

IT Automation & AI Tooling

Every agent, integration and automated workflow built for the IT Operations team this year — what each one does, how it works, and where it runs.

Adam Schembri
Systems Engineer

20 August 2026
Internal use only

Hillspire/SysEngineering
source of record

15

AGENTS & TOOLS

6

SCHEDULED JOBS

3CLOUD RUN
SERVICES**21**

WORKSPACE ORGS

462

COMMITTS

32

MERGED PRS

SYSTEMS OF RECORD

Okta

Google Workspace

TriNet HR export

GoDaddy · RDAP

Vendor status feeds

Slack Enterprise Grid

THE TOOLING LAYER

AI assistant · Slack, agentic, read-only

Service desk · Slack modal + queued worker

Scheduled jobs · 5 unattended workflows

Identity engineering · on-demand, dry-run first

Shared libraries · secrets, HTTP, reporting

Guardrails · fail-closed, audited, idempotent

WHERE IT LANDS

Slack answers + alerts

Confluence (IPO space)

JSM Assets + tickets

BigQuery audit dataset

Okta profile writes

PDF / HTML reports

Everything reads from a system of record, and everything writes somewhere a person actually looks.

LIVE

Running in production today

COMPLETE

A finished job — kept for the record and for re-runs

POC

Built and validated, not yet released

Read-only means read-only. Where a tool is meant to read, the client it uses has no write capability at all — enforced by tests, not by policy.

Nothing writes blind. Anything that changes data dry-runs first, is safe to re-run, and leaves a report you can hand to a director.

01 The catalogue at a glance

Every tool in one table: what it does, what it is built on, and what it is called in Slack. The sections that follow are the deep dive on each one.

NAMING CONVENTION

Anything with a face in Slack gets a human first name, so people ask **Greg** rather than *the Google Workspace Admin Assistant*, and report an outage from **Sally** rather than *outage_slack_ping*. The name is the product; the repo folder is the implementation detail.

 **Greg** Google Admin Support

 **Sally** SaaS Outage Status

 **Ava** API Key Alerts

Headless jobs that only write to Confluence or JSM Assets have no Slack presence, so they take no name. Helpdesk Tasks is the next one due a name as it moves to production.

SLACK NAME	TOOL	WHAT IT DOES	TECH STACK	STATUS
CONVERSATIONAL AGENTS				
 Greg	Google Workspace Admin Assistant	Answers plain-English Workspace admin questions across all 21 organizations. Strictly read-only.	FastAPI · Cloud Run · Claude Opus 5 · Admin SDK · Cloud Identity · Chrome Mgmt · Slack Events	LIVE
SLACK SERVICE DESK				
—	Helpdesk Tasks	Mailbox and offboarding actions across every Workspace organization, from one Slack modal.	FastAPI · Cloud Run · Cloud Tasks · Gmail API · Admin SDK · Slack modals	LIVE
—	Helpdesk Audit Pipeline	Turns every helpdesk action into a durable BigQuery record and a monthly Confluence page.	Cloud Logging sink · BigQuery · Cloud Run · Cloud Scheduler · Confluence REST	LIVE
ALWAYS-ON AUTOMATIONS				
 Sally	SaaS Outage Watcher	Watches 16 vendor status feeds and posts once when an incident opens and once when it resolves.	Python · Actions (5 min) · Statuspage / incident.io / StatusCast · Slack Block Kit	LIVE
—	Okta Audit Log	Logs every new group, app integration, group-to-app assignment and admin grant in Okta to Confluence.	Python · Actions (15 min) · Okta System Log · Confluence REST + content properties	LIVE
 Ava	Okta API Key Ping & Key Log	Keeps the HR-to-Okta provisioning tokens alive, and posts every key created or revoked.	Python · Actions (10-day + hourly) · Okta API · Slack webhook · Confluence REST	LIVE
—	Domain Expiry Sync	Syncs real registrar expiry dates onto the domain records in JSM Assets, and reports the rest.	Node.js · Actions (monthly) · GoDaddy API · RDAP fallback · JSM Assets AQL	LIVE
IDENTITY ENGINEERING · ON DEMAND				
—	Okta Title Sync & Title Nudge	Corrected every Okta job title, then forced the Okta-to-Slack SCIM push to land tenant-wide.	Node.js · Okta Users API · HR CSV parser · 1Password CLI · Slack SCIM	COMPLETE
—	Slack Title Audit	Read-only proof of which users that SCIM push actually reached, and why the rest were blank.	Node.js · Slack Web API + SCIM v2 · Okta API · headless Chrome PDF	COMPLETE
—	Okta Licence Cleanup	Buckets every Okta account against HR data to find the genuinely reclaimable licence seats.	Node.js · Okta Users API · HR CSV join · markdown + PDF · JSON audit log	COMPLETE
—	Okta Policy Replicate	Copies a parent org's Okta security policies into a new spinoff tenant, remapping every ID.	Node.js · Okta Policy / Group / Zone APIs · cross-org name remapper	LIVE
—	Okta Profile Backfill	One-time profile attribute backfill for accounts predating the TriNet integration.	Node.js · Okta Users API · HR CSV · partial-profile PATCH	COMPLETE
—	Okta Entity Status	Stamps a for-profit / non-profit attribute on every active user from their login domain.	Node.js · Okta Users API · entity tax-status lookup table	COMPLETE

