CARE

WHITEPAPER

# Continuous Assurance for Continuously Changing Agents

## From point-in-time reviews to maintained assurance

An agent approved once may no longer be the same operational proposition after its tools, instructions, or surroundings change.

**AGENTIC CARE**

https://ai-managementsystem.com

## Contents


01 An accepted agent does not stand still

02 Periodic reviews miss changes between assessments

03 A tool change alters an existing risk decision

04 Maintain a baseline that can be challenged and renewed

05 Assurance needs independent checks

06 Choose evidence and review triggers deliberately

07 Deciding what requires continuous verification

08 Assurance follows change, not the audit calendar

09 Start with one agent


## An accepted agent does not stand still

An agent approved once may no longer be the same operational proposition after its tools, instructions, or surroun

A periodic assessment evaluates a particular configuration and operating context. New tools, data sources, prompts business processes can invalidate its premises long before the next scheduled review.

> **KEY FINDING**
>
> Assurance must follow the operating arrangement as it changes, rather than merely follow the calendar.

## Periodic reviews miss changes between assessments

Even when software code is unchanged, the practical capabilities of an agent can change because permissions and changed.

Track changes to purpose, actions, sensitive data, tool access, escalation, owner, runtime, and the systems affected. should cause a fresh assessment of the relevant part of the operating model, not necessarily a complete re-docume everything.

Use an accepted baseline to explain what changed and why the change matters. Without that baseline, every reviev

## A tool change alters an existing risk decision

> **EXAMPLE**
>
> A previously acceptable reporting agent is later connected to a customer database. No model yet the consequence of mistakes has.

Define which triggers require review: permissions, dependencies, business processes, external effects, incidents, or l

The decisive question is not simply whether the agent can carry out the task. It is whether the organization underst the operating arrangement in which it does so.

## Maintain a baseline that can be challenged and renewed

Periodic reporting can surface neglected ownership, open risk findings, incomplete reviews, and stale definitions. Ev focuses attention after a significant change. Both are needed: scheduled checks catch quiet neglect; events catch ra

A report describing an absence of findings should be distinguished from a report describing an absence of observa coverage is not evidence of safety.

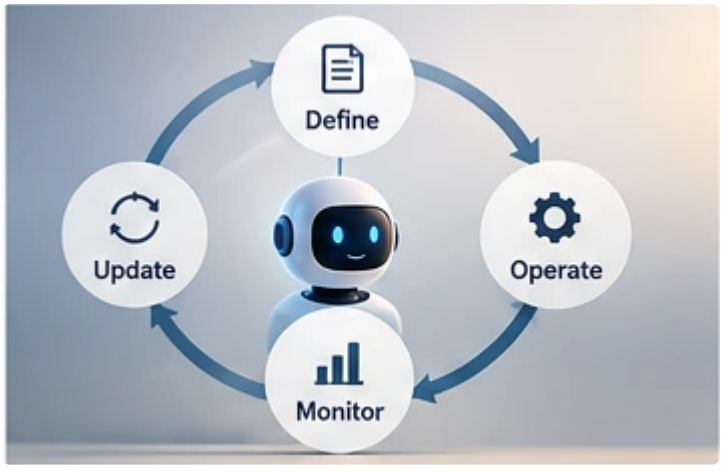
**AGENT AND AUTOMATION**

**Prepare descriptions, changes, findings and proposals.**

**ACCOUNTABLE PEOPLE**

**Validate context, assess consequ accept decisions.**

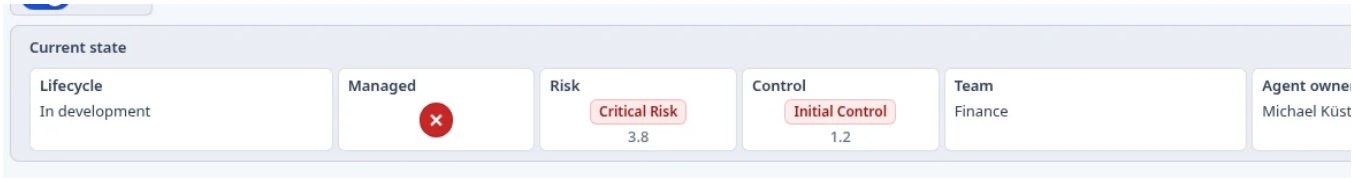
A continuing record of proposed and accepted changes makes reassessment part of operating practice rather than documentation project.




Assurance is a recurring cycle of definition, operation, monitoring and revision




Observed CARE pending-import approval for Finance Syncing: an ingestion waiting for approval with a field-by-field C comparison (Accept/Discard not actioned in this capture).




Observed CARE Current state for Finance Syncing: Lifecycle In development, Managed unmarked, Critical Risk 3.8, Initi Finance, Agent owner Michael Küsters.

## Assurance needs independent checks

Self-registration and self-evaluation reduce friction but introduce correlated error: the same agent may misunderst purpose and its success. Where consequences are material, independent tests, transaction audit evidence, and hum necessary.

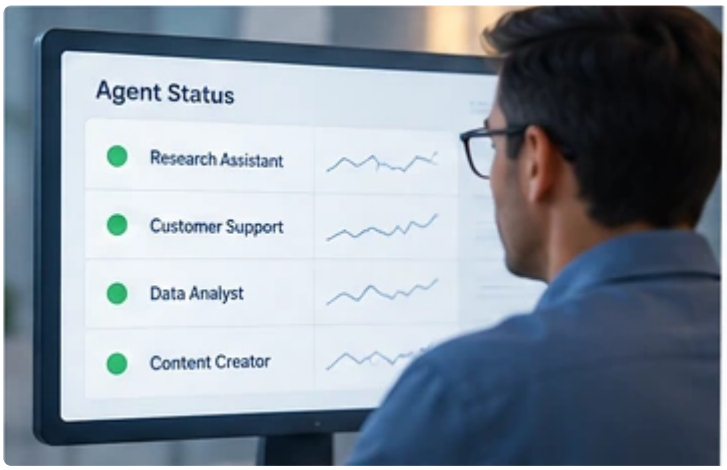
CARE provides a managed record and review workflow; continuous technical assurance depends on the quality and the connected evidence.

> **MANAGEMENT IMPLICATION**
>
> Define which triggers require review: permissions, dependencies, business processes, external e

Use this comparison to distinguish the current operating habit from the management capability the organization n

| Periodic-only approach | Maintained assurance approach |
| --- | --- |
| Reassess on the calendar | Also reassess after consequential change |
| Current document replaces past | Accepted baseline and change history |
| Green status for missing data | Coverage gaps remain explicitly unknown |

Use the comparison to test one real agent rather than discussing an abstract enterprise-wide target state. Where th unknown, record that uncertainty and assign responsibility for resolving it.




Portfolio oversight requires current status and evidence, not just an initial assessment.

## Deciding what requires continuous verification

Management decides which changes are material, which evidence requires refresh, and when intervention is necess a management baseline; actual runtime verification depends on the telemetry and integration coverage available to

## Assurance follows change, not the audit calendar

> Assurance must follow the operating arrangement as it changes, rather than merely follow the

The first practical improvement is to create one current, accountable record and use it to make a better manageme scalable system follows when that discipline is repeated across agents and maintained as conditions change.

1. the agent to https://ai-managementsystem.com/under-care.
2. it is finished, log into CARE and review its documentation.

---

Images and text generated with the assistance of ChatGPT by OpenAI.

---

**AGENTIC CARE**

Instant AI Management System for your Agents, as a Managed Service.

**https://ai-managementsystem.com**