CLAUDE COWORK

# The Legal Productivity Plugin Handbook

Version 1.0.0 | For In-House Legal Teams

---

VERSION `1.0.0`

PLUGIN `legal`

RationalEyes.ai

contact@rationaleyes.ai

February 2026

# Table of Contents

## Version 1.0.0 | For In-House Legal Teams

# Part I: Introduction

## What Is the Legal Plugin?

The Legal Productivity Plugin transforms Claude into a specialized assistant for in-house legal teams. It automates contract review, NDA triage, compliance workflows, legal briefings, and templated responses—all configurable to your organization's specific playbook and risk tolerances.

This plugin is designed for legal operations managers, commercial counsel, privacy officers, compliance specialists, and litigation support teams who need to move faster without sacrificing quality or risk management.

**Critical disclaimer:** This plugin assists with legal workflows but does not provide legal advice. All AI-generated analysis should be reviewed by qualified legal professionals before being relied upon for legal decisions.

## Target Personas and Their Workflows

| PERSONA | PRIMARY USE CASES | KEY COMMANDS | KEY SKILLS |
|---|---|---|---|
| **Commercial Counsel** | Contract negotiation, vendor management, deal support | `/review-contract`, `/vendor-check` | contract-review, legal-risk-assessment |
| **Product Counsel** | Product reviews, ToS, privacy policies, IP matters | `/review-contract`, `/brief topic` | contract-review, compliance |
| **Privacy / Compliance** | DPA reviews, DSRs, regulatory monitoring | `/respond dsr`, `/brief daily` | compliance, canned-responses |
| **Litigation Support** | Discovery holds, document prep, case briefings | `/respond hold`, `/brief incident` | canned-responses, meeting-briefing |
| **Legal Operations** | Process optimization, triage, knowledge management | `/triage-nda`, `/brief daily` | nda-triage, legal-risk-assessment |

## Installation and Quick Start

**Install the plugin:**

**Cowork (recommended):** Open **Plugin Settings** in the Cowork desktop app, find **Legal**, and click **Install**. The plugin activates immediately — no CLI required.

**Claude Code CLI (alternative):** If you are using Claude Code in the terminal rather than Cowork, install via:

```
claude plugins add knowledge-work-plugins/legal
```

> **Note:** *All standard Cowork plugins, including Legal, are available from Plugin Settings with a single click. The CLI command above is only needed for Claude Code terminal users.*

No restart required.

**First-time setup** (recommended):

1. **Configure your playbook**: Create `.claude/legal.local.md` in your project directory to define your organization's contract positions, NDA defaults, and response templates.
2. **Connect your tools**: The plugin pre-configures MCP servers for Slack, Box, Egnyte, Atlassian, and Microsoft 365. Authenticate when prompted.
3. **Test a workflow**: Try `/triage-nda` with a sample NDA to see the classification system in action.

## How the Plugin Works

The legal plugin combines three complementary systems:

**Commands** — Explicit actions you invoke by typing a slash command (e.g., `/review-contract`, `/triage-nda`). Commands are workflows you trigger when you need them.

**Skills** — Domain expertise that loads automatically when topics come up. When you're discussing contract terms, the `contract-review` skill activates. When you're handling a data subject request, the `compliance` skill loads. Skills work in the background without you having to invoke them explicitly.

**MCP integrations** — Connections to your existing tools (CLM, document storage, email, chat) that let Claude pull context and take actions across your legal tech stack.

This architecture means you can work naturally—sometimes invoking specific workflows with commands, other times having Claude consult its legal knowledge automatically based on what you're discussing.

# Part II: Core Concepts and Architecture

## The Playbook System

The playbook is the heart of the legal plugin. It defines your organization's negotiation positions, risk tolerances, and standard terms. Without a playbook, the plugin can still analyze contracts using general commercial standards, but it cannot assess deviations from *your* positions.

**Playbook location:** `.claude/legal.local.md` in your project directory (or any local settings file Claude can access).

**What goes in a playbook:**

| SECTION | PURPOSE | EXAMPLE |
|---|---|---|
| **Contract Review Positions** | Standard terms for each major clause type | "Limitation of liability: Mutual cap at 12 months of fees paid/payable" |
| **Acceptable Ranges** | What you can agree to without escalation | "Acceptable range: 6-24 months of fees" |
| **Escalation Triggers** | Terms requiring senior review | "Escalation: Uncapped liability, consequential damages inclusion" |
| **NDA Defaults** | Standard NDA positions | "Mutual obligations required; term: 2-3 years standard, 5 years for trade secrets" |
| **Response Templates** | Configured templates for common inquiries | Paths to template files or inline templates |

**Example playbook structure:**

```
# Legal Playbook Configuration

## Contract Review Positions

### Limitation of Liability
- **Standard position**: Mutual cap at 12 months of fees paid/payable
- **Acceptable range**: 6-24 months of fees
- **Escalation trigger**: Uncapped liability, consequential damages inclusion

### Indemnification
- **Standard position**: Mutual indemnification for IP infringement and data breach
- **Acceptable**: Indemnification limited to third-party claims only
- **Escalation trigger**: Unilateral indemnification, uncapped indemnification

### IP Ownership
- **Standard position**: Each party retains pre-existing IP; customer owns customer da
- **Escalation trigger**: Broad IP assignment, work-for-hire for pre-existing IP

### Data Protection
- **Standard position**: Require DPA for any personal data processing
- **Requirements**: Sub-processor notification, data deletion on termination, breach n
- **Escalation trigger**: No DPA offered, cross-border transfer without safeguards

## NDA Defaults
- Mutual obligations required
- Term: 2-3 years standard, 5 years for trade secrets
- Standard carveouts: independently developed, publicly available, rightfully received
- Residuals clause: acceptable if narrowly scoped

## Response Templates
[Configure paths to template files or define inline templates]
```

**When no playbook is configured:** The plugin informs you and offers two options: (1) help you set up your playbook, or (2) proceed with generic review using widely-accepted commercial standards as the baseline. It clearly notes when operating in generic mode.

## The Traffic Light Classification System

The plugin uses a three-tier risk classification system across multiple workflows:

### GREEN — Acceptable

- Aligns with or exceeds your standard position
- Minor variations that are commercially reasonable
- No action needed beyond noting for awareness

**YELLOW — Negotiate**

- Falls outside standard but within negotiable range
- Common in the market but not your preference
- Requires attention and redline suggestions, but not escalation
- Includes specific alternative language and fallback positions

**RED — Escalate**

- Falls outside acceptable range or triggers escalation criteria
- Unusual or aggressive terms posing material risk
- Requires senior counsel, outside counsel, or business decision-maker sign-off
- Includes risk explanation, market alternatives, and exposure estimates

This system appears in contract review, NDA triage, and risk assessment workflows. It provides consistent, actionable guidance: GREEN means proceed, YELLOW means negotiate with specific talking points, RED means escalate with clear reasoning.

## Tool Connectivity via MCP

The plugin connects to external services through MCP (Model Context Protocol) servers. Five categories are pre-configured:

| CATEGORY | PRE-CONFIGURED SERVERS | PURPOSE |
|---|---|---|
| **Chat** | Slack | Team requests, notifications, triage from channels |
| **Cloud Storage** | Box, Egnyte | Playbooks, templates, executed agreements, precedents |
| **Office Suite** | Microsoft 365 | Email, calendar, document collaboration |
| **Project Tracker** | Atlassian (Jira/Confluence) | Matter tracking, tasks, knowledge base |
| **CLM** | (Not pre-configured) | Contract lifecycle management, approval workflows |

**Additional supported categories** (require manual configuration):

- **CRM** (Salesforce, HubSpot) — Vendor/customer relationship data
- **E-signature** (DocuSign, Adobe Sign) — Signature workflows
- **Additional storage** (Dropbox, SharePoint, Google Drive)

**Graceful degradation:** If a tool is unavailable, the plugin notes the gap and suggests manual checks. Commands continue to work with reduced context rather than failing entirely.

**Authentication:** SSE-based servers (like many SaaS tools) prompt for OAuth authentication on first use. HTTP servers may require API tokens configured as environment variables.

## The Tool Placeholder System

The plugin uses `~category` placeholders for tool-agnostic references:

- `~chat` → Slack (or Teams, if you configure it)
- `~cloud storage` → Box or Egnyte
- `~CLM` → Your contract management system
- `~project tracker` → Atlassian (or Linear, Asana, etc.)

This design makes the plugin adaptable to different tech stacks. See `CONNECTORS.md` in the plugin directory for the complete list of placeholder categories and supported alternatives.

---

# Part III: Commands Reference

## /review-contract — Contract Review Against Playbook

**Purpose:** Analyze a contract clause-by-clause against your organization's negotiation playbook. Flag deviations, generate redlines, and provide business impact analysis.

**Invocation:**

```
/review-contract
```

**Accepts:**

- File upload (PDF, DOCX, etc.)
- URL to a contract in CLM or cloud storage
- Pasted contract text

**Workflow:**

1. **Accept the contract** in any format
2. **Gather context** — asks for:
   - Which side are you on? (vendor, customer, licensor, licensee)
   - Deadline for finalization
   - Focus areas (e.g., "data protection is critical")
   - Deal context (size, strategic importance, relationship)
3. **Load the playbook** from local settings
4. **Clause-by-clause analysis** covering:
   - Limitation of liability
   - Indemnification
   - IP ownership
   - Data protection
   - Confidentiality
   - Representations & warranties
   - Term & termination
   - Governing law & dispute resolution
   - Insurance, assignment, force majeure, payment terms

5. **Flag deviations** using GREEN/YELLOW/RED classification
6. **Generate redline suggestions** with:
   - Current language (quoted from contract)
   - Proposed redline (specific alternative language)
   - Rationale (suitable for sharing with counterparty)
   - Priority (must-have, should-have, nice-to-have)
   - Fallback position (for YELLOW items)
7. **Business impact summary** with overall risk, top 3 issues, negotiation strategy, timeline considerations
8. **CLM routing** (if connected) — recommend approval workflow based on risk

**Output structure:**

```
## Contract Review Summary
- Document, parties, your side, deadline, review basis

## Key Findings
- Top 3-5 issues with severity flags

## Clause-by-Clause Analysis
### [Clause Category] — [GREEN/YELLOW/RED]
- Contract says: [summary]
- Playbook position: [your standard]
- Deviation: [gap description]
- Business impact: [practical meaning]
- Redline suggestion: [specific language, if YELLOW/RED]

## Negotiation Strategy
- Recommended approach, priorities, concession candidates

## Next Steps
- Specific actions
```

**When to use:**

- Vendor contracts during procurement
- Customer agreements requiring review
- Partnership or licensing agreements
- Any commercial agreement requiring risk assessment

**Example invocation:**

```
/review-contract

[Upload vendor SaaS agreement]

Context:
- We are the customer
- Need to close by end of quarter
- Focus on data protection and liability caps
- $250K annual contract value
```

## /triage-nda — NDA Pre-Screening

**Purpose:** Rapidly classify incoming NDAs as GREEN (standard approval), YELLOW (counsel review), or RED (significant issues) to route appropriately.