SLACK NAME	TOOL	WHAT IT DOES	TECH STACK	STATUS
—	Okta Group Scrape	Read-only CSV export of every Okta group and every group membership, for audit and migration.	Node.js (stdlib only) · Okta Groups API · Link-header pagination · CSV	COMPLETE
—	JSM Invoice Scraper	Captures hardware invoice PDFs from the SysEng mailbox and links them to the right asset record.	Apps Script · Gmail · Drive · Sheets · Apple Business Manager · JSM Assets	POC

02 The Workspace assistant

A Slack-native agent with no scripted commands and no menus. The model reads the question, decides which read-only lookups will answer it and for which organization, runs them, and writes the reply from live data. That is why follow-ups and odd phrasings work.

Google Workspace Admin Assistant

Ask anything about any of our Google Workspace organizations, in plain English, from Slack.

SLACKCLAUDE OPUS 5WORKSPACECLOUD RUN

Answers Workspace admin questions without anyone opening an Admin Console — accounts and suspensions, who holds admin roles, 2-Step Verification and SSO posture, audit and login activity, Chromebooks and Chrome extensions, org units, groups and domains. Name the organization however you like: its name, a nickname, or any email domain that belongs to it.

Slack DM
or @mention

Cloud Run
FastAPI · signed

Claude Opus 5
tool loop

~20 read-only tools
each scoped to one organization

Admin SDK
directory · devices

Reports & Audit
logins · admin log

Cloud Identity
2SV · SSO policy

Chrome Management
devices · extensions

21 Google Workspace organizations
each reached with its own delegated service account · read-only scopes only · routed from the domain in your question

No scripted commands: the model picks the lookups, runs them live, and writes the answer.

It analyses, it doesn't just report. It reads what Google returns and says what stands out — a Super Admin who hasn't signed in for two years, accounts enforced for 2SV but not enrolled, a permission change made just before an offboarding. Where it can't see something, it says so, rather than letting an empty result imply all clear.

Scopes
Every OAuth scope ends in .readonly, and a unit test fails the build if one doesn't.

Code
Only list, get and report calls exist. There is no mutating path to reach.

Grant
Each organization only ever authorizes the read-only scope list.

WHY IT CAN'T GO WRONG It cannot suspend, edit or delete anything even if someone asks it to — and it reads administrative data only: settings, membership, activity. Never anyone's mail, files or messages.

RUNS ON
Cloud Run · us-central1

COVERAGE
21 organizations routable

INTERFACE
Slack DM or @mention

ONBOARDING
One Admin Console change — no redeploy

03 Slack service desk

Not an agent — a deterministic tool with a modal, for work that must do exactly what was asked, every time. Helpdesk staff get a form; the backend handles routing, permission, execution and the audit record.

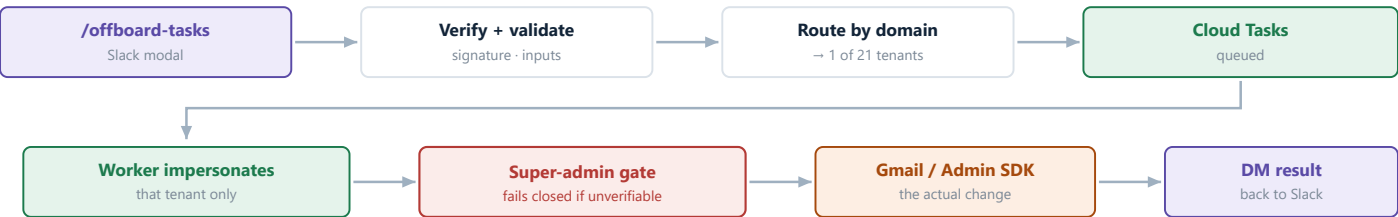
Helpdesk Tasks offboarding + mailbox module

LIVE

Mailbox and offboarding tasks across every Workspace organization, from one Slack modal.

