architect. Both need to shape permissions, evaluation, source discipline and workflow boundaries.

An AI-augmented legal department is not a lawyer who types faster. It is a company that can see its obligations, preserve its reasoning and bring human judgment to the point where it matters.

Roles, rhythm, and where it *fails*.

The in-house lawyer moves toward negotiation strategy, product decisions, management advice and board counsel. The role also designs legal decision systems: playbooks, approval paths, source standards and the boundary between preparation and authority.

The compliance lead or DPO becomes an obligation architect. The role maintains the relationship between regulation, processing activities, controls, policies and evidence. DPO independence remains important. Business owners remain accountable for their processing and controls.

Quality and vendor-management roles gain responsibility for structured evidence, third-party data and control performance. External counsel concentrates on independent opinions, litigation and unfamiliar jurisdictions.

Junior development needs deliberate redesign. First-pass work once taught document structure and issue spotting. Juniors now need to review machine-produced drafts against source material, identify weak reasoning and explain disagreements to senior counsel.

The rhythm

CURATED START

One contract type, one approved playbook and one accountable workflow owner

DEPENDABLE USE

Source checks, high-impact error review and approved reasoning returned to the knowledge base

CHANGED WEEKLY RHYTHM

Connected registers, exception briefings and work assigned from events rather than inboxes

CONTINUOUS COVERAGE

Cross-system portfolio review, stable permissions and role design around judgment

The pace is set by playbook quality, data cleanup, permissions, testing and behavior change. Model access is not the long pole.

WHERE IT FAILS Vague playbooks. Scattered originals. A tool added without redesigning the workflow. Average accuracy measured while high-impact errors go unexamined. Approved decisions never returned to the knowledge base. Permissions broader than the purpose. Review work placed on top of the old process. Released time treated only as a reason to remove capacity.

Involve the people whose work changes before it changes. The operating model holds when lawyers, control owners, business leaders and specialists can see where their judgment begins and where the machine must stop.

Twelve questions for the function's *leader*.

- 1 A contract assistant could review every customer agreement against your fallback positions before a lawyer opens it. Which agreement type would you start with?
- 2 A live contract register could identify each notice date, price change and renewal obligation without relying on a spreadsheet. What is the cost of the dates you cannot currently see?
- 3 Every approved exception could improve the next review and preserve judgment that now sits in one person's memory. Who decides when an exception becomes an accepted position?
- 4 A regulatory monitor could propose which policies, contracts, systems and owners a new rule may affect. Which regulatory change took the longest to translate into action last year?
- 5 A policy assistant could identify stale sections and prepare cited amendments when the underlying obligation changes. Which important policy has not been substantively reviewed in the past year?
- 6 A DPIA and privacy-request workflow could pre-fill known facts, identify missing evidence and locate likely records without releasing them. Where does your team lose most time in privacy work?
- 7 An inventory could connect every company agent to its owner, purpose, data, vendor and approval status. Can you currently name every agent that processes employee or customer information?
- 8 Continuous control testing could flag missing evidence when a control fails instead of waiting for the annual audit. Which control would benefit most from continuous attention?
- 9 A protected case assistant could build whistleblowing chronologies and track deadlines while investigators retain every credibility decision. Which administrative step most often slows an investigation?
- 10 A dispute assistant could review large document sets, build a cited chronology and let counsel reach case strategy earlier. Which current matter is consuming expensive review time?
- 11 An outside-counsel monitor could compare invoices, budgets, outcomes and prior matters before new work is assigned. Which types of work should now remain inside the company?
- 12 Insurance and board briefings could stay current, showing changed exposure, coverage gaps, overdue decisions and weak evidence. How much leadership time is spent rebuilding information the company already holds?

These are the questions the programme is built to answer with the people who carry the accountability, using their own contracts, controls and decisions rather than a generic demonstration.