**Invocation:**

```
/triage-nda
```

**Accepts:**

- File upload
- URL to NDA document
- Pasted NDA text

**Workflow:**

1. **Accept the NDA**
2. **Load NDA playbook** from local settings (or use market-standard defaults)
3. **Quick screen** against criteria:
    - Mutual vs. unilateral structure
    - Definition of confidential information
    - Term and confidentiality survival period
    - Standard carveouts (independent development, public knowledge, third-party receipt, legal compulsion)
    - Permitted disclosures (employees, advisors, affiliates)
    - Return/destruction obligations
    - Residuals clause presence and scope
    - Non-solicitation or non-compete provisions (should not be in NDA)
    - Governing law and jurisdiction

4. **Classify** as GREEN, YELLOW, or RED
5. **Generate triage report** with:
    - Classification and reasoning
    - Screening results table
    - Issues found with severity and suggested fixes
    - Routing recommendation

**Classification criteria:**

**GREEN — Standard Approval:**

- All criteria met
- Market-standard provisions
- No unusual terms
- Route: Approve via standard delegation

**YELLOW — Counsel Review Needed:**

- Minor deviations (broader definition, longer term, missing one carveout)
- Residuals clause present but narrowly scoped
- Minor jurisdiction issue
- Route: Flag specific issues for counsel

**RED — Significant Issues:**

- Unilateral when mutual is required
- Missing critical carveouts
- Non-solicitation/non-compete embedded
- Unreasonable term (10+ years)
- Overbroad definition capturing public information
- Route: Full legal review, do not sign

**When to use:**

- New NDA from sales or business development
- Deciding whether NDA needs full counsel review
- Standardizing NDA screening across legal team
- Training junior team members on NDA evaluation

**Example invocation:**

```
/triage-nda

[Upload NDA from new vendor]

Purpose: Exploratory discussions with SaaS vendor
```

## /vendor-check — Vendor Agreement Status

**Purpose:** Check existing agreements with a vendor across all connected systems. Provides consolidated view of the legal relationship.

**Invocation:**

```
/vendor-check [vendor name]
```

**Workflow:**

1. **Identify the vendor** — handles variations (legal name vs. trade name, parent/subsidiary)
2. **Search connected systems** in priority order:
   - CLM (if connected) — active, expired, pending agreements
   - CRM (if connected) — account status, relationship type
   - Email — recent contract-related correspondence
   - Document storage — executed agreements, redlines
   - Chat — team discussions about vendor
3. **Compile agreement status** for each found agreement:
   - Agreement type (NDA, MSA, SOW, DPA, SLA, etc.)
   - Status (active, expired, in negotiation, pending signature)
   - Effective and expiration dates
   - Auto-renewal terms
   - Key terms summary
   - Amendment history
4. **Gap analysis** — identify missing agreements (e.g., MSA exists but no DPA, and vendor handles personal data)
5. **Generate report** with:
   - Relationship overview
   - Agreement summary table
   - Gap analysis
   - Upcoming actions (expirations, renewals, needed agreements)

- Sources checked and sources unavailable

**When to use:**

- Business team asks about engaging existing vendor
- Checking before signing new agreement
- Vendor relationship review
- Determining if new NDA is needed
- Preparing for vendor negotiation

**Example invocation:**

```
/vendor-check Acme Corporation

Question: Can we proceed with a new SOW or do we need a new NDA?
```

## /brief — Legal Team Briefing

**Purpose:** Generate contextual briefings for legal work in three modes: daily summary, topic research, or incident response.

**Invocation:**

```
/brief daily              # Morning brief
/brief topic [query]      # Research brief on specific question
/brief incident [topic]   # Rapid brief on developing situation
```

### *Daily Brief Mode*

Scans connected sources for legal-relevant items to start your day.

**Sources scanned:**

- Email: contract requests, compliance questions, counterparty responses, external counsel communications
- Calendar: today's meetings needing legal prep, upcoming deadlines
- Chat: overnight messages, legal team channels, direct messages, urgent requests
- CLM: contracts awaiting review, approaching expirations
- CRM: deals moving to legal stages

**Output structure:**

```
## Daily Legal Brief — [Date]

### Urgent / Action Required
[Items needing immediate attention]

### Contract Pipeline
- Awaiting Your Review: [count and list]
- Pending Counterparty Response: [count]
- Approaching Deadlines: [items due this week]

### New Requests
[Contract reviews, NDA requests, compliance questions]

### Calendar Today
[Meetings with legal relevance and needed prep]

### Team Activity
[Key messages from legal channels]

### This Week's Deadlines
[Upcoming deadlines and filing dates]

### Sources Not Available
[Gaps in coverage]
```

### *Topic Brief Mode*

Research and synthesize information on a specific legal question from available sources.

**Searches:**

- Documents: internal memos, prior analyses, playbooks, precedent
- Email: prior communications on topic
- Chat: team discussions
- CLM: related contracts or clauses

**Output structure:**

```
## Topic Brief: [Topic]

### Summary
[2-3 sentence executive summary]

### Background
[Context and history from internal sources]

### Current State
[Organization's current position/approach]

### Key Considerations
[Factors, risks, open questions]

### Internal Precedent
[Prior decisions, memos, positions]

### Gaps
[Missing information, unavailable sources]

### Recommended Next Steps
```

**Important:** Topic briefs synthesize available internal sources. They do not substitute for formal legal research. For current case law or authority, consult Westlaw/Lexis or outside counsel.

### *Incident Brief Mode*

Rapid briefing for developing situations requiring immediate legal attention (data breaches, litigation threats, regulatory inquiries).

**Scans:**

- Email: communications about incident
- Chat: real-time discussions, escalations
- Documents: relevant policies, response plans, insurance
- Calendar: scheduled response meetings
- CLM: affected contracts, indemnification provisions

**Output structure:**

```
## Incident Brief: [Topic]
**Prepared**: [timestamp]
**Classification**: [severity if determinable]

### Situation Summary
[What is known]

### Timeline
[Chronological events]

### Immediate Legal Considerations
[Regulatory notifications, preservation, privilege]

### Relevant Agreements
[Implicated contracts, insurance policies]

### Internal Response
[Activity already occurring]

### Key Contacts
[Relevant internal and external contacts]

### Recommended Immediate Actions
1. [Most urgent]
2. [Second priority]
3. [ ... ]

### Information Gaps
[What is not yet known]

### Sources Checked
```

**Privilege note:** Incident briefs should be marked as attorney-client privileged / work product when appropriate.

**When to use:**

- Daily brief: every morning to prioritize your day
- Topic brief: researching prior positions, understanding organizational precedent
- Incident brief: data breaches, litigation threats, regulatory inquiries, IP disputes

**Example invocations:**

```
/brief daily

/brief topic "what is our position on unlimited liability in vendor contracts?"

/brief incident "potential data breach - vendor reported unauthorized access"
```

## /respond — Generate Templated Response

**Purpose:** Generate responses for common legal inquiries using configured templates with escalation trigger detection.

**Invocation:**

```
/respond [inquiry-type]
```

**Supported inquiry types:**

- `dsr` / `data-subject-request` — GDPR/CCPA data access, deletion, correction
- `hold` / `discovery-hold` — Litigation hold notices
- `vendor` / `vendor-question` — Vendor legal inquiries
- `nda` / `nda-request` — NDA requests from business teams
- `privacy` / `privacy-inquiry` — Privacy-related questions
- `subpoena` — Subpoena responses
- `insurance` — Insurance claim notifications
- `custom` — Use custom template

**Workflow:**

1. **Identify inquiry type**
2. **Load template** from local settings (or offer to create one)
3. **Check escalation triggers** before generating:
   - DSR triggers: minor's data, regulatory authority requester, litigation hold conflict, employee with active dispute
   - Hold triggers: criminal liability, unclear scope, ongoing operations impact
   - Vendor triggers: dispute/breach, litigation threat, regulatory compliance question
   - Subpoena triggers: ALWAYS requires counsel review
4. **Gather specific details** to customize:
   - DSR: requester name, request type, applicable regulation, deadline
   - Hold: matter name, custodians, scope, outside counsel contact

    - Vendor: vendor name, reference agreement, specific question
5. **Generate response** with:
    - Appropriate tone for audience
    - All required legal elements
    - Clear next steps
    - Appropriate disclaimers
6. **Present draft** for review before sending

**Output structure:**

```
## Generated Response: [Inquiry Type]

**To**: [recipient]
**Subject**: [subject line]

---

[Response body]

---

### Escalation Check
[No triggers detected OR flagged triggers with recommendations]

### Follow-Up Actions
1. [Post-send actions]
2. [Calendar reminders]
3. [Tracking requirements]
```

**When to use:**

- Responding to routine data subject requests
- Issuing litigation holds
- Answering vendor questions about contract terms
- Providing NDA to business teams
- Any common inquiry with established template

**Example invocation:**

```
/respond dsr

Request details:
- Requester: John Smith
- Type: Access request (GDPR)
- Received: Feb 14, 2025
- Deadline: March 16, 2025
```

---

# Part IV: Skills Deep Dive

Skills are domain expertise packages that load automatically when relevant topics arise. Unlike commands (which you explicitly invoke), skills work in the background—Claude consults them when needed based on conversation context.

## contract-review — Playbook-Based Contract Analysis

**Triggers when discussing:**

- Contract review, agreement analysis
- Vendor contracts, customer agreements
- Clause negotiation, redline generation
- Risk assessment in commercial agreements

**Core knowledge:**

**Playbook-based methodology:**

1. Load organization's playbook (standard positions, acceptable ranges, escalation triggers)
2. Identify contract type and user's side (vendor/customer/licensor/licensee)
3. Read entire contract before flagging (clauses interact)
4. Analyze each material clause against playbook
5. Consider holistic risk allocation

**Clause analysis framework:**

Covers 12 major clause categories with specific review points for each:

| CLAUSE | KEY ELEMENTS | COMMON ISSUES |
|---|---|---|
| **Limitation of Liability** | Cap amount, carveouts, mutual vs. unilateral, consequential damages | Cap at fraction of fees, asymmetric carveouts, broad exceptions eliminating cap |
| **Indemnification** | Scope, mutuality, cap, procedure, survival | Unilateral when mutual warranted, indemnification for "any breach", no defense control |
| **IP Ownership** | Pre-existing IP, developed IP, work-for-hire, license grants | Broad IP assignment capturing pre-existing, unrestricted feedback clauses |

| CLAUSE | KEY ELEMENTS | COMMON ISSUES |
|---|---|---|
| **Data Protection** | DPA requirement, sub-processors, breach notification, cross-border transfers | No DPA when processing personal data, inadequate breach timeline, no transfer protections |
| **Term & Termination** | Duration, renewal, termination for convenience, wind-down | Long term with no convenience termination, short auto-renewal notice window |
| **Governing Law** | Jurisdiction, arbitration vs. litigation, venue | Unfavorable jurisdiction, mandatory arbitration in remote venue |

**Deviation classification:**

- **GREEN**: Aligns with or better than standard; no action needed
- **YELLOW**: Outside standard but negotiable; requires redline with fallback
- **RED**: Outside acceptable range; requires escalation with risk explanation

**Redline generation best practices:**

1. Be specific — provide exact language ready to insert
2. Be balanced — firm on critical points, commercially reasonable overall
3. Explain rationale — brief explanation suitable for counterparty
4. Provide fallback — alternative if primary ask rejected
5. Prioritize — indicate must-have vs. nice-to-have