SLACK CLOUD RUN + TASKS GMAIL + ADMIN SDK

Out-of-office, mailbox delegation, send-as aliases, forwarding, delegate listing, Google Group membership, and a bundled offboarding sequence. It works out which organization a mailbox belongs to from its domain — so helpdesk staff never need to know which console a user lives in, or hold admin rights in it.



Blocked requests get a deliberately generic Slack reply — it reveals nothing about why.

The guardrail is checked four times, and the last check happens after the queue — inside the worker, before any Google call.

FAILS CLOSED

Every route's admin account is protected automatically, and the worker reads the target's Directory record and refuses any account holding an administrator role. If that role check itself can't be completed, the request stops — before any Google API call, not after.

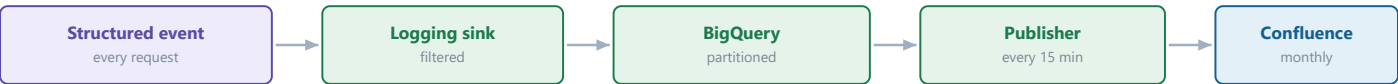
ROUTES	BULK MODE	REPLACES
21 organizations, one shared config	One action across many mailboxes, by CSV	Manual console work + an Okta Workflows path

Helpdesk Audit Pipeline

LIVE

Turns every helpdesk action into a durable audit dataset and a readable monthly Confluence page.

BIGQUERY CLOUD SCHEDULER CONFLUENCE



RECORDED

requester · action · mailbox · organization · result · per-step counts · guardrail reason

NEVER

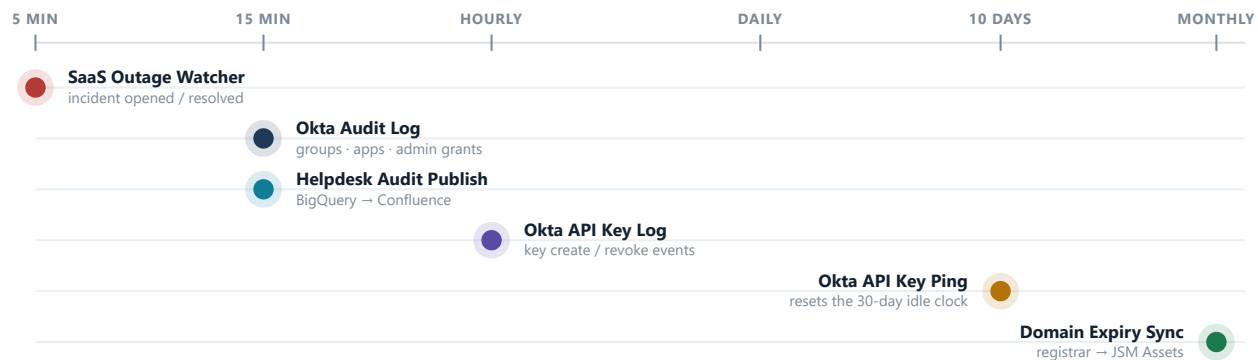
message content · tokens · service-account keys · raw exception bodies

BigQuery is the durable source of truth; the Confluence page is a view rebuilt from it, so a retry can never duplicate a row.

CADENCE	DESIGN
Publishes every 15 minutes	Confluence outages cannot affect a live request

04 Always-on automations

Unattended jobs on GitHub Actions. Each keeps something true that would otherwise drift — an audit trail, a token, an expiry date, an outage timeline.



Six unattended workflows. A failed run is itself the alert — every job exits non-zero when something needs a person.

Okta Audit Log → Confluence

LIVE

A running, human-readable record of every consequential change made in Okta.

SYSTEM LOG CONFLUENCE IPO

Appends a row for each new group created, app integrated, group-to-app assignment, and admin role granted to a user or a group. A parent index tracks running counts per month — so “what changed in Okta in June” is a page, not a log query.

