



Ops Control Center

ITIL operations in one view: from alert to decision

Concept prototype on sample data · Roman Krol

The problem in day-to-day operations

1

No prioritised view

Every morning starts with searching many tools.

2

Change friction

Approvals take long, conflicts surface late.

3

Broken learning loop

Recurring incidents never really get fixed.

4

Providers without evidence

SLA talks without your own numbers and proof.

5

Recovery unproven

Backups without a restore test.

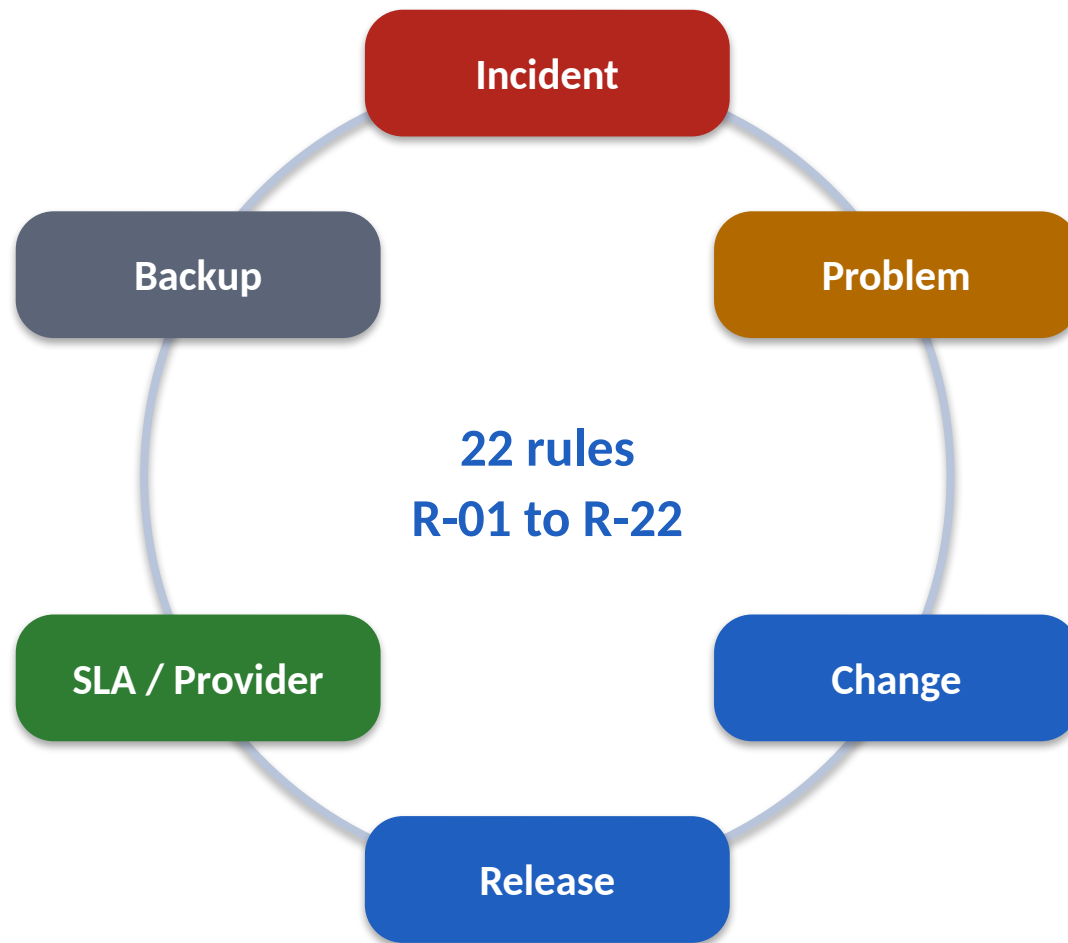
6

Reporting toil

The monthly report costs hours of manual work.

Source: desk research at vendor level (docs/itsm-research.md), not yet validated with practitioners

The idea: one loop with rules as guardrails



Prioritised, not searched

One list, "Handlungsbedarf": what to do today, with the rule behind it.