**Negotiation priority framework:**

- **Tier 1 (Must-Haves)**: Deal breakers — uncapped liability, missing data protection, core IP risks
- **Tier 2 (Should-Haves)**: Material risk but negotiation room — liability cap adjustments, indemnification scope
- **Tier 3 (Nice-to-Haves)**: Concession candidates — preferred governing law, notice periods, minor definitions

**When this skill activates:**

- Any contract review workflow
- Questions about specific contract clauses
- Negotiation strategy discussions
- Risk assessment in commercial agreements

## nda-triage — NDA Screening and Classification

**Triggers when discussing:**

- NDA review, confidentiality agreements
- Triage criteria, screening NDAs
- NDA approval, routing decisions
- Standard NDA positions

**Core knowledge:**

**Screening checklist** (13 criteria):

1. **Agreement structure**: Mutual vs. unilateral, appropriate for context
2. **Definition scope**: Not overbroad, reasonable marking requirements
3. **Standard carveouts**: All five required (public, prior possession, independent development, third-party, legal compulsion)
4. **Obligations**: Reasonable standard of care, use restriction, need-to-know disclosure
5. **Permitted disclosures**: Employees, contractors, advisors, affiliates
6. **Term**: Agreement term and confidentiality survival reasonable (2-5 years standard)
7. **Return/destruction**: Reasonable with legal/compliance retention exception
8. **Remedies**: Injunctive relief reasonable, no liquidated damages
9. **No non-solicitation**: Should not be in NDA
10. **No non-compete**: Should not be in NDA
11. **No residuals** (or narrowly scoped): Limited to unaided memory, excludes trade secrets
12. **No unusual provisions**: Exclusivity, audit rights, IP assignment don't belong
13. **Governing law**: Reasonable commercial jurisdiction

**Classification rules:**

**GREEN** (all must be true):

- Mutual or appropriate unilateral
- All standard carveouts present
- Term within standard range
- No non-solicitation/non-compete/exclusivity
- No or narrow residuals
- Reasonable jurisdiction
- Standard remedies
- Permitted disclosures include employees, contractors, advisors

**YELLOW** (one or more):

- Broader definition but not unreasonable
- Term longer than standard but in market range
- Missing one carveout (can be added)
- Narrow residuals clause present
- Acceptable but non-preferred jurisdiction

**RED** (one or more):

- Unilateral when mutual required
- Missing critical carveouts (especially independent development)
- Non-solicitation or non-compete provisions
- Unreasonable term (10+ years without justification)
- Overbroad definition capturing public information
- Broad residuals clause (effectively a license)
- IP assignment or license grant
- Not actually an NDA (contains commercial terms)

**Common issues and positions:**

| ISSUE | STANDARD POSITION | REDLINE APPROACH |
|---|---|---|
| Overbroad definition | Limit to marked/identified confidential info | Narrow to reasonable person standard |
| Missing independent development | Must include carveout | Add standard carveout language |
| Non-solicitation of employees | Does not belong in NDA | Delete entirely or limit to targeted solicitation, 12 months max |
| Broad residuals | Resist; limit if required | Limit to unaided memory, exclude trade secrets and patents |
| Perpetual confidentiality | 2-5 years standard | Replace with defined term, offer trade secret carveout |

**When this skill activates:**

- NDA screening and triage
- NDA review requests
- Questions about NDA standards
- Training on NDA evaluation

## compliance — Privacy Regulations and DPA Review

**Triggers when discussing:**

- GDPR, CCPA, CPRA, privacy regulations
- Data processing agreements, DPAs
- Data subject requests, DSRs
- Privacy compliance, cross-border transfers
- Regulatory monitoring

**Core knowledge:**

**Regulation overview:**

**GDPR (EU/EEA):**

- Scope: Processing personal data of EU/EEA individuals
- Key rights: Access, rectification, erasure, portability, restriction, objection
- Response timeline: 30 days (extendable by 60)
- Breach notification: 72 hours to supervisory authority
- International transfers: Require SCCs, adequacy decisions, or BCRs
- DPO requirement: Public authority, large-scale processing of special categories, systematic monitoring

**CCPA/CPRA (California):**

- Scope: Businesses collecting California resident personal information (meeting thresholds)
- Key rights: Know, delete, opt-out of sale, correct (CPRA), limit sensitive PI use (CPRA)
- Response timeline: Acknowledge in 10 business days, respond in 45 calendar days (extendable by 45)
- Service provider agreements: Must restrict use to business purpose

**Other key regulations:** LGPD (Brazil), POPIA (South Africa), PIPEDA (Canada), PDPA (Singapore), Privacy Act (Australia), PIPL (China), UK GDPR

**DPA review checklist:**

Required elements (GDPR Article 28):

- Subject matter, duration, nature, purpose of processing
- Types of personal data and categories of data subjects
- Controller obligations and rights documented

Processor obligations must include:

- Process only on documented instructions
- Personnel confidentiality commitments
- Appropriate security measures (Article 32)
- Sub-processor requirements (authorization, notification, same obligations, liability)
- Assistance with data subject rights
- Assistance with security, breach notification, DPIAs
- Deletion or return on termination
- Audit rights
- Breach notification without undue delay (24-48 hours to enable 72-hour regulatory deadline)

International transfer requirements:

- Transfer mechanism identified (SCCs, adequacy, BCRs)
- Current EU SCCs (June 2021 version) if applicable
- Correct SCC module (C2P, C2C, P2P, P2C)
- Transfer impact assessment completed
- Supplementary measures for gaps
- UK addendum if UK data in scope

**Common DPA issues:**

| ISSUE | RISK | STANDARD POSITION |
|---|---|---|
| Blanket sub-processor authorization | Loss of control | Require notification with right to object |
| Breach notification >72 hours | May prevent timely regulatory notification | Require 24-48 hour notification |
| No audit rights | Cannot verify compliance | Accept SOC 2 Type II + audit upon cause |
| Unclear data deletion timeline | Indefinite retention | Require deletion within 30-90 days of termination |
| Unspecified processing locations | Data could be anywhere | Require disclosure of locations |
| Outdated SCCs | Invalid transfer mechanism | Require current EU SCCs (2021 version) |

**Data subject request handling:**

Process:

1. Identify request type (access, rectification, erasure, restriction, portability, objection, opt-out, limit use)
2. Identify applicable regulation and timeline
3. Verify identity (reasonable measures proportionate to sensitivity)
4. Log request (date, type, requester, regulation, deadline, handler)
5. Check exemptions (legal claims, legal obligations, public interest, freedom of expression)
6. Gather data across systems
7. Prepare response or denial with legal basis
8. Inform of right to complain to supervisory authority
9. Document request and response

**When this skill activates:**

- DPA review and negotiation
- Data subject request handling
- Privacy compliance questions
- Regulatory requirement questions
- Cross-border data transfer issues

## canned-responses — Template Management and Escalation Detection

**Triggers when discussing:**

- Templated responses, canned responses
- Response templates, template management
- Common legal inquiries
- Template creation, template customization

**Core knowledge:**

**Template organization:**

Each template should include:

1. Category (inquiry type)
2. Template name
3. Use case description
4. Escalation triggers (when NOT to use)
5. Required variables
6. Template body with placeholders

7. Follow-up actions
8. Last reviewed date

**Response categories:**

1. **Data Subject Requests** — Acknowledgment, verification, fulfillment, denial, extension
2. **Discovery Holds** — Initial hold, reminder, modification, release
3. **Privacy Inquiries** — Cookie questions, privacy policy, data sharing, children's data
4. **Vendor Legal Questions** — Status inquiries, amendment requests, compliance certifications
5. **NDA Requests** — Standard form, acceptance with markup, declining, renewal
6. **Subpoena / Legal Process** — Acknowledgment, objection, extension request, compliance cover
7. **Insurance Notifications** — Initial claim, supplemental information

**Escalation triggers (universal):**

- Potential litigation or regulatory investigation
- Inquiry from regulator, government, law enforcement
- Response could create binding commitment or waiver
- Potential criminal liability
- Media attention involved or likely
- Unprecedented situation
- Multiple jurisdictions with conflicting requirements
- Involves executive leadership or board

**Category-specific escalation triggers:**

**DSR triggers:**

- Request from minor or on behalf of minor
- Data subject to litigation hold
- Requester in active dispute with organization
- Employee with active HR matter
- Broad scope (fishing expedition)
- Special category data (health, biometric, genetic)

**Discovery hold triggers:**

- Potential criminal liability
- Unclear or disputed preservation scope
- Conflicts with regulatory deletion requirements

- Prior holds for related matters
- Custodian objects to scope

**Vendor question triggers:**

- Disputing contract terms
- Threatening litigation or termination
- Could affect ongoing negotiation
- Involves regulatory compliance (not just contract interpretation)

**Subpoena triggers:**

- ALWAYS requires counsel review (templates are starting points only)

**Template format:**

```
## Template: [Name]
**Category**: [category]
**Version**: [version] | **Last Reviewed**: [date]

### Use When
- [Condition 1]
- [Condition 2]

### Do NOT Use When (Escalation Triggers)
- [Trigger 1]
- [Trigger 2]

### Variables
| Variable | Description | Example |
|---|---|---|
| {{var1}} | [what it is] | [example] |

### Subject Line
[Template with {{variables}}]

### Body
[Response body with {{variables}}]

### Follow-Up Actions
1. [Action 1]
2. [Action 2]
```

**When escalation trigger detected:**

1. Stop — do not generate templated response
2. Alert user to detected trigger

3. Explain which trigger and why it matters
4. Recommend escalation path
5. Offer draft for counsel review (clearly marked) rather than final response

**When this skill activates:**

- Template response generation
- Template creation or modification
- Questions about when to use templates
- Escalation trigger identification

## legal-risk-assessment — Risk Severity Framework

**Triggers when discussing:**

- Legal risk assessment, risk classification
- Risk scoring, risk levels
- Contract risk, deal exposure
- Escalation criteria, when to escalate

**Core knowledge:**

**Severity x Likelihood matrix:**

**Severity levels (impact if risk materializes):**

1. **Negligible**: Minor inconvenience, no material impact
2. **Low**: Limited impact, <1% of value, minor disruption
3. **Moderate**: Meaningful impact, 1-5% of value, noticeable disruption
4. **High**: Significant impact, 5-25% of value, significant disruption, likely public attention
5. **Critical**: Severe impact, >25% of value, fundamental disruption, regulatory action likely

**Likelihood levels (probability):**

1. **Remote**: Highly unlikely, no precedent, exceptional circumstances required
2. **Unlikely**: Could occur but not expected, limited precedent
3. **Possible**: May occur, some precedent, foreseeable triggers
4. **Likely**: Probably will occur, clear precedent, common triggers
5. **Almost Certain**: Expected to occur, strong pattern, triggers present/imminent

**Risk score = Severity × Likelihood**

| SCORE | RISK LEVEL | COLOR | ACTION |
|---|---|---|---|
| 1-4 | Low | GREEN | Accept, document, monitor quarterly |
| 5-9 | Medium | YELLOW | Mitigate, monitor monthly, assign owner, brief stakeholders |
| 10-15 | High | ORANGE | Escalate to senior counsel, develop mitigation plan, brief leadership, weekly review |
| 16-25 | Critical | RED | Immediate escalation to GC/C-suite/Board, engage outside counsel, establish response team, daily+ review |

**Documentation standards:**

Risk assessment memo should cover:

