GUIDE · AGS RESOURCE LIBRARY

The Governance-by-Design Primer

Most control failures are design failures. This primer shows how to put governance into a process while it is still being drawn, so the control is part of how the work runs rather than a report written after it.

Why controls bolted on afterwards fail

A control added after a process is live has to fight the process. It sits outside the flow of work, so it depends on someone remembering to apply it, and it is measured by a report written days or weeks later. By the time a breach is visible, the work has already gone out of the door.

Governance by design reverses the order. The control is specified at the same moment as the step it governs: who may perform it, what evidence it must produce, how quickly it must complete, and what happens when it does not.

- Late controls rely on memory and goodwill; designed controls rely on the process itself.
- If a control cannot be measured from the event log, it is a statement of intent, not a control.
- Every control should name an owner, a threshold, and a consequence.

The four design questions

Before a process is signed off, four questions should have written answers. They take an hour to answer and save quarters of remediation.

- What must always be true? These become your invariants — required steps, approval limits, segregation of duties.
- What must never happen? These become your prohibitions — the same person raising and approving, a payment without a match, a change without a test.
- How will we know? Name the recorded event that proves each answer. No event, no control.
- Who acts when it breaks? A breach with no named owner is a notification, not governance.

From policy to measurable rule

Policy language is deliberately broad; a rule has to be narrow enough to evaluate. The translation step is where most governance programmes stall, and it is mechanical once you have the pattern.

Take the policy sentence, isolate the measurable noun, attach a threshold, and bind it to an activity in the process. 'Invoices should be approved promptly' becomes 'the Approve activity must occur within 48 hours of Invoice received, measured per case, owned by the Finance Operations lead'.

- Cycle-time limits: a step, or a whole case, must complete inside a stated window.

- Required steps: a named activity must appear in every case of this type.
- Segregation of duties: two named activities must be performed by different people.
- Thresholds: value, volume, or rework count above which a second pair of eyes is required.

Evidence that survives an audit

An auditor is not asking whether you believe the control worked. They are asking for the record. Designed controls produce that record automatically: the case, the activity, the timestamp, the actor, the rule that was evaluated, and the outcome.

Store the evidence with the breach rather than reconstructing it later. A breach record that carries its own evidence can be exported, reviewed, and closed without a hunt through inboxes.

A ninety-day starting path

You do not need a programme. You need one process, one set of rules, and one month of history.

- Weeks 1–2: pick a process with real volume and real pain. Pull an event log with case, activity, and timestamp.
- Weeks 3–6: discover the actual map, agree the four design questions, and write between five and ten rules.
- Weeks 7–10: run the rules over history. Expect surprises; tune thresholds rather than arguing with the data.
- Weeks 11–13: assign owners to exceptions, agree the review cadence, and publish the first evidence pack.

Video walkthrough — key points

1. Governance by design

- Controls written with the process
- Not bolted on afterwards

Welcome to the Governance by Design primer from Automated Governance Systems. Most control failures are design failures. In the next few minutes we will look at why controls added after the fact tend to fail, and how to build them into a process while it is still being drawn.

2. Why late controls fail

- They sit outside the flow of work
- They depend on someone remembering
- Breaches surface days later

A control added after a process is live has to fight that process. It sits outside the flow of work, it depends on a person remembering to apply it, and it is measured by a report written days or weeks afterwards. By the time a breach becomes visible, the work has already left the building.

3. The four design questions

- What must always be true?
- What must never happen?
- How will we know?
- Who acts when it breaks?

Before a process is signed off, four questions need written answers. What must always be true. What must never happen. How will we know, naming the recorded event that proves it. And who acts when it breaks. An hour spent here saves quarters of remediation later.

4. Policy to measurable rule

- Isolate the measurable noun
- Attach a threshold
- Bind it to an activity

Policy language is broad. A rule has to be narrow enough to evaluate. Take the policy sentence, isolate the measurable noun, attach a threshold, and bind it to an activity. Invoices should be approved promptly becomes: the approve activity must occur within forty eight hours of invoice received, measured per case, owned by the finance operations lead.

5. Evidence that survives audit

- Case, activity, timestamp, actor
- Rule evaluated, outcome recorded

An auditor is not asking whether you believe the control worked. They are asking for the record. Designed controls produce that record automatically: the case, the activity, the timestamp, the actor, the rule that was evaluated, and the outcome. Store the evidence with the breach, rather than reconstructing it months later.

6. Ninety days, one process

- Weeks 1–2: pick a process, pull the log
- Weeks 3–6: map it, write five to ten rules
- Weeks 7–13: run, tune, assign, publish

You do not need a programme to start. Pick one process with real volume and real pain. Pull an event log. Discover the map, write five to ten rules, run them over history, and tune the thresholds rather than arguing with the data. Assign owners to the exceptions and publish your first evidence pack. Ninety days, one process, and governance that is finally measurable.