NO DATABASE

The last-processed timestamp lives in a property on the index page itself. The integration needs no storage of its own, and rows de-duplicate against what's already published, so re-scanning a window is always safe.

CADENCE	PAGE	LIVE SINCE
Every 15 minutes	IPO · 3.C.1	May 2026

Okta API Key Ping & Key Log

A Ava LIVE

Stops the HR-to-Okta provisioning tokens dying quietly, and logs every key created or revoked.

API TOKENS CONFLUENCE IPO ALERTING

Okta deactivates an API token after 30 days of inactivity. Each entity's TriNet integration uses its own token, and entities that go a while without hiring never exercise theirs — so it dies silently, and the failure only surfaces when the next new hire fails to provision. One cheap read-only call resets the clock, and the run doubles as an audit of which tokens are alive, dead or erroring.

STATED HONESTLY

Pinging cannot revive a dead token, and Okta shows a token's value only once. This tells you which integrations need a new key issued — it can't recover them.

CADENCE	SCOPE	PAGE
Keepalive ~every 10 days · key log hourly	16 per-entity provisioning tokens	IPO · 3.C.2

Domain Expiry Sync

registrar → JSM Assets

LIVE

Keeps every domain's expiry date in the asset register true to what the registrar actually says.

JSM ASSETS CONFLUENCE GODADDY · RDAP

Reads every domain and expiry date from the registrar and writes to Assets only where the calendar date genuinely differs. Everything it doesn't touch — domains missing from Assets, unsupported registrars, blank registrar fields — is reported rather than silently skipped, and each live run publishes a monthly Confluence page.

SELF-DISCOVERING SCHEMA Object type and attribute IDs are resolved at runtime from their display names. If a name is wrong, the first run prints the real available names and stops — instead of writing a date into the wrong field.

CADENCE Monthly, 1st of the month	SAFETY Dry-run default on manual runs	IN PROGRESS Auto-creating newly bought domains
---	---	--

SaaS Outage Watcher

S Sally

LIVE

One Slack channel that tells you when a vendor is down — and when they're back.

BLOCK KIT ALERTS 16 PUBLIC STATUS FEEDS

Posts on two events only: an incident *opening* and that same incident *resolving*. Between those edges it stays silent, so the channel reads as a clean outage timeline rather than a firehose. The active-incident state is committed back only when it changes, which makes its history an outage log.

A BROKEN FEED CAN'T FAKE A RECOVERY If a vendor's own status page errors, that vendor's known incidents are held in state rather than reported as resolved.

Documented gap: Okta publishes no public status feed — its status page sits behind a login — so it can't be polled this way. Covering it needs a paid aggregator, or piping Okta's own Trust notifications into Slack.

CADENCE Every 5 minutes	VENDORS Slack · Zoom · Google · GitHub · NetSuite · Splunk · +10	REQUESTED BY The CIO
-----------------------------------	--	--------------------------------

05 Identity engineering

On-demand tools for the projects that move identity data at scale — a Slack SCIM migration, a licence overage, a tenant spinoff. Each dry-runs by default and reports before it writes.

Okta Title Sync & Title Nudge

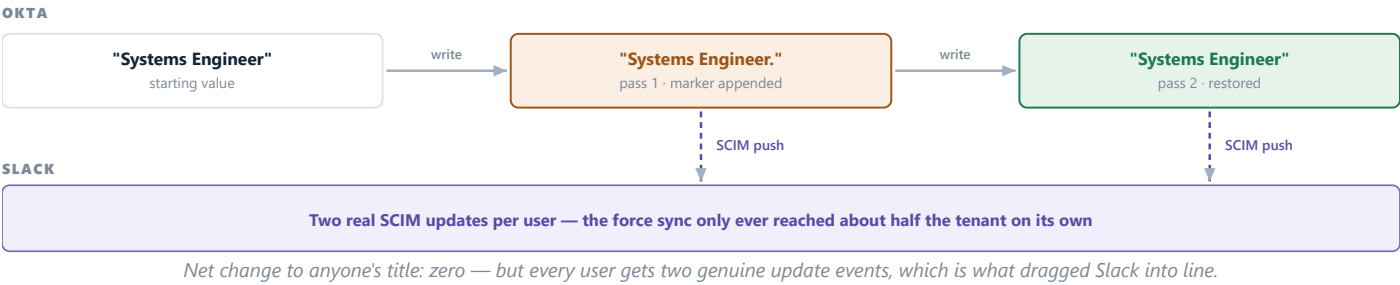
COMPLETE

Got every job title in Okta right before Slack started treating Okta as the truth — then forced Slack to catch up.