1. Risk description
2. Background and context
3. Severity assessment with rationale
4. Likelihood assessment with rationale
5. Risk score and level
6. Contributing factors
7. Mitigating factors
8. Mitigation options (with effectiveness, cost, recommendation)
9. Recommended approach
10. Residual risk (post-mitigation)
11. Monitoring plan and trigger events
12. Next steps with owners and deadlines

**When to engage outside counsel:**

Mandatory:

- Active litigation
- Government investigation
- Criminal exposure
- Securities issues
- Board-level matters

Strongly recommended:

- Novel legal issues

- Jurisdictional complexity
- Material financial exposure
- Specialized expertise needed
- Regulatory changes materially affecting business
- Significant M&A transactions

Consider:

- Complex contract disputes
- Employment claims (discrimination, harassment, wrongful termination, whistleblower)
- Potential data breaches with notification obligations
- Material IP disputes
- Insurance coverage disputes

**When this skill activates:**

- Risk assessment and scoring
- Risk classification decisions
- Escalation determinations
- Questions about when to engage outside counsel

## meeting-briefing — Meeting Preparation and Action Tracking

**Triggers when discussing:**

- Meeting preparation, meeting brief
- Board meetings, deal reviews
- Briefing for meetings, meeting prep
- Action items, meeting follow-up

**Core knowledge:**

**Meeting prep methodology:**

1. **Identify meeting context**
    - Title and type
    - Participants and roles
    - Agenda and topics
    - Your role (advisor, presenter, observer, negotiator)
    - Preparation time available

2. **Assess prep needs by meeting type:**

| MEETING TYPE | KEY PREP NEEDS |
|---|---|
| Deal Review | Contract status, open issues, counterparty history, negotiation strategy, approvals |
| Board / Committee | Legal updates, risk highlights, pending matters, regulatory developments, resolutions |
| Vendor Call | Agreement status, open issues, performance, relationship history, objectives |
| Regulatory | Matter background, compliance status, prior communications, counsel briefing, privilege considerations |
| Litigation | Case status, recent developments, strategy, settlement parameters |

3. **Gather context from sources:**
   - Calendar: meeting details, prior meetings, related meetings, conflicts
   - Email: recent correspondence, prior follow-ups, open action items, shared documents
   - Chat: discussions about topic, messages from participants, team discussions
   - Documents: agendas, prior notes, agreements, briefings, shared materials
   - CLM: relevant contracts, status, open items, amendments
   - CRM: account info, relationship history, deal stage, stakeholder map
4. **Synthesize into briefing** with structure:
   - Meeting details
   - Participants table (name, org, role, interests, notes)
   - Agenda / expected topics
   - Background and context
   - Key documents
   - Open issues table
   - Legal considerations
   - Talking points
   - Questions to raise
   - Decisions needed
   - Red lines / non-negotiables (if negotiation)
   - Prior meeting follow-up
5. **Identify preparation gaps** — what couldn't be found, unavailable sources, unanswered questions

**Action item tracking:**

Best practices:

- **Be specific**: "Send redline of Section 4.2 to counterparty" not "Follow up on contract"
- **Assign an owner**: Exactly one owner per item
- **Set deadline**: Specific date, not "soon"
- **Note dependencies**: If item depends on other action or external input
- **Distinguish types**: Legal team actions, business team actions, external actions, follow-up meetings

Tracking cadence:

- High priority: Daily until completed
- Medium priority: At next team sync or weekly
- Low priority: At next scheduled meeting or monthly
- Overdue: Escalate to owner and manager, flag in next meeting

**When this skill activates:**

- Meeting preparation requests
- Questions about briefing meetings
- Action item tracking and follow-up
- Board preparation, deal review preparation

---

# Part V: Workflows and Use Cases

## Workflow 1: Vendor Contract Review from Request to Signature

**Scenario:** Sales team sends a vendor SaaS agreement that needs review before the deal can close.

**Step-by-step:**

1. **Receive request** (via email, Slack, CLM notification)
2. **Run initial review:**

```
/review-contract

[Upload vendor agreement]

Context:
- We are the customer
- Deadline: End of quarter (14 days)
- Focus: Data protection and liability
- Deal: $180K annual SaaS contract
```

3. **Review output** — The plugin produces:
   - Clause-by-clause analysis with GREEN/YELLOW/RED flags
   - 3 RED items (uncapped liability for data breach, no DPA offered, unilateral indemnification)
   - 5 YELLOW items (liability cap at 3 months fees, 30-day auto-renewal notice, vendor-favorable governing law)
   - Specific redline language for all issues
   - Negotiation strategy: lead with RED items, use YELLOW as negotiation chips
4. **Prepare redline** using plugin-generated language:
   - Copy suggested redlines into Word/CLM
   - Prioritize: Must-have (RED items), should-have (top YELLOW items), nice-to-have (remaining YELLOW)
   - Add business context from deal team
5. **Send to counterparty** with cover email:
   - "We've reviewed the agreement. Attached are our proposed redlines."

- "The primary issues relate to data protection requirements and liability allocation."
- "Happy to discuss on a call if that would be helpful."

6. **Receive counterparty response:**
   - Accepted RED items (DPA added, liability capped)
   - Pushed back on mutual indemnification
   - Accepted 2 of 5 YELLOW items
7. **Evaluate remaining issues:**

```
/review-contract

[Upload revised agreement]

Question: Is the remaining unilateral indemnification scope acceptable given they'v
```

8. **Make decision:**
   - Plugin confirms the combination of capped indemnification + limited scope is within YELLOW range
   - Falls within acceptable commercial risk
   - Document the deviation and rationale
9. **Route for approval** (if CLM connected, plugin recommends workflow):
   - Standard approval for contracts <$200K with no RED items
   - Route to Director for sign-off
10. **Signature and storage:**
    - Send to DocuSign (or other e-signature tool)
    - Store executed copy in CLM/document repository
    - Update vendor-check database (if you run `/vendor-check Vendor Name` in future, this agreement appears)

**Time saved:** What would typically take 2-3 hours of manual review reduces to 30-45 minutes with focused attention on actual issues rather than reading every standard clause.

## Workflow 2: NDA Triage for Sales Team

**Scenario:** Business development receives 8 new NDAs from prospects. They need quick screening to determine which require legal review.

**Step-by-step:**

1. **Receive batch request:**
   - Slack message: "Legal team, we have 8 NDAs from new prospects. Can you triage these for us?"
2. **Triage each NDA:**

   **NDA 1:**

   ```
   /triage-nda
   [Upload NDA from Prospect A]
   ```

   - Result: **GREEN** — Mutual, all carveouts present, 3-year term, standard provisions
   - Action: "This is standard. You can sign under delegation of authority. No legal review needed."

   **NDA 2:**

   ```
   /triage-nda
   [Upload NDA from Prospect B]
   ```

   - Result: **YELLOW** — Missing independent development carveout, 5-year term (longer than standard but acceptable), minor jurisdiction issue
   - Action: "Needs quick legal review. I'll add the missing carveout. Should take 15 minutes."

   **NDA 3:**

   ```
   /triage-nda
   [Upload NDA from Prospect C]
   ```

   - Result: **RED** — Unilateral (only we have obligations), contains 12-month non-solicitation clause, overbroad definition
   - Action: "Significant issues. This isn't actually a standard NDA. We need to send our form or heavily redline this. I'll handle directly."

   **NDAs 4-8:** Similar triage process
3. **Summarize results for business team:**

```
Triage complete:
- 4 NDAs: GREEN → You can approve and sign
- 2 NDAs: YELLOW → I'll review and turn around today
- 2 NDAs: RED → I'll handle these directly, will need negotiation

For the GREEN NDAs, I've confirmed they meet our standards.
Please route through your standard NDA approval process.
```

4. **Handle YELLOW NDAs (15 minutes each):**
   - Add missing carveout to NDA 2
   - Revise jurisdiction clause in NDA 5
   - Send to counterparties with brief note
   - Set reminder to follow up in 3 days
5. **Handle RED NDAs (requires deeper engagement):**
   - NDA 3: Send our standard mutual NDA form with note: "Our policy requires mutual NDAs. Attached is our standard form which has been pre-approved by both sides' legal teams at other companies."
   - NDA 7: The embedded non-solicit is a deal-breaker. Escalate to business team: "This NDA includes provisions that extend beyond confidentiality. Before I invest time redlining, please confirm this deal is worth the legal lift."

**Time saved:** 8 NDAs that would traditionally require 4-6 hours of legal review time reduce to 1.5 hours, with 4 routed for immediate signature and 2 handled in parallel.

**Quality improvement:** Consistent screening criteria across all NDAs. Junior business team members get the same quality assessment a senior attorney would provide.

## Workflow 3: Daily Legal Team Standup with AI Brief

**Scenario:** Legal team of 5 starts each day with a standup. Traditionally, each person manually reviews email, CLM, calendar to know what's happening.

**Step-by-step:**

1. **Morning routine (8:45 AM):**

```
/brief daily
```

2. **Review generated brief** (2-3 minutes):

```
## Daily Legal Brief — February 14, 2025

### Urgent / Action Required
- Vendor contract for Acme Corp expires in 7 days (no renewal executed yet)
- Data subject request from EU received yesterday (28-day response deadline)
- Board meeting tomorrow: draft resolutions need review by 5 PM today

### Contract Pipeline
- Awaiting Your Review: 3 contracts
  1. SaaS agreement - CloudVendor ($200K annual)
  2. Professional services - ConsultCo ($85K project)
  3. Partnership agreement - PartnerX (revenue share)
- Pending Counterparty Response: 5 contracts
- Approaching Deadlines: 2 contracts need to close by month-end

### New Requests (Overnight)
- NDA request from Sales for new enterprise prospect
- Privacy team question about CCPA opt-out handling
- Vendor question about amendment to existing MSA

### Calendar Today
- 10:00 AM: Deal review for Q2 partnership
  *Prep needed*: Review partnership agreement draft, know open issues
- 2:00 PM: Vendor call with DataProvider legal
  *Prep needed*: Know current DPA status, understand data processing concerns

### Team Activity
- #legal channel: Compliance team asking about new state privacy law
- DM from CFO: Needs advice on stock option plan amendment

### This Week's Deadlines
- Feb 16: Response to regulatory inquiry due
- Feb 17: Board resolutions finalized
- Feb 18: Partnership agreement target close date
```

3. **Team standup (9:00 AM):**
   - Each person knows their priorities
   - "I'm focused on the Acme renewal and the board resolutions today."
   - "I'll handle the three new contracts in pipeline and the partnership deal review."
   - "I'll take the DSR and the privacy team question."
   - Team can quickly identify gaps and reassign if needed
4. **Follow up on flagged items:**
   - Acme renewal: Immediately email vendor: "Our agreement expires in 7 days. Do you have a renewal ready or should we extend the current agreement?"

- DSR: Run `/respond dsr` to generate acknowledgment
- Board resolutions: Block 2 hours this afternoon to finalize

**Time saved:** 15-20 minutes per person per day (1.5 hours for team of 5) previously spent manually reviewing sources. Information is pre-synthesized and prioritized.

**Quality improvement:** Nothing falls through cracks. The AI brief catches the approaching expiration that might have been missed until it became urgent.

## Workflow 4: Data Breach Incident Response

**Scenario:** 3:00 PM on Friday, you receive notification that a vendor may have experienced unauthorized access to systems containing customer personal data. You need to brief leadership immediately.

