

Governance-by-Design

Most control failures are design failures. Governance-by-design puts the control into the service while it is still being drawn, so it is part of how the work runs rather than a report written after it — and so the assurance team inherits something testable.

The four design questions

Before a new service is signed off, four questions should have written answers. They take about an hour and save quarters of remediation.

Teams that answer them produce services whose controls can be evaluated from the event log on day one. Teams that skip them produce services that need a control retrofit within a year.

- What must always be true? These become invariants.
- What must never happen? These become prohibitions.
- How will we know? Name the recorded event that proves each answer.
- Who acts when it breaks? A breach with no owner is a notification.

Designing the evidence, not just the control

A control that cannot be observed is an intention. At design time it costs almost nothing to emit the event that proves a step happened, who did it, and when. Retrofitting that same event into a live service is expensive and often politically impossible.

So the design review asks for the evidence schema alongside the process design.

- Every control names the event that evidences it.
- Evidence is emitted by the service, not reconstructed later.
- Retention and access are decided before launch, not after a request.

Fitting it into how teams already work

Governance-by-design fails when it becomes a separate gate. It works when it is a short, standard section of the design document and a checklist item in the review that teams already hold.

We supply the templates, run the first few reviews with your teams, and then hand the habit over.

- One page added to the design template, not a new committee.
- Reviewers trained on the same four questions.
- Exceptions recorded with an expiry date.

Video walkthrough — key points

1. Late controls fight the process

- Added after go-live
- Depend on memory
- Measured weeks later

A control added after a process is live has to fight that process. It sits outside the flow of work, depends on someone remembering it, and is measured by a report written days or weeks later. Governance by design reverses the order.

2. Four questions, one hour

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

Before a new service is signed off, four questions should have written answers. What must always be true. What must never happen. How will we know. And who acts when it breaks. An hour of answers saves quarters of remediation.

3. Design the evidence too

- Name the proving event
- Emit it from the service
- Decide retention up front

A control that cannot be observed is an intention. At design time it costs almost nothing to emit the event that proves a step happened, who did it and when. Retrofitting that same event into a live service is expensive and often impossible.

4. Make it a habit, not a gate

- One page in the design template
- Same reviewers
- Exceptions expire

Governance by design fails when it becomes a separate gate. It works when it is a short standard section of the design document and a checklist item in the review teams already hold. We run the first few with you, then hand the habit over.

© Automated Governance Systems. Shared for use inside your organisation. For a walkthrough against your own processes, book a session at ags-apip.lovable.app/book-demo.