PROFILE WRITES SCIM

Slack Enterprise Grid's title field was switched from user-edited to SCIM-managed, sourced from Okta. The moment that flipped, every wrong title in Okta was going to propagate to every Slack profile at once — and Slack keeps no history to roll back to. **Title Sync** swept the tenant against the HR export and wrote one attribute, skipping anyone already correct so the write volume was the genuine delta. It never nulls a title out.

Title Nudge solved the follow-on: the force sync only reached about half the tenant. Since any real change to a title fires a fresh SCIM push, the tool manufactures one for everybody.



WHY THE RESTORE ISN'T "STRIP THE CHARACTER" Nine real HR titles already end in a period — *Managing Director, Comms.* and similar — so a naive strip would corrupt them and push the corruption downstream as the new truth. And ~265 accounts have no HR record at all, so an HR-only restore would abandon them wearing the marker permanently.

SCALE	TESTED	PACING
~730 titled users, two passes each	34 offline assertions before production	Throttled — each write fans out to SCIM

Slack Title Audit

COMPLETE

Read-only proof of whether that SCIM push actually landed. Every call is a GET.

USERS.LIST + SCIM CROSS-REFERENCE

Before force sync it captures the baseline, because force sync destroys every user-edited title and anything not captured is gone permanently. After, it finds who ended up blank and — crucially — *why*. A raw list of blanks isn't a finding: most people are blank because Okta has no title for them either. The finding is the one bucket where **Okta has a title and Slack doesn't**.

IT WAITS FOR THE RIGHT ANSWER SCIM is asynchronous, so straight after a force sync a user Okta hasn't reached yet looks identical to one it failed on. The tool samples on an interval and only reports once the blank count holds steady across three consecutive samples — and shows the settling curve so you can watch it converge.

ACCESS	TESTED	OUTPUT
The client has no write method at all	42 offline assertions	JSON snapshot + HTML and PDF report

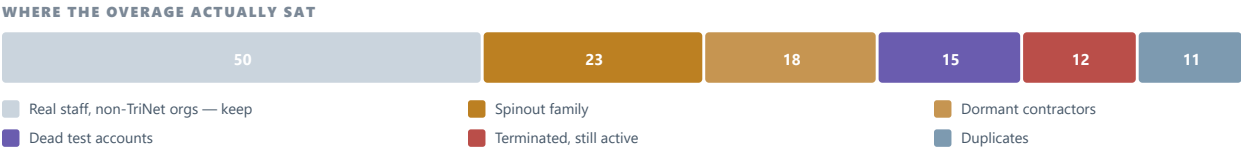
Okta Licence Cleanup

COMPLETE

Found where our Okta seat overage actually was — and, more usefully, where it wasn't.

READ-ONLY HR JOIN

Enumerates every account, joins both HR tabs, and sorts each one into a bucket: service account, spinout, current employee, terminated-but-active, dormant, contractor, duplicate or orphan. The reporting tool is strictly read-only — there is intentionally no deactivation code inside it.



REALISTIC RECLAIM POOL 55–65 seats. Roughly 50 of the 129 are real staff at organizations TriNet simply does not manage.

Offboarding turned out to be healthy — 375 of 387 terminated staff were already deprovisioned. The overage was structural.

WHY IT BUCKETS INSTEAD OF DEACTIVATING ON ABSENCE Absence from the HR sheet is ambiguous — it means either “terminated” *or* “never was an employee”. The service accounts that feed the HR sheet aren't in the HR sheet, so deactivating on absence would have broken the sync that produces the data. A first wave that wrongly caught four new hires is why there's now a permanent new-hire guard and an undo tool.