**Step-by-step:**

1. **Immediate incident brief:**

```
/brief incident "Vendor DataProvider reported potential unauthorized access to syst
```

2. **Review generated brief** (available in 60 seconds):

```
## Incident Brief: Vendor DataProvider Potential Data Breach
**Prepared**: Feb 14, 2025 15:05
**Classification**: High severity (potential personal data breach)

### Situation Summary
Vendor DataProvider (our CRM data processor) reported at 14:45 today that they
detected unauthorized access to production systems. Investigation ongoing.
Scope not yet determined.

### Timeline
- 14:30: DataProvider security team detected anomalous access
- 14:45: DataProvider notified our security team via email
- 15:00: Security team escalated to legal
- 15:05: This brief prepared

### Immediate Legal Considerations
- **GDPR breach notification**: If personal data compromised, 72-hour clock starts
  when we become "aware" of breach. Awareness = 15:00 today = 72-hour deadline
  is Monday 15:00.
- **CCPA notification**: If California resident data compromised, may trigger
  notification requirements
- **Contractual obligations**: DPA requires DataProvider to notify us "without
  undue delay"
```

```
- **Litigation hold**: Consider preservation hold pending investigation
- **Privilege**: Mark all investigation communications as attorney-client privilege

### Relevant Agreements
- Data Processing Agreement with DataProvider (executed Jan 2024)
  * Section 8: Data Breach Notification - requires notification within 24 hours
  * Section 9: Security Obligations - specifies required safeguards
  * Section 12: Liability - cap at 12 months fees ($500K) with carveout for
    data breaches (uncapped)
- Cyber Insurance Policy with InsureCo (policy #12345)
  * Coverage limit: $5M
  * Notification required within 48 hours of awareness

### Internal Response
[Based on email/chat scan:]
- Security team conducting initial assessment
- CTO notified, preparing to brief CEO
- PR team aware, preparing holding statement
- Customer success team on standby pending decision on customer notification

### Key Contacts
- Internal: CISO (Jane Smith), CTO (Bob Johnson), CEO (Alice Chen)
- External: Outside counsel (Wilson & Partners - data breach response)
- Vendor: DataProvider General Counsel (Tom Wilson, tom@dataprovider.com)
- Insurance: InsureCo Claims (claims@insureco.com, 1-800-INSURE)

### Recommended Immediate Actions
1. **Notify cyber insurance** (within 48-hour window) - URGENT
2. **Engage outside counsel** for breach response (Wilson & Partners has
   retainer) - URGENT
3. **Implement litigation hold** for all employees involved in vendor
   relationship - TODAY
4. **Document timeline** of when we became aware (for 72-hour GDPR clock) - TODAY
5. **Request detailed scope** from DataProvider (what data, how many individuals,
   which jurisdictions) - TODAY
6. **Brief C-suite** on timeline, obligations, and potential exposure - TODAY
7. **Prepare holding statement** for potential regulatory/customer inquiries - TODAY
8. **Review contractual notification obligations** to customers - MONDAY AM

### Information Gaps
- Scope of compromised data (DataProvider investigating)
- Number of affected individuals
- Jurisdictions of affected individuals
- Nature of unauthorized access (exfiltration vs. just access?)
- DataProvider's root cause and remediation plan

### Sources Checked
- Email (DataProvider notification, internal escalation)
- Chat (Slack #security-incidents, #legal channels)
- Documents (DataProvider DPA, cyber insurance policy)
```

```
- CLM (vendor agreement search)

**Sources not available**: DataProvider's investigation details (pending),
customer database (need to query), regulatory guidance specific to this incident
```

3. **Immediate execution** (next 30 minutes):

   **Action 1 - Notify insurance (5 minutes):**

   ```
   /respond insurance

   Incident: Potential data breach at vendor DataProvider
   Policy: #12345
   Date of awareness: Feb 14, 2025 15:00
   ```

   Send generated notification email to InsureCo.

   **Action 2 - Engage outside counsel (5 minutes):** Call Wilson & Partners data breach team: "We have a potential vendor data breach. Need your team activated immediately. Sending details via encrypted email."

   **Action 3 - Litigation hold (10 minutes):**

   ```
   /respond hold

   Matter: DataProvider Security Incident - Feb 2025
   Custodians: All employees who manage DataProvider relationship, security team,
   legal team, executive team
   Scope: All communications with DataProvider, all documents related to data
   processing agreement, all incident response communications
   ```

   **Action 4 - Brief C-suite (10 minutes):** Use the incident brief to prepare 5-minute verbal brief for CEO:

   - "At 3 PM today we were notified of potential unauthorized access at our CRM vendor DataProvider."
   - "We have 72 hours from now to notify regulators if personal data was compromised (GDPR requirement)."
   - "We've notified our cyber insurance and engaged outside counsel."
   - "We've implemented legal hold on all relevant communications."
   - "Next steps: We're awaiting scope details from the vendor. We'll know within 24 hours whether regulatory notification is required."

- "Potential exposure: Regulatory fines if we don't notify properly. Customer notification may be required. Reputational risk."

4. **Follow-up throughout weekend:**
   - Monitor DataProvider investigation
   - Outside counsel advises on notification obligations as scope clarifies
   - Document all steps taken and timeline
   - Prepare draft regulatory notification (if needed)
   - Prepare customer notification (if needed)

**Time saved:** 2-3 hours of manual gathering of context. The incident brief provided everything needed to brief leadership and take immediate actions within minutes of notification.

**Risk reduced:** The brief immediately flagged the 72-hour GDPR clock, the insurance notification deadline, and the litigation hold requirement—any of which could have been missed in the initial chaos without a systematic approach.

## Workflow 5: Board Meeting Preparation

**Scenario:** Quarterly board meeting in 3 days. General Counsel needs to prepare legal update, risk summary, and resolutions for approval.

**Step-by-step:**

1. **Generate board meeting brief** (1 week before meeting):

```
/brief topic "board meeting preparation - legal updates and risk summary for Q1 boa
```

2. **Review brief** — pulls from prior board materials, risk register, CLM, email:

```
## Topic Brief: Q1 Board Meeting - Legal Update

### Summary
Legal update should cover: litigation update (2 active matters), regulatory
developments (new state privacy law), significant contracts (3 closed this
quarter), risk register changes (2 new high risks added, 1 closed).

### Background
Prior board legal updates (from document search):
- Q4 2024: Focused on year-end compliance, new vendor agreements,
  employment matter settlement
- Q3 2024: Emphasized data privacy program enhancements, IP portfolio review
```

```
### Current State
Active matters requiring board awareness:
1. **Litigation**: Vendor dispute with OldVendor ($250K claim); employment
   matter with former employee (settlement discussions ongoing)
2. **Regulatory**: New state privacy law effective July 2025 (requires
   compliance program updates)
3. **Contracts**: Closed 3 significant agreements this quarter (Enterprise
   customer $2M annual, strategic partnership with PartnerCo, new office lease)
4. **Risk Register**: Added HIGH risks: data processing vendor concentration
   (3 critical vendors), trade secret protection gaps in R&D (mitigation plan
   in progress)

### Key Considerations
- Board previously requested quarterly updates on vendor concentration risk
  (this was added to high-risk list this quarter)
- New privacy law may require board committee oversight (recommend discussion)
- Settlement authority for employment matter may need board approval if exceeds
  $100K (currently negotiating in $75-125K range)

### Internal Precedent
- Board legal updates typically 10-15 minutes
- Format: Slide deck with executive summary, then deep dives on material items
- Board prefers metrics: number of contracts, cycle time, legal spend vs. budget

### Recommended Next Steps
1. Prepare slide deck (use Q4 template from Documents)
2. Get litigation update from outside counsel
3. Prepare draft resolution for employment settlement authority (if needed)
4. Coordinate with CFO on legal spend metrics
5. Prepare backup materials (risk register detail, contract summaries)
```

3. **Prepare materials** using brief as outline:

**Slide 1: Executive Summary**

- 2 active litigation matters
- 3 significant contracts closed
- 1 new regulatory requirement
- 2 high risks added to register

**Slide 2: Litigation Update**

- Matter 1: OldVendor dispute (expected resolution timeline, exposure range)
- Matter 2: Employment matter (settlement discussions, board authority may be needed)

**Slide 3: Regulatory Update**

- New state privacy law (effective date, requirements, compliance timeline, budget impact)

**Slide 4: Significant Contracts**

- Enterprise customer $2M annual (strategic importance, key terms)
- PartnerCo partnership (revenue share model, IP considerations)
- Office lease (term, expansion options)

**Slide 5: Risk Register Highlights**

- New HIGH risk: Vendor concentration (context, mitigation plan)
- New HIGH risk: Trade secret protection (gaps identified, remediation underway)
- Closed risk: Prior quarter's contract compliance concern resolved

**Slide 6: Metrics**

- Contracts closed: 47 this quarter (vs. 52 prior quarter)
- Average contract cycle time: 18 days (improved from 24 days)
- Legal spend: $425K (vs. $450K budget)
- Outside counsel spend: $180K (vs. $200K budget)

4. **Prepare resolutions** for board approval:

**Resolution 1: Employment Settlement Authority**

```
RESOLVED, that the officers of the Company are authorized to settle the
employment matter with [Former Employee] for an amount not to exceed $125,000,
on terms acceptable to the General Counsel.
```

**Resolution 2: Privacy Compliance Program**

```
RESOLVED, that the Audit Committee is designated to oversee the Company's
privacy compliance program and receive quarterly reports from the General
Counsel and Chief Privacy Officer regarding compliance with applicable
privacy laws.
```

5. **Circulate for review** (2 days before meeting):
   - Send to CEO for feedback
   - Send to CFO for metrics validation
   - Send to outside counsel for litigation update review
6. **Meeting day prep** (morning of meeting):

```
/brief daily
```

- Check for any overnight developments
- Review talking points
- Prepare for questions

7. **Post-meeting follow-up:**
   - Document board approvals
   - Update risk register with board feedback
   - Action items from board questions
   - File meeting materials

**Time saved:** 4-6 hours of preparation time. The topic brief provided the outline, flagged prior board preferences, and identified all material items requiring inclusion.

---

# Part VI: Customization and Extension

## Understanding Your Customization Options

The legal plugin is designed for customization. Every organization has different contract positions, approval workflows, risk tolerances, and tool integrations. The plugin provides three approaches to customization, each with different trade-offs.

| APPROACH | WHAT YOU CHANGE | DURABILITY | COMPLEXITY | BEST FOR |
|---|---|---|---|---|
| **A: Direct Modification** | Edit plugin files directly | Overwritten by updates | Low | Quick experiments, personal customization |
| **B: Fork the Plugin** | Copy entire plugin, modify copy, install fork | Permanent (until you update fork) | Medium | Team-wide customization, significant changes |
| **C: Complementary Skills** | Add project-level skills via CLAUDE.md | Permanent | Low | Company-specific knowledge, local additions |

**Most organizations use a combination:** Approach C for company-specific knowledge (templates, approval workflows, team structures), plus light Approach A for testing new features.

## Approach A: Direct Modification (Quick Experiments)

Edit plugin files in place to add content, modify workflows, or tweak positions.