Rules, not gut feeling

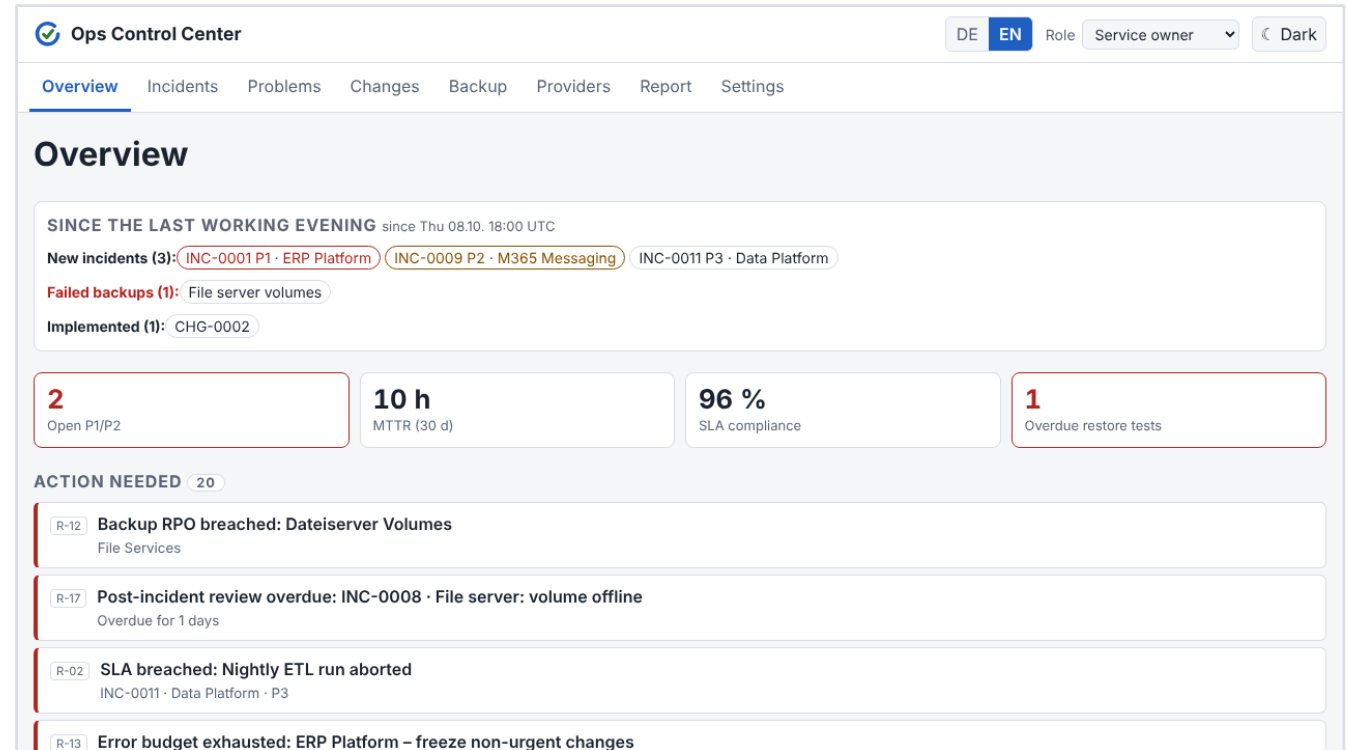
The logic is deterministic and tested, not estimated.

Provable

Every change writes an immutable audit entry (R-15).

