ASSURANCE · AGS SOLUTIONS

Continuous Controls Monitoring

Periodic testing looks at a handful of cases months after the fact. Continuous controls monitoring tests every case as it completes, so a failing control surfaces while the work can still be corrected — and the annual audit becomes a review of records that already exist.

Why sampling stopped being enough

A sample of twenty-five cases from a population of forty thousand tells you very little about the other thirty-nine thousand, nine hundred and seventy-five. It was a reasonable compromise when testing was manual; it is hard to defend when the event data is already there.

Continuous monitoring inverts the economics. The cost of testing one case and the cost of testing every case are almost identical once the rule is written, so coverage stops being a budget decision.

- Every completed case is tested, not a sample drawn from it.
- Findings are dated to the day the breach happened, not the quarter it was found.
- Assurance effort moves from gathering evidence to investigating exceptions.

What you need before you start

Three things make a control monitorable: an event that proves the step occurred, a threshold that can be measured, and a person accountable for the outcome. Controls missing any of the three are recorded as gaps rather than quietly skipped.

Most organisations find that around two thirds of their control set is already monitorable from existing system events, and the remaining third needs one or two new events captured at source.

- A case reference, an activity name, and a timestamp for every step.
- A measurable threshold — time, value, count, or sequence.
- A named owner who receives the exception and can act on it.

Handling exceptions without drowning the team

The first week of monitoring usually produces more exceptions than anyone expected, because the true failure rate was never visible. The answer is not to weaken the rule but to triage: group exceptions by cause, fix the systemic ones, and route the rest.

Each exception carries the case, the rule, the threshold breached, and the evidence, so an owner can judge it in a minute rather than reconstructing what happened.

- Run in observation mode first to establish the real baseline.

- Cluster exceptions by root cause before assigning individual owners.
- Close the loop: every exception ends in accepted, corrected, or rule changed.

What the audit looks like afterwards

When controls are monitored continuously, the audit conversation changes from "show me your evidence" to "show me your exceptions and what you did about them". The records already exist, dated and attributable.

Internal audit can re-run the same tests independently, which is a stronger assurance position than reviewing a pack the business assembled about itself.

- Evidence is generated as a by-product of the work, not compiled afterwards.
- Auditors can re-run the tests themselves over the same period.
- Control failures show a trend line, so improvement is demonstrable.

Video walkthrough — key points

1. Sampling versus full population

- Twenty-five of forty thousand
- Months of delay
- Coverage as a budget line

Periodic testing samples a handful of cases months after the work happened, which tells you very little about the rest of the population. Continuous monitoring tests every case as it completes, so coverage stops being a budget decision.

2. Three things make a control monitorable

- An event
- A threshold
- An owner

A control can be monitored when there is an event proving the step occurred, a threshold that can be measured, and a named person accountable for the outcome. Controls missing any of the three are recorded as gaps rather than quietly skipped.

3. Expect a spike, then a slope

- Observation mode first
- Cluster by root cause
- Then enforce

The first week produces more exceptions than anyone expects, because the true failure rate was never visible. Run in observation mode, group the exceptions by cause, fix the systemic ones, and only then move the stable rules into enforcement.

4. Exceptions people can actually action

- Case attached
- Rule and threshold named
- Closed three ways

Each exception arrives with the case, the rule, the threshold breached and the supporting evidence, so an owner can judge it in a minute. Every exception ends in one of three states: accepted, corrected, or rule changed.

5. A calmer audit

- Evidence already exists
- Auditors re-run the tests
- Trends, not snapshots

Because evidence is produced as a by-product of the work, the audit becomes a review of records that already exist. Auditors can re-run the same tests independently, and control performance shows as a trend rather than a snapshot.