**Example: Adding industry-specific compliance to the compliance skill**

Location: `/path/to/legal/1.0.0/skills/compliance/SKILL.md`

Add a new section:

```
## Healthcare Compliance (HIPAA)

### Scope
Applies to covered entities (healthcare providers, health plans, healthcare
clearinghouses) and business associates that create, receive, maintain, or
transmit protected health information (PHI).

### Key Obligations for In-House Legal
- **Business Associate Agreements (BAAs)**: Required for any third party that
  handles PHI on behalf of covered entity
- **Minimum necessary**: Limit use/disclosure of PHI to minimum necessary
- **Breach notification**: Notify HHS and affected individuals within 60 days
  of discovery
- **Security Rule**: Administrative, physical, and technical safeguards
- **Privacy Rule**: Individual rights to access, amendment, accounting

### BAA Review Checklist
Required elements:
- [ ] Describes permitted uses and disclosures of PHI
- [ ] Prohibits use or disclosure except as permitted or required
- [ ] Requires appropriate safeguards
- [ ] Requires business associate to report breaches and security incidents
- [ ] Requires business associate to ensure any subcontractors have BAAs
- [ ] Allows covered entity to audit and access books/records
- [ ] Requires return or destruction of PHI at termination
- [ ] Authorizes covered entity to terminate if BA violates material term

### Common BAA Issues
| Issue | Risk | Standard Position |
|-------|------|-------------------|
| No subcontractor BAA requirement | BA could share PHI without safeguards | Require BA
| Unclear breach definition | May not learn of breaches timely | Use federal breach de
| No audit rights | Cannot verify HIPAA compliance | Require audit rights or accept an
```

**Result:** The compliance skill now includes HIPAA knowledge. When you discuss BAAs or healthcare compliance, this content loads automatically.

**Caution:** Next time the plugin updates, this addition may be overwritten. Document what you added so you can re-apply if needed.

## Approach B: Fork the Plugin (Team-Wide Customization)

Create a customized version of the plugin for your organization.

**Example: Creating "legal-pharma" for pharmaceutical company**

**Step 1: Copy the plugin**

```
cp -r /path/to/legal/1.0.0 /path/to/legal-pharma/1.0.0
```

### Step 2: Update plugin.json

Edit `.claude-plugin/plugin.json`:

```
{
  "name": "legal-pharma",
  "version": "1.0.0",
  "description": "Legal productivity plugin adapted for pharmaceutical and life scienc
  "author": {
    "name": "YourCompany Legal Team"
  }
}
```

### Step 3: Add pharma-specific command

Create `commands/mlr-review.md`:

```
---
description: Review promotional materials for medical-legal-regulatory (MLR) complianc
argument-hint: "<promotional material file or text>"
---

# /mlr-review — Medical-Legal-Regulatory Review

Review promotional materials for compliance with FDA regulations on pharmaceutical mar

## Inputs

Accept promotional material in any format:
- File upload (PDF, DOCX, image)
- URL to material in document system
- Pasted copy

Ask for context:
1. **Material type** — sales aid, website content, email, display ad, video, journal a
2. **Audience** — HCP (physician, pharmacist, nurse) or DTC (patient)?
3. **Product** — which pharmaceutical product is this for?
4. **Claims** — what efficacy or safety claims are made?

## Review Process

### Step 1: Material Classification

Classify the material:
```

```
- **Branded promotional**: Names product, makes claims → Full MLR review required
- **Unbranded disease awareness**: Discusses condition, no product → Medical/legal rev
- **Reminder advertising**: Product name only, no claims → Abbreviated review
- **Scientific exchange**: Peer-to-peer, balanced data → Medical review

### Step 2: Fair Balance Check

For branded promotional materials, verify:
- [ ] **Efficacy claims supported**: Every claim has cited clinical data reference
- [ ] **Risk information prominence**: Side effects, contraindications, warnings
      presented with equal prominence to efficacy
- [ ] **Indication statement accurate**: Matches approved prescribing information exac
- [ ] **No off-label claims**: No explicit or implied claims for unapproved indication
- [ ] **Black box warnings**: If applicable, prominently displayed
- [ ] **Brief summary**: Included for print materials (or accessible for digital)

### Step 3: Regulatory Requirements

Check for required elements based on material type:
- Indication statement
- Brief summary (print) or link to full prescribing information (digital)
- Copyright and trademark notices
- "See full prescribing information" language
- Reference citations for all claims
- Adverse event reporting contact information

### Step 4: Prohibited Content

Flag if present:
- Off-label uses or implications
- Comparative claims without head-to-head data
- Minimization of risks
- Unsubstantiated superiority claims
- Patient testimonials without proper disclosures
- Manipulated or misleading data presentation

### Step 5: Generate Review

Output structured review:

\`\`\`
## MLR Review: [Material Name]

**Material Type**: [classification]
**Audience**: [HCP/DTC]
**Product**: [name]
**Reviewer**: [your name]
**Date**: [today]

### Fair Balance Assessment: [PASS / FAIL]
```

```
[Details of fair balance evaluation]

### Required Elements: [COMPLETE / INCOMPLETE]
- Indication statement: [PRESENT / MISSING / INCORRECT]
- Brief summary: [PRESENT / MISSING / NOT REQUIRED]
- Citations: [PRESENT / INCOMPLETE]
[etc.]

### Prohibited Content: [NONE / ISSUES FOUND]
[Details if issues found]

### Issues Requiring Correction

#### RED — Must Fix Before Approval
[Critical issues that prevent approval]

#### YELLOW — Should Fix
[Issues that should be addressed but don't prevent approval if business determines]

### Recommendations
[Specific suggested corrections]

### Approval Status: [APPROVED / APPROVED WITH CHANGES / REJECTED]
\`\`\`

## Notes

- All promotional materials require three-way sign-off: Medical, Legal, Regulatory
- This review covers legal considerations; medical and regulatory review still require
- Maintain copies of approved materials and review documentation per retention require
```

### Step 4: Add pharma-specific skill

Create `skills/clinical-trial-agreements/SKILL.md`:

```
---
name: clinical-trial-agreements
description: >
  Clinical trial agreement review and negotiation for pharmaceutical companies.
  Use when reviewing investigator agreements, CRO contracts, site agreements,
  or consulting agreements with clinical investigators. Includes publication
  rights, data ownership, regulatory compliance, and investigator obligations.
---

# Clinical Trial Agreements Skill

## Agreement Types
```

```
| Agreement Type | Purpose | Key Parties | Critical Terms |
|---|---|---|---|
| **Clinical Trial Agreement (CTA)** | Site conducts trial per protocol | Sponsor, Sit
| **CRO Agreement** | CRO manages trial on sponsor's behalf | Sponsor, CRO | SOW, moni
| **PI Consulting Agreement** | PI provides advisory services | Sponsor, PI | Scope, f
| **Data Transfer Agreement** | Transfer of clinical data | Data provider, Recipient |

## CTA Key Terms Review

### Budget and Payment
- [ ] Budget attached as exhibit, itemized by visit/procedure
- [ ] Payment triggered by completed, evaluable visits (not just enrollment)
- [ ] Indirect costs/overhead reasonable (typically 20-30%)
- [ ] Expense reimbursement process defined
- [ ] Audit rights reserved for sponsor

### Regulatory and Compliance
- [ ] Site commits to conduct per protocol, GCP, regulations
- [ ] IRB/IEC approval required before initiation
- [ ] Site commits to timely SAE and protocol deviation reporting
- [ ] Site permits regulatory inspections and sponsor audits
- [ ] Site maintains essential documents per ICH GCP

### Data Ownership and Use
- [ ] Sponsor owns all clinical trial data
- [ ] Site grants sponsor rights to use data for regulatory submissions
- [ ] Site retains medical records per regulations
- [ ] De-identification requirements if data shared

### Publication Rights
- [ ] Sponsor has publication review rights (typically 30-60 days)
- [ ] Sponsor can delay publication for patent filing (typically 60-90 days)
- [ ] Sponsor can require redaction of confidential information
- [ ] Multi-site trials: Coordinated publication approach
- [ ] PI academic freedom balanced with sponsor confidentiality

### Indemnification
- [ ] Sponsor indemnifies site for product-related injuries
- [ ] Site indemnifies sponsor for site negligence/misconduct
- [ ] Clear allocation of liability for protocol vs. non-protocol care
- [ ] Insurance requirements specified

### Termination
- [ ] Either party can terminate for cause
- [ ] Sponsor can terminate without cause (with notice and wind-down costs)
- [ ] Patient care continuation addressed
- [ ] Data and IP provisions survive termination

## Red Flags in CTAs
```

```
| Red Flag | Why It Matters | Standard Position |
|---|---|---|
| Site owns clinical data | Sponsor needs data for regulatory submissions | Sponsor mu
| Unrestricted publication by PI before trial complete | Could compromise trial or rev
| Site controls protocol amendments | Sponsor is responsible to regulators for protoco
| No audit rights for sponsor | Cannot verify data integrity and GCP compliance | Spon
| PI can delegate to anyone | Unqualified personnel performing trial procedures | Dele

## Fair Market Value and Anti-Kickback

When reviewing PI compensation:
- Compensation must be for legitimate services
- Amount must be consistent with fair market value
- No payment per patient enrolled (AKS concern)
- Payment for time and effort, not outcomes
- Documented methodology for FMV determination
- Disclosure requirements for PI conflicts of interest

All PI payments should be reviewed by compliance for AKS and Sunshine Act implications
```

### Step 5: Update CONNECTORS.md

Add pharma-specific tool categories:

```
## Connectors for this plugin

| Category | Placeholder | Included servers | Other options |
|---|---|---|---|
| Chat | `~~chat` | Slack | Microsoft Teams |
| Cloud storage | `~~cloud storage` | Box, Egnyte | SharePoint, Veeva Vault |
| CLM | `~~CLM` | — | Ironclad, Agiloft |
| CRM | `~~CRM` | — | Salesforce, Veeva CRM |
| Clinical trial management | `~~CTMS` | — | Veeva CTMS, Medidata |
| Document management | `~~DMS` | — | Veeva Vault, Documentum |
| MLR workflow | `~~MLR` | — | Veeva PromoMats, Zinc |
```

### Step 6: Package and distribute

```
cd /path/to/legal-pharma/1.0.0
zip -r /tmp/legal-pharma.plugin . -x "*.DS_Store"
```

Distribute `legal-pharma.plugin` to your legal team. When they install it, they get all pharma customizations.

**Maintenance:** When the original legal plugin updates, review changes and merge relevant updates into your fork.

## Approach C: Complementary Skills via CLAUDE.md (Lightest Touch)

Add company-specific knowledge without touching the plugin.