Overview: what needs doing today

- Action list sorted by severity, every row with its rule ID
- Four key figures: open P1/P2, MTTR, SLA compliance, restore tests
- Incident board and service health with error budget (R-13)
- Since the last working evening: new incidents, failed backups, implemented changes



Incidents: guardrails when resolving

- SLA clocks and escalation L1 to L3 (R-02, R-03)
- P1/P2 cannot be closed without cause and actions (R-01)
- Blast radius over dependencies, suspect change (R-10)
- Status message for P1/P2 at the push of a button, post-incident review (R-17)

The screenshot displays the 'Ops Control Center' interface. At the top, there's a navigation bar with 'Overview', 'Incidents' (selected), 'Problems', 'Changes', 'Backup', 'Providers', 'Report', and 'Settings'. User controls on the right show 'DE', 'EN', 'Role: Service owner', and a 'Dark' mode toggle. Below the navigation, a breadcrumb trail shows '← Incidents'. The main header for the incident is 'INC-0001 · ERP: order booking unavailable' with a 'P1' severity indicator. Below this, a status bar shows 'ERP Platform', 'Performance', 'In progress', 'L1 Operator', and 'Assigned to: Operator A'. There are 'Details' and 'Audit (1)' buttons. Two progress bars are shown: 'Response (R-02)' at 60% and 'Resolution (R-02)' with 2h 29min left. A section for 'Dependent services (blast radius): Fleet Maintenance System' is present. A warning box states 'Suspect change (R-10): CHG-0002 · ERP: database index rebuild'. At the bottom, there are input fields for 'Cause (required, R-01)' and 'Actions (required, R-01)', an 'Escalate' button, and a 'Resolve' button. A 'Draft status update' button is also visible.

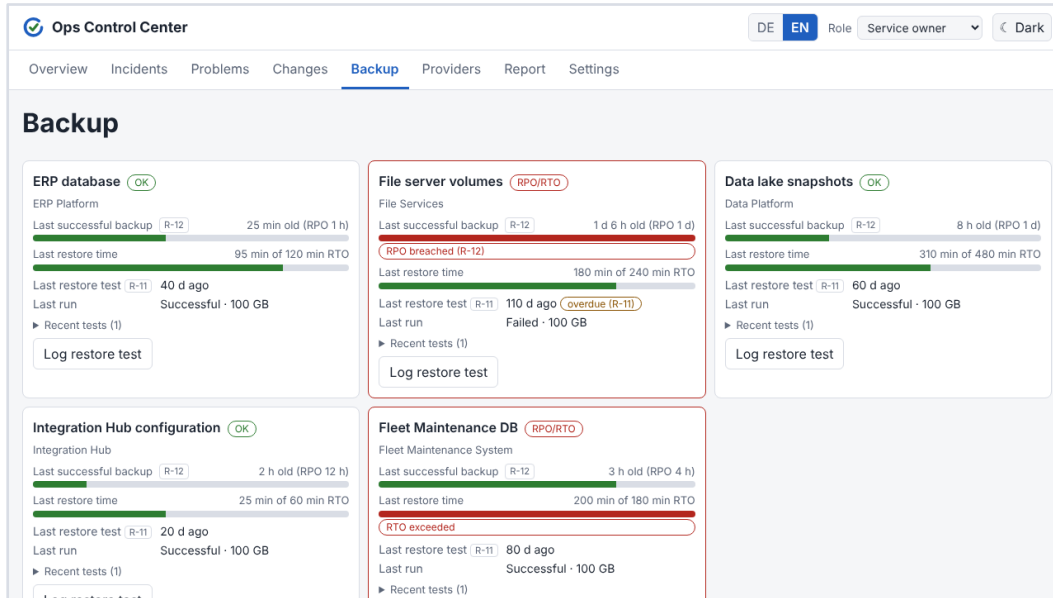
Changes: risk, approval, rollback

- Rollback plan and test evidence are mandatory (R-05)
- Risk calculated live (R-06), approvals by role (R-07)
- Freeze on an open P1 (R-08), conflicts between changes (R-09)
- Free maintenance window suggested, standard change fast path (R-19)

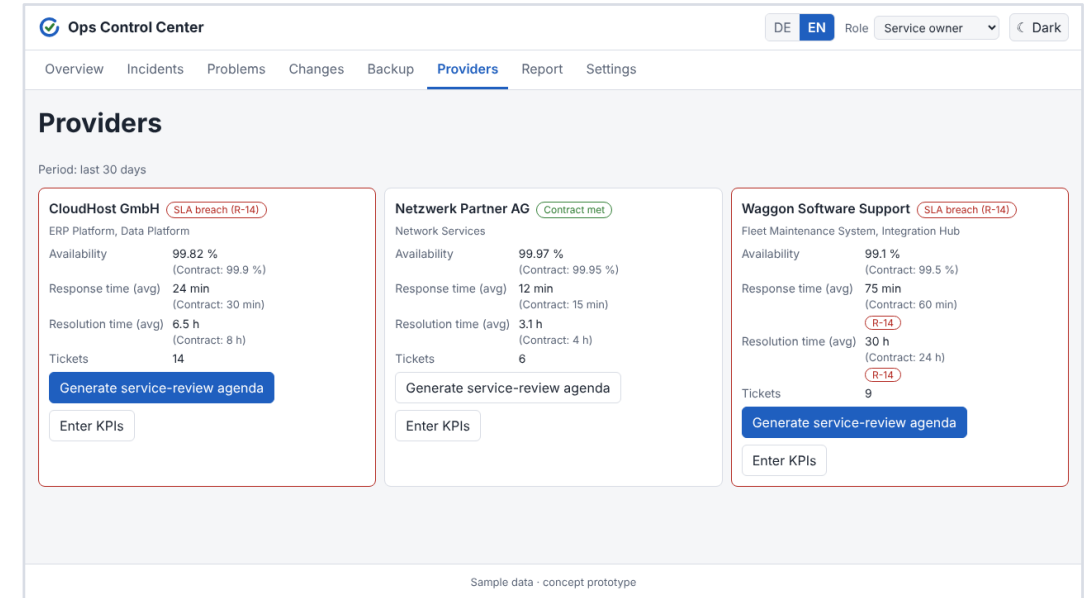
The screenshot shows the 'Ops Control Center' interface with the 'Changes' tab selected. The form includes the following fields and controls:

- Title:** A text input field containing 'Clean up firewall rules'.
- Service:** A dropdown menu with 'Data Platform' selected.
- Type:** A dropdown menu with 'Normal' selected.
- Impact (1-3):** A dropdown menu with '3' selected.
- Likelihood (1-3):** A dropdown menu with '2' selected.
- Start:** A date and time picker showing 'mm/dd/yyyy, --:-- --'.
- End:** A date and time picker showing 'mm/dd/yyyy, --:-- --'.
- Duration (min):** A text input field with '120' and a 'Suggest a free window' button.
- Rollback plan:** A text area with 'R-05' entered.
- Test evidence:** A text area with 'R-05' entered.
- Risk (live):** A label 'R-06' followed by a red status indicator 'High - Score 8'.
- Buttons:** 'Save draft' and 'Cancel' buttons at the bottom.

