

Operations & Service Delivery · Service Delivery · Production Support

SMT Request Automation Agent

CAI Score L3 · Operate — Bounded autonomy

▲ this agent

L1 Assist	L2 Draft	L3 Operate	L4 Decide	L5 Autonomous
TIER	PILLAR	AUTOMATION	HUMAN ROLE	
L3 · Operate	Operations & Service Delivery	≈75% of routine effort	Owns exceptions and oversight	

01 — Executive summary

SMT Request Automation Agent is a CAI Score L3 (Operate) agent for operations & service delivery. Automates incoming support requests end-to-end — intake, classification, and fulfilment of standard requests — routing exceptions to people. It operates with bounded autonomy: a person owns exceptions and retains workflow oversight. Indicatively, it can redirect around 75% of the routine effort this work consumes.

02 — Problem & context

- Standard requests queue behind a person keying the same steps all day.
- Turnaround on routine requests is measured in days, not minutes.

03 — Representative use cases

- Automates the full intake-to-fulfilment loop for standard, low-risk requests — no manual keying required.
- Reduces turnaround on routine requests from days to minutes by removing the human queue.
- Classifies every incoming request and routes non-standard or complex items to the correct team automatically.
- Handles high-volume request types — access requests, information requests, standard provisioning — without scaling headcount.
- Generates the evidence to track FTE capacity released, request volumes, and routing accuracy.

04 — How to use it

- 1 Connect it in your tenant to the systems this work already touches (production support).
- 2 Confirm scope, the named owner, and the oversight the tier requires.
- 3 Detects the trigger in the workflow
- 4 Handles routine in-policy cases end to end
- 5 Escalates exceptions to the owner
- 6 Logs every action for audit
- 7 Review the audit log and KPI movement after each cycle; tune scope as you learn.

05 — Where it fits in the process

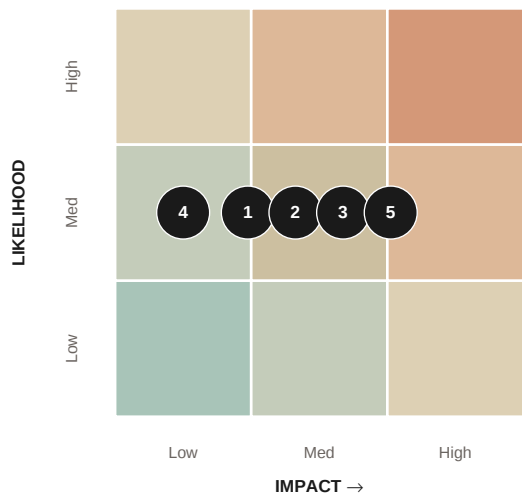
Replaces the manual request-handling lane entirely for standard, low-risk requests, while everything non-standard is routed to the right team.



Operating loop for a L3 agent – bounded autonomy.

06 — Risk assessment

#	RISK	LIKELIHOOD	IMPACT	MITIGATION / CONTROL
1	Incorrect or incomplete output	Medium	Medium	Routine cases only; exceptions and anything material are escalated to the named owner, with a full audit trail.
2	Over-reliance / reduced human scrutiny	Medium	Medium	Tier oversight keeps a human in the loop; KPIs monitor quality so reliance never outruns control.
3	Exposure of sensitive data	Medium	Medium	Runs inside your own tenant; Colleague AI processes none of your data, and access stays under your existing controls.
4	Behavioural drift over time	Medium	Low	Periodic review against KPIs and sampling detects drift; scope and prompts are version-controlled.
5	Out-of-policy or edge-case handling	Medium	Medium	Scope is bounded and documented; anything outside it is escalated, not improvised.



Residual likelihood × impact after the tier's built-in controls. Numbers map to the table above.

07 — Regulatory & compliance impact

FRAMEWORK	RELEVANCE	HOW THIS AGENT ALIGNS
EU AI Act	Operational use under human oversight; logging and risk-tiering apply.	Documented risk tier, human oversight and event logging per agent — designed to map to the obligations.
DORA	Relevant where the function is in scope for financial-sector operational resilience.	Actions are logged and attributable, supporting resilience and traceability requirements — designed to map to.
GDPR	Applies wherever personal data is in scope of the workflow.	Data stays in your tenant; Colleague AI processes none of it. Purpose limitation and minimisation are preserved.
ISO/IEC 42001	AI management-system controls: roles, monitoring, review.	The agent operates within a documented management system — defined tier, named roles, logging and review. Designed to meet; not certified.

“Designed to map to” / “designed to meet” describe alignment with the CAI Score framework, not external certification. Confirm obligations with your compliance function.

08 — Value & illustrative ROI

Automates incoming support requests end-to-end — intake, classification, and fulfilment of standard requests — routing exceptions to people.

Assumptions (illustrative — replace with your own)	Result
12 FTE engaged · 1840 productive h/FTE/yr · 75% addressable · €45/h blended	≈ 16,560 hours/yr redirected · ≈ €745,000/yr indicative value



Figures are an illustrative model to be validated against your own volumes and rates – not a guarantee.

KPIs to track

Approx. 12 FTE of capacity released · faster turnaround · consistent handling.

09 — Recommendations

- Define the standard-request taxonomy and fulfilment rules explicitly before deployment.
- Set conservative in-scope criteria at first; expand the automated lane gradually as accuracy is confirmed.
- Assign a named owner for exception routing; review the exception log weekly for the first month.
- Baseline request volume, turnaround time, and manual effort before go-live so the gain is quantifiable.

10 — Governance & method

This agent runs in your own Microsoft/Azure tenant; Colleague AI hosts only the control plane (score, policy, audit) and processes none of your data. A person owns exceptions and retains workflow oversight. Every action is time-stamped and attributable. The CAI Score classification is documented and open to challenge.

This dossier is an evaluation document. ROI and automation figures are illustrative models, not commitments. Compliance statements describe the CAI Score framework and are not a certification of your compliance with any law or standard. © Colleague AI – proprietary. CAI Score™.