**Example: Adding company approval workflow and templates**

**Step 1: Create project-level skill**

Create `.claude/skills/acme-legal-processes/SKILL.md`:

```
---
name: acme-legal-processes
description: >
  Acme Corporation legal department processes, approval workflows, and
  response templates. Use when determining approval requirements at Acme,
  routing contracts for review, understanding escalation paths, or generating
  responses to common legal inquiries at Acme Corp.
---

# Acme Corp Legal Processes

## Contract Approval Matrix

| Contract Type | Value | Approver | Turnaround SLA |
|---|---|---|---|
| NDA | Any | Legal Ops (delegation) | Same day |
| Vendor SaaS | < $25K | Commercial Counsel | 3 business days |
| Vendor SaaS | $25K-$100K | Senior Counsel | 5 business days |
| Vendor SaaS | > $100K | Associate GC + Procurement | 7 business days |
| Customer Agreement | < $50K | Commercial Counsel | 3 business days |
| Customer Agreement | $50K-$250K | Senior Counsel | 5 business days |
| Customer Agreement | > $250K | Associate GC + Sales VP | 7 business days |
| Partnership / Strategic | Any | GC + Business Lead + CEO | 10 business days |

## Standard Contract Positions (Acme Corp Playbook)

### Limitation of Liability
- **Standard (Acme as Customer)**: Mutual cap at 12 months fees; carveouts for IP infr
- **Standard (Acme as Vendor)**: Cap at 12 months fees paid/payable; carveouts for IP
- **Escalation trigger**: Uncapped liability, cap below 6 months fees, asymmetric carv

### Data Protection
- **Standard**: Require DPA for any processing of personal data (customer, employee, o
- **DPA musts**: Sub-processor notification rights, 24-hour breach notification, SCCs
- **Escalation trigger**: Vendor refuses DPA, processes data in China/Russia without e
```

```
### Governing Law
- **Preferred**: Delaware (Acme is incorporated in Delaware)
- **Acceptable**: New York, California, England & Wales, Singapore
- **Escalation trigger**: Mandatory arbitration in unfavorable venue, unusual jurisdic

## Legal Team Structure

- **General Counsel**: Sarah Johnson (sarah.johnson@acme.com)
  - Approves: All > $250K, all strategic deals, all litigation, board matters
  - Slack: @sarah.johnson

- **Associate General Counsel**: Michael Chen (michael.chen@acme.com)
  - Oversees: Commercial, product, compliance teams
  - Approves: $100K-$250K contracts, significant compliance matters
  - Slack: @michael.chen

- **Senior Counsel, Commercial**: Emily Davis (emily.davis@acme.com)
  - Focus: Vendor contracts, procurement, partnerships
  - Approves: $25K-$100K vendor contracts
  - Slack: @emily.davis

- **Commercial Counsel**: Robert Martinez (robert.martinez@acme.com)
  - Focus: Customer agreements, sales enablement
  - Approves: < $50K customer agreements
  - Slack: @robert.martinez

- **Legal Ops Manager**: Jennifer Kim (jennifer.kim@acme.com)
  - Focus: Process, templates, CLM administration, NDA triage
  - Slack: @jennifer.kim

## Response Templates (Acme Corp)

### Data Subject Request Acknowledgment

Subject: Your Data Request - Reference {{request_id}}

Dear {{requester_name}},

We received your request dated {{request_date}} to {{request_type}} your personal
data under {{regulation}}.

We are processing your request and will respond by {{response_deadline}}. If we
need additional information to verify your identity or locate your data, we will
contact you.

If you have questions, please reply to this email with your request reference
number: {{request_id}}.

Sincerely,
```

```
Acme Corp Privacy Team
privacy@acme.com

### Litigation Hold Notice

[PRIVILEGED AND CONFIDENTIAL - ATTORNEY-CLIENT COMMUNICATION]

TO: {{custodian_name}}
FROM: Acme Corp Legal Department
DATE: {{date}}
RE: LEGAL HOLD NOTICE - {{matter_name}}

You are receiving this notice because you may possess documents, communications,
or data relevant to {{matter_description}}.

IMMEDIATE ACTION REQUIRED: You must preserve all documents and electronically
stored information related to {{matter_scope}} from {{start_date}} to present.

DO NOT delete, destroy, modify, or discard any potentially relevant materials,
including:
- Email (Acme email and personal email if used for work)
- Documents (local computer, shared drives, cloud storage)
- Chat messages (Slack, Teams, any messaging)
- Calendar entries
- Text messages (if business-related)

This hold remains in effect until you receive written notice from Legal that it
has been released.

Please acknowledge receipt of this notice by {{acknowledgment_deadline}} by
replying to legal.holds@acme.com with "ACKNOWLEDGED" and the matter name.

Questions? Contact {{legal_contact}} at {{contact_email}}.
```

### Step 2: Add routing rules in CLAUDE.md

Edit your project's `CLAUDE.md`:

```
## Acme Corp Legal Department Integration

When working on legal matters for Acme Corporation:

1. **Apply Acme processes**: Always consult the acme-legal-processes skill for
   approval requirements, escalation paths, and team structure.

2. **Contract approval routing**: When reviewing a contract, determine the
   approval path based on the Acme contract approval matrix (contract type
   and value). Include the specific approver name and turnaround SLA in your
   recommendations.

3. **Use Acme playbook**: When the legal plugin loads a generic playbook,
   supplement it with Acme-specific positions from the acme-legal-processes
   skill (limitation of liability, data protection, governing law).

4. **Use Acme templates**: When generating responses via the /respond command,
   use Acme Corp response templates from the acme-legal-processes skill rather
   than generic templates.

5. **Route to specific people**: When recommending escalation or routing,
   provide the specific Acme team member's name and Slack handle from the
   legal team structure.
```

**Result:** The legal plugin works unchanged, but now incorporates Acme-specific workflows, positions, and templates. When the plugin updates, your Acme customizations remain intact.

## Choosing the Right Approach

| SCENARIO | RECOMMENDED APPROACH |
|---|---|
| Testing a new clause analysis for one contract | A (Direct Modification) |
| Adding industry-specific compliance to your team's workflow | B (Fork) |
| Documenting your company's approval process | C (CLAUDE.md + complementary skill) |
| Creating pharma-specific version for distribution | B (Fork with new name) |
| Adding your response templates | C (CLAUDE.md + complementary skill) |
| Substantially changing contract review methodology | B (Fork) |

| SCENARIO | RECOMMENDED APPROACH |
| --- | --- |
| Adding knowledge about your company's legal team structure | C (CLAUDE.md + complementary skill) |

**Most organizations use C for company-specific knowledge** (it's durable and low-risk), occasionally use A for quick tests, and reserve B for significant customizations they want to distribute to their entire team.

---

# Part VII: Advanced Topics

## Integrating with Your CLM System

Contract Lifecycle Management (CLM) integration transforms the legal plugin from a review tool into an end-to-end workflow automation system.

**What CLM integration enables:**

- **Automatic contract ingestion**: Plugin pulls contracts directly from CLM for review
- **Workflow routing**: Plugin recommends approval path based on contract type and risk
- **Status tracking**: Plugin knows what stage each contract is in
- **Metadata extraction**: Plugin can pre-fill contract details (parties, value, effective dates)
- **Post-review actions**: Plugin can move contracts to next stage or assign to reviewers

**Pre-configured CLM options:**

The plugin does not pre-configure specific CLM systems (unlike Slack or Box). You must configure your CLM connection manually.

**Common CLMs with MCP servers:**

- **Ironclad**: HTTP MCP server (check Ironclad documentation for endpoint)
- **Agiloft**: HTTP MCP server (requires API configuration)
- **DocuSign CLM**: HTTP MCP server (OAuth flow)
- **Concord**: HTTP MCP server
- **LinkSquares**: HTTP MCP server

**Configuration example (Ironclad):**

Edit `.mcp.json` in the plugin directory:

```
{
  "mcpServers": {
    "slack": { "type": "http", "url": "https://mcp.slack.com/mcp" },
    "box": { "type": "http", "url": "https://mcp.box.com" },
    "ironclad": {
      "type": "http",
      "url": "https://api.ironcladapp.com/mcp",
      "headers": {
        "Authorization": "Bearer ${IRONCLAD_API_TOKEN}"
      }
    }
  }
}
```

Set environment variable:

```
export IRONCLAD_API_TOKEN="your_token_here"
```

**Workflow enhancement with CLM:**

Before CLM integration:

```
/review-contract
[Upload file manually]
[Review output]
[Manually email stakeholders]
[Manually update CLM]
```

After CLM integration:

```
/review-contract

[Plugin asks: "I see 3 contracts awaiting legal review in Ironclad. Which one?"]
[You select: "Vendor Agreement - Acme Corp"]
[Plugin pulls contract, parties, value, owner automatically]
[Review output includes]: "Recommended routing: Commercial Counsel approval
(contract value $45K falls in their delegation). I can move this to 'Legal
Approved' stage and assign to Sarah for signature. Proceed?"
```

**Customizing CLM workflows:**

Add CLM-specific instructions to your playbook ( `.claude/legal.local.md` ):

```
## CLM Workflow Routing (Ironclad)

After contract review, route based on risk classification:

| Risk Level | Ironclad Workflow | Assignee |
|---|---|---|
| GREEN (all GREEN, no YELLOW or RED) | Move to "Legal Approved" | Return to business
| YELLOW (one or more YELLOW, no RED) | Move to "Redlines Needed" | Assign to appropri
| RED (one or more RED) | Move to "Senior Review Required" | Assign to Associate GC |

Contract type to counsel assignment:
- Vendor/procurement contracts → Emily Davis (emily.davis@acme.com)
- Customer agreements → Robert Martinez (robert.martinez@acme.com)
- Partnerships → Michael Chen (michael.chen@acme.com)
```

The legal plugin's `contract-review` skill will incorporate these routing rules when connected to Ironclad.

## Building a Legal Knowledge Base with Skills

As your team uses the legal plugin, you'll identify recurring questions, patterns, and organizational knowledge that should be captured. Skills are the mechanism for codifying this knowledge.

**Example: Creating a "precedent-analysis" skill for your team**

**Step 1: Identify the knowledge domain**

Your team frequently answers questions like:

- "Have we ever agreed to unlimited liability?"
- "What's our position on IP ownership in professional services agreements?"
- "How have we handled force majeure in prior vendor contracts?"

This knowledge should be a skill: **precedent-analysis**.

**Step 2: Create the skill structure**

```
.claude/skills/precedent-analysis/
├── SKILL.md
├── references/
│   ├── limitation-of-liability-precedents.md
│   ├── ip-ownership-precedents.md
│   └── data-protection-precedents.md
└── examples/
    ├── vendor-agreement-redlines-2024.md
    └── customer-agreement-positions-2024.md
```

### Step 3: Write SKILL.md

```
---
name: precedent-analysis
description: >
  Acme Corp legal precedent and prior positions on contract terms. Use when
  researching how Acme has handled specific contract issues previously,
  understanding the organization's negotiation history, finding prior redline
  language, or determining consistency with past positions.
---

# Precedent Analysis Skill

## How to Use Organizational Precedent

When analyzing a contract term:
1. Check if Acme has addressed this issue before (see references/)
2. Identify the pattern in prior positions
3. Note any context that made prior positions different
4. Apply consistent reasoning to current situation

## Precedent Database Structure

Precedents are organized by clause type in `references/`:
- **limitation-of-liability-precedents.md**: Liability caps, carveouts, and exceptions
- **ip-ownership-precedents.md**: IP allocation, work-for-hire, license grants
- **data-protection-precedents.md**: DPA terms, sub-processors, breach notification

Each precedent includes:
- **Situation**: Contract type, counterparty, year
- **Issue**: Specific term or clause in question
- **Position taken**: What Acme agreed to (or walked away from)
- **Rationale**: Why that position was appropriate
- **Outcome**: Whether the deal closed, lessons learned

## When Precedent Applies vs. Distinguishing
```

```
**Apply precedent when:**
- Contract type is similar (vendor SaaS to vendor SaaS)
- Business context is comparable (similar deal size, criticality)
- No material facts distinguish the situations

**Distinguish precedent when:**
- Business need has changed (prior contract was pre-product launch; now at scale)
- Risk profile is different (prior vendor was non-critical; current is mission-critica
- Market conditions evolved (prior deal was 2020; market norms have shifted)
- Different regulations now apply (GDPR wasn't in effect for prior deal)

Always note when you're distinguishing precedent and explain why.

## Creating New Precedent

After each significant negotiation, document the precedent:
1. Add entry to appropriate reference file
2. Include all fields: situation, issue, position, rationale, outcome
3. Note any distinguishing facts or unique circumstances
4. Update precedent if organizational position changes

This ensures future team members benefit from accumulated experience.
```