Backup and provider: evidence, not gut feeling



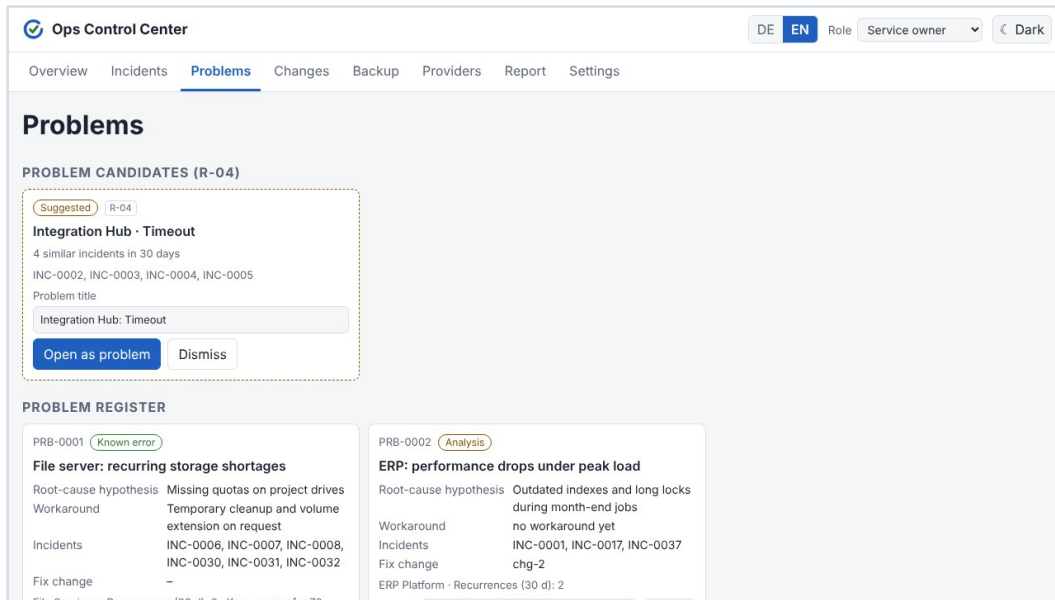
Backup



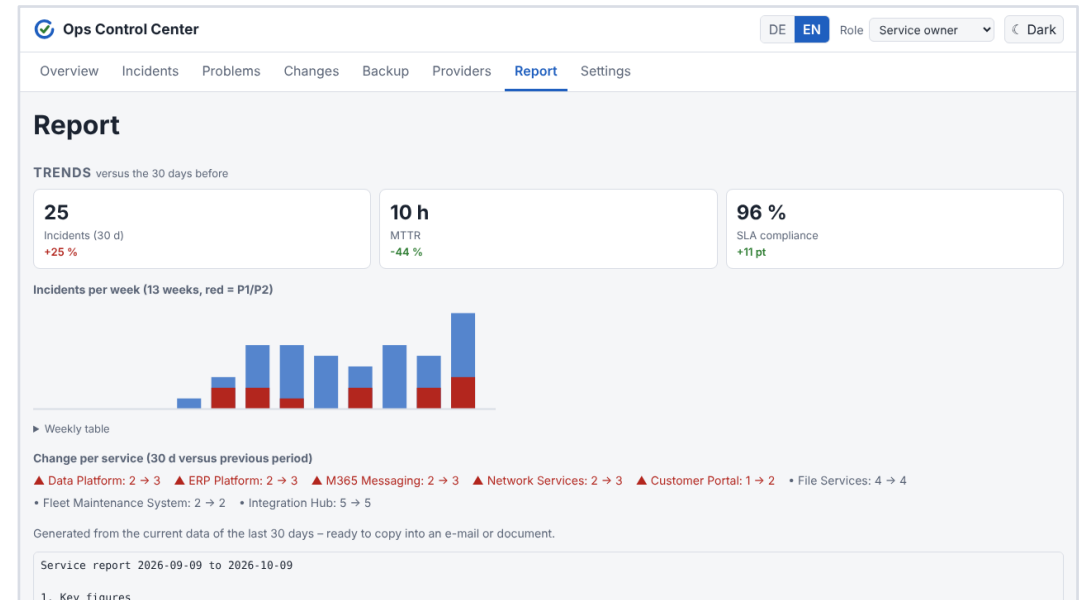
Provider

- Log a restore test: a backup only counts once it is recoverable (R-11, R-12)
- Provider KPIs against the contract (R-14), service-review agenda with evidence
- The service-credit deadline runs along (R-21)

