

THE OPERATIONAL ASSURANCE MANIFESTO

A founding statement for the discipline of Operational Assurance

Strategy is not execution.

Organisations have never had more strategy. More policies. More procedures. More controls. More technology. More dashboards. More transformation programmes. More data.

And yet none of these things guarantee that the right thing actually happens when work gets done.

A policy can exist and still not be followed. A process can be designed and still be bypassed. A control can be documented and still fail. A transformation programme can be delivered and still fail to change behaviour. A dashboard can tell you what went wrong without helping prevent it. And an AI agent can execute a task perfectly - while executing the wrong task perfectly.

This is the execution gap.

As organisations become larger, faster, more automated and increasingly dependent on both human and artificial intelligence, that gap is becoming one of the most important sources of operational risk.

We believe it is time for a new enterprise capability.

Operational Assurance.

01. The enterprise has an execution blind spot.

Most organisations are very good at defining what should happen.

Strategy defines the objective. Governance defines the boundaries. Policies define the rules. Processes define the workflow. Technology provides the tools. Audit examines the outcome.

But between what should happen and what actually happens, there is a blind spot.

It exists in thousands of everyday decisions: a document created from the wrong template; an approval skipped because someone is in a hurry; a procurement requirement misunderstood; a mandatory field completed incorrectly; a policy interpreted differently by two teams; an AI agent taking an action its designers never anticipated.

Individually, these moments can appear insignificant. Collectively, they determine whether an organisation actually operates the way it intended.

The organisation does not become its strategy when the strategy is written. It becomes its strategy through millions of moments of execution. Those moments need assurance.

02. Compliance after the fact is too late.

Traditional assurance is often retrospective. We create policies. We train people. We establish controls. We conduct audits. We investigate failures. We produce reports. We remediate.

All of these things remain important. But increasingly, they are not enough.

Finding a mistake three months later does not undo the mistake. Discovering a pattern of non-compliance during an audit does not prevent the hundreds of decisions that created it.

The future of assurance must therefore move closer to the moment of work itself: from periodic to