### Step 4: Populate references with actual precedents

`references/limitation-of-liability-precedents.md`:

```
# Limitation of Liability Precedents

## Precedent: Vendor SaaS - CloudVendor (2024)

**Situation**: Vendor SaaS agreement, $180K annual, customer data processing, Q1 2024

**Issue**: Vendor proposed cap at 3 months fees ($45K); we requested 12 months ($180K)

**Position taken**: Agreed to 6 months fees ($90K) with explicit carveout for data bre

**Rationale**:
- 6 months was within acceptable range (we accept 6-24 months)
- Data breach carveout was critical given they process customer personal data
- Deal needed to close by quarter-end; 6 months was vendor's maximum
- Business confirmed $90K cap was acceptable risk for this vendor

**Outcome**: Deal closed. Documented as acceptable deviation from 12-month standard.

**Lessons**: For vendors processing sensitive data, the breach carveout is more import

---
```

```
## Precedent: Customer Agreement - Enterprise Corp (2023)

**Situation**: Customer agreement, $2M annual, our SaaS product, Q4 2023

**Issue**: Customer (Fortune 500) requested uncapped liability

**Position taken**: Declined uncapped; agreed to cap at 24 months fees ($4M) with carv

**Rationale**:
- We never agree to uncapped liability (deal-breaker)
- 24 months is our maximum (2x standard)
- Customer accepted after we explained: (1) we carry insurance to that level, (2) unli
- Carveouts were mutual (customer wanted same protections)

**Outcome**: Deal closed with 24-month cap. Set precedent for other enterprise deals.

**Lessons**: Fortune 500 customers often request uncapped liability as a starting posi

---

## Precedent: Vendor SaaS - Dataprocessor Inc (2022) - WALKED AWAY

**Situation**: Vendor SaaS, $250K annual, would process all customer personal data, Q2

**Issue**: Vendor refused any cap on liability (wanted unlimited exposure on both side

**Position taken**: Walked away from deal

**Rationale**:
- Uncapped liability violates company policy (exceeds GC approval authority)
- Vendor was unwilling to negotiate (said "unlimited is our standard")
- Business found alternative vendor (Competitor Co) with standard terms

**Outcome**: Did not sign. Business proceeded with Competitor Co.

**Lessons**: Some vendors (especially smaller ones without enterprise experience) are
```

### Step 5: Use the skill

Now when reviewing contracts:

```
/review-contract

[Upload vendor SaaS agreement with 3-month liability cap]

Context:
- We are customer
- $150K annual
- They process customer personal data

[Plugin generates review including]:

"Limitation of Liability: YELLOW

Current language: Cap at 3 months fees paid ($37.5K)

Playbook position: 12 months fees

Precedent: In CloudVendor deal (2024), we accepted 6 months fees with uncapped
data breach carveout for a similar vendor processing customer data. That deal
was $180K annual; this is $150K.

Recommendation: Negotiate to 6 months fees ($75K) with explicit uncapped carveout
for data breaches and confidentiality breaches. This aligns with our CloudVendor
precedent and falls within acceptable range.

Fallback: If vendor refuses 6 months, we have accepted 3 months in the past when
the breach carveout is strong and deal value is under $200K. Ensure carveout
language is explicit and mutual."
```

The precedent analysis skill ensures consistency across your legal team and preserves institutional knowledge as team members change.

## Advanced Risk Assessment and Quantification

The legal-risk-assessment skill provides qualitative risk scoring (severity × likelihood). For sophisticated legal teams, you can extend this to quantitative risk analysis.

**Example: Creating a "quantitative-risk" complementary skill**

`.claude/skills/quantitative-legal-risk/SKILL.md`:

```
---
name: quantitative-legal-risk
description: >
  Quantitative legal risk assessment and expected value calculations for contract
  risks, litigation exposure, and compliance risks. Use when the legal team needs
```

```
  to quantify exposure in dollar terms, calculate expected value of litigation,
  perform cost-benefit analysis of legal positions, or present financial risk to
  business stakeholders.
---

# Quantitative Legal Risk Assessment

## Expected Value Framework

For quantifiable legal risks, calculate Expected Value (EV):

**EV = Probability × Impact**

**Example: Litigation Risk**
- Probability of losing: 30%
- Impact if we lose: $500K judgment + $200K legal fees = $700K
- EV = 0.30 × $700K = $210K

This means the expected cost of this litigation is $210K, which can be compared to set

## Decision Matrix for Settlement vs. Litigation

| Factor | Settlement | Litigation |
|---|---|---|
| **Expected cost** | Settlement amount | EV of judgment + legal fees to verdict |
| **Certainty** | Known (100% probability of cost) | Uncertain (probability-weighted)
| **Timeline** | Immediate or near-term | Extended (months to years) |
| **Collateral impact** | Minimal | Discovery burden, management time, reputational ri

**Decision rule**: Settle if settlement < (EV of litigation + collateral costs), unles

**Example calculation:**

Settlement offer: $150K
EV of litigation: $210K (calculated above)
Legal fees to trial: $300K total (already incurred $100K, $200K more to verdict)
Collateral costs: Executive time ($50K), reputational risk (hard to quantify)

Expected cost of litigation = $210K (EV) + $200K (future legal fees) + $50K (collatera
Settlement cost = $150K

Recommendation: Settle. Expected savings = $460K - $150K = $310K.

## Contract Risk Quantification

When reviewing contracts, quantify exposure where possible:

**Limitation of Liability Cap**
- Annual contract value: $100K
- Proposed cap: 3 months fees ($25K)
```

```
- Our standard: 12 months fees ($100K)
- Gap in coverage: $75K
- Probability of claim: 5% (based on vendor type and our history)
- Expected incremental risk: 0.05 × $75K = $3,750

Question for business: Is this vendor relationship worth an incremental $3,750 in expe

**Indemnification Uncapped**
- If we agree to uncapped indemnification for IP infringement:
- Assume worst-case: Major IP claim at $2M
- Probability based on vendor's IP risk profile: 2%
- Expected exposure: 0.02 × $2M = $40K
- Our standard (capped at $100K) expected exposure: 0.02 × $100K = $2K
- Incremental risk: $38K

## Compliance Risk Quantification

**Regulatory Fine Risk**

Example: GDPR breach notification failure
- Potential fine: Up to 4% of global revenue (€20M for Acme Corp)
- Probability of fine if violation: 80% (GDPR enforcement is active)
- Likely fine (not maximum): €500K (based on comparable cases)
- Probability of violation: 10% (based on controls)
- Expected cost: 0.10 × 0.80 × €500K = €40K annually

This €40K expected cost justifies €40K annual investment in compliance controls.

## Cost-Benefit of Legal Positions

When deciding whether to negotiate a term:

**Negotiation decision framework:**

Cost of negotiation:
- Legal time: 3 hours @ $300/hour = $900
- Delay in deal: 1 week = potential revenue delay
- Risk of losing deal: 10% × deal value

Benefit of negotiation:
- Reduction in expected risk (calculate EV improvement)
- Strategic value (precedent for future deals)

**Example: Should we negotiate the 3-month liability cap to 12 months?**

Cost of negotiation:
- Legal time: 2 hours @ $300/hour = $600
- Delay: 3 days (no material revenue impact)
- Risk of losing deal: 5% × $100K annual value = $5K expected cost
- Total expected cost: $5,600
```

```
Benefit of negotiation:
- EV improvement: From $3,750 to $937 expected exposure = $2,813 reduction in risk
- Precedent value: If we always accept 3-month caps, it becomes our de facto standard

Decision: Negotiate. Even if we only value risk reduction ($2,813 benefit vs. $5,600 c

## Presenting Quantitative Risk to Business Stakeholders

When presenting contract risks to non-legal business stakeholders, use expected value:

**Instead of**: "This contract has a YELLOW risk level due to the low liability cap."

**Say**: "This contract caps our recovery at $25K if the vendor breaches. Our standard

This quantification helps business stakeholders make informed decisions and understand
```

**Using quantitative risk in contract review:**

After creating this skill, add to your `CLAUDE.md`:

```
## Quantitative Risk Analysis

When reviewing contracts for Acme Corp, supplement qualitative risk assessment
(GREEN/YELLOW/RED) with quantitative analysis from the quantitative-legal-risk
skill when:

1. Business stakeholders need to understand financial exposure
2. Deciding whether to negotiate a term (cost-benefit analysis)
3. Evaluating settlement offers in litigation
4. Prioritizing compliance investments

Present both qualitative (YELLOW) and quantitative (expected $X,XXX exposure)
assessments for material risks.
```

Now contract reviews include both:

- Qualitative: "YELLOW — Liability cap below standard"
- Quantitative: "Expected incremental risk: $3,750 based on 5% claim probability and $75K gap"

This gives business stakeholders the information they need to make economically rational decisions about legal risk.

---

**End of Legal Plugin Handbook**

# Appendix: Quick Reference

## Command Invocation Quick Reference

| COMMAND | SYNTAX | PRIMARY USE |
|---|---|---|
| `/review-contract` | `/review-contract` | Clause-by-clause contract analysis against playbook |
| `/triage-nda` | `/triage-nda` | Rapid NDA screening and classification |
| `/vendor-check` | `/vendor-check [vendor name]` | Check existing agreements with vendor |
| `/brief daily` | `/brief daily` | Morning brief of legal-relevant items |
| `/brief topic` | `/brief topic [query]` | Research brief on specific legal question |
| `/brief incident` | `/brief incident [topic]` | Rapid brief for developing situation |
| `/respond` | `/respond [inquiry-type]` | Generate templated response |

## Risk Classification Quick Reference

| LEVEL | SCORE | COLOR | ACTION |
|---|---|---|---|
| Low | 1-4 | GREEN | Accept, document, monitor quarterly |
| Medium | 5-9 | YELLOW | Mitigate, monitor monthly, assign owner |
| High | 10-15 | ORANGE | Escalate to senior counsel, develop plan |
| Critical | 16-25 | RED | Immediate escalation, engage outside counsel |

## Files Analyzed Summary

**AGENT_REPORT_START** Plugin: legal Version: 1.0.0 Files analyzed: 18

- plugin.json (1)
- Commands (5): review-contract.md, triage-nda.md, vendor-check.md, brief.md, respond.md
- Skills (6): contract-review/SKILL.md, nda-triage/SKILL.md, compliance/SKILL.md, canned-responses/SKILL.md, legal-risk-assessment/SKILL.md, meeting-briefing/SKILL.md

- Configuration (3): .mcp.json, CONNECTORS.md, README.md
- Reference material (3): 00-plugin-development-guide.md, CLAUDE.md, project structure

Handbook word count: ~18,500 words Start time: 1771068399 End time: 1771068435 Estimated token usage: ~70,000 tokens **AGENT_REPORT_END**

# RationalEyes.ai

contact@rationaleyes.ai

Intelligent Automation for Knowledge Work

The Legal Productivity Plugin Handbook — Version 1.0.0