Learning loop and reports



Problems

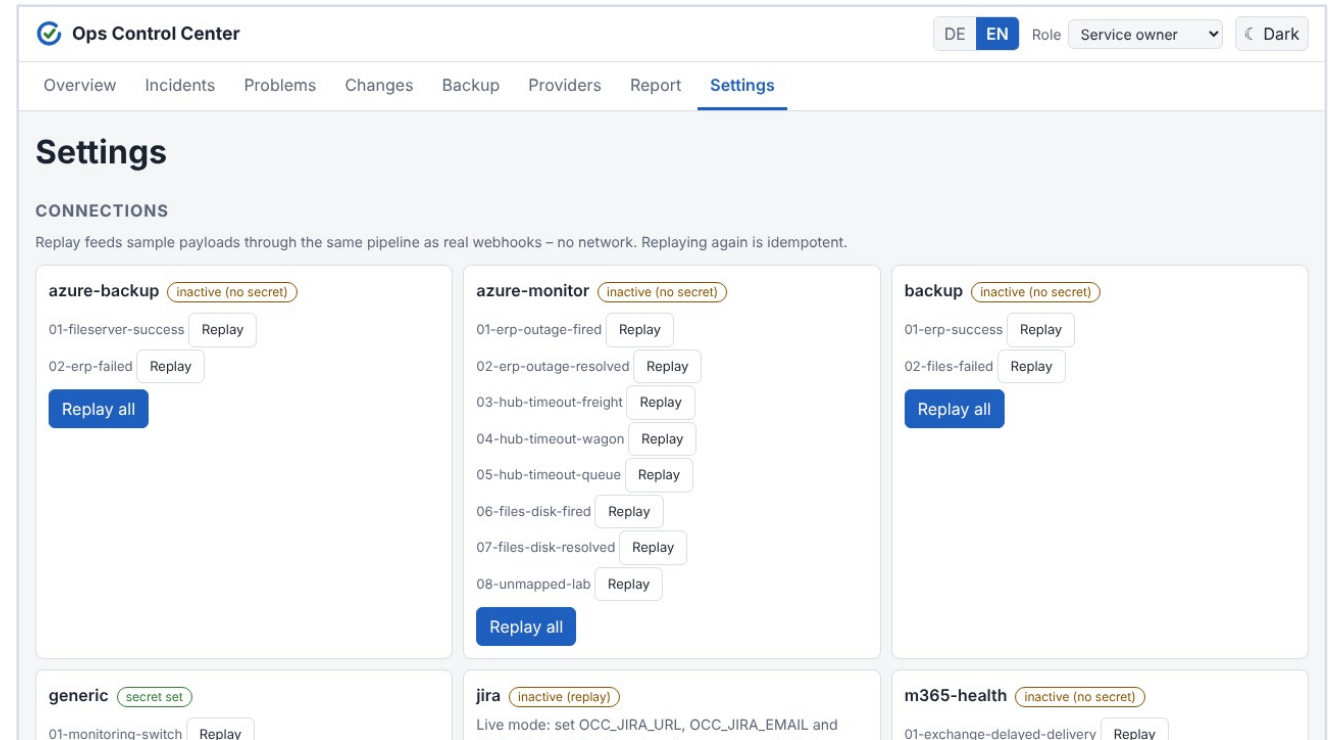


Report

- Problem candidates from recurring incidents (R-04), known error with workaround
- Monthly report and trends at the push of a button, ready to copy
- Decisions are suggested, never executed automatically

Sources: data arrives by itself

- Jira live: polled every minute, edits are followed, link back to the ticket
- Azure Monitor, M365, Azure Backup, provider reports (sample data in replay mode)
- Webhook for backup results with a script for the Windows server
- Unknown signals wait in a mapping queue (R-22)



ITIL practice and what the tool enforces

ITIL practice	Guardrail in the tool	Rules
Incident Management	SLA clocks, escalation, mandatory fields on close	R-01 to R-03
Problem Management	Candidates, known error with workaround, age	R-04, R-20
Change Enablement	Rollback, risk, approvals, freeze, conflicts, fast path	R-05 to R-09, R-19
Service Level Management	Error budget against SLO, SLA warnings	R-02, R-13
Supplier Management	Contract KPIs, review agenda, service-credit deadline	R-14, R-21
Service Continuity	RPO/RTO, restore tests	R-11, R-12
Continual Improvement	Post-incident review, trends, monthly report	R-17

Honest status

Verified

- 424 automated tests, 11 browser tests including accessibility (WCAG 2.1 AA)
- Jira connection verified live with demo tickets
- Login, audit log, access protection per the security baseline

Limits

- Concept prototype on sample data, not a production system
- Other sources run in replay mode; no MFA
- Windows operation prepared, not yet tested on a real server

Next: run on an own server, more sources live, conversations with practitioners