OUTCOME	TOOLING
Director-approved deactivation policy, by bucket	Report · batch deactivation · reactivation undo
SAFETY	
Dry-run default · service-account denylist · audit log	

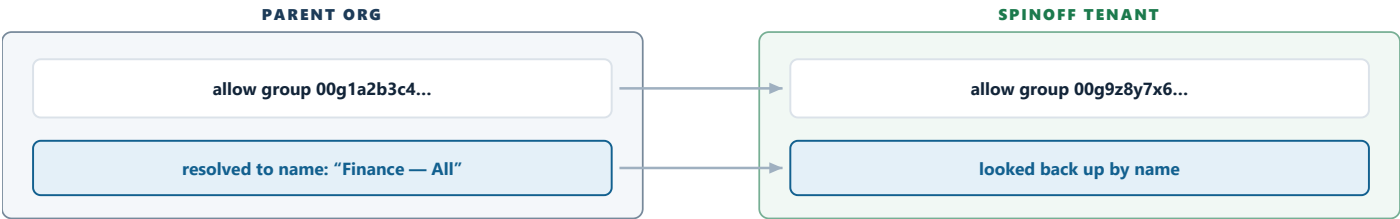
Okta Policy Replicate

LIVE

Gives a spinoff entity's brand-new Okta tenant the parent org's security posture, instead of a hand-rebuild.

POLICIES CROSS-ORG

Copies authentication, authenticator-enrollment, password and global session policies from the parent org into a new tenant. Okta has no native export/import, so the alternative is rebuilding by hand — slow, and quietly divergent from the parent from day one.



Anything that cannot be resolved is a blocker — the run refuses to start rather than leaving a tenant half-configured.

DRY RUN IS THE DEFAULT HERE Writing takes an explicit flag — the inverse of the other sync tools. Deliberate: those write a data field, this writes a tenant's authentication policy.

FIRST USE	HELD BACK
Password policy applied live to a spinoff, Aug 2026	Session policy — parity would have loosened the new tenant
REUSABLE	
Built generic for the next spinoff	

Okta Profile Backfill	One-time backfill of profile attributes for legacy accounts predating the TriNet integration. Completed May 2026 — 147 users, zero failures.	COMPLETE
Okta Entity Status	Stamps a for-profit / non-profit attribute on every active user from their login domain, driven by the entity tax-status sheet. Idempotent; unmapped domains are reported, never guessed at.	COMPLETE
Okta Group Scrape	Read-only exporter producing two CSVs — one row per group, one per membership — for audit and migration work. The token can be entered at a hidden prompt so it never touches disk.	COMPLETE
JSM Invoice Scraper	Apps Script intake that captures hardware invoice PDFs to a locked Drive folder, then reconciles order numbers to device serials so the invoice link lands on the right asset record.	POC

06 Shared foundations

The conventions that make all of the above consistent with each other — extracted from real use, not designed up front.

Secrets never live on disk Scripts only read an environment variable; the invocation decides where the value came from — 1Password	Employee data stays out of the repo A tracked .gitignore only protects the branches it exists on. So HR exports and report	Read-only tools have no write methods The Slack read client has no post method; the assistant has no mutating path. It is a	Every run leaves something readable A shared module renders a print-styled HTML report and a PDF from the same run data, so
--	--	---	---

on a laptop, Actions secrets in CI, Secret Manager on Cloud Run. Same script, all three.

snapshots default outside the working tree entirely — removing the failure mode instead of guarding it.

property of the code, not a rule someone has to remember.

any job's output can be attached to a ticket without reformatting.

07 How this came together

- **Dec 2025 – Mar 2026** Endpoint and migration scripting — Sophos removal and migration validation, Windows imaging and desktop management — then the Rise web properties: a live fellow directory, an events calendar, a dynamic handbook, and widgets.
- **Apr 2026** First backend services. The Slack offboarding module and the first Workspace admin assistant backend land on Cloud Run.
- **May 2026** Okta Audit Log goes live to Confluence. The profile backfill and entity-status syncs complete.
- **Jun 2026** The helpdesk module moves to a hardened Cloud Run backend. Token keepalive goes live. Licence reconciliation produces a director-approved policy.
- **Jul 2026** Outage watcher and domain expiry sync ship — the busiest month of the year at 148 commits.
- **Aug 2026** Helpdesk bulk actions and the super-admin guardrail; the BigQuery-to-Confluence audit pipeline; policy replication for the first spinoff tenant; the Slack title migration; and the assistant's rebuild onto an agentic Claude Opus 5 backbone with multi-tenant routing.

Where to start

A question about Workspace? Ask the assistant in Slack. **A mailbox change?** Helpdesk Tasks. **Is a vendor down?** The outage channel already knows. **What changed in Okta?** The audit pages under 3.C.1.

Want one of these extended, or something new automated? Contact Adam Schembri or the IT Operations team. Most of these started as one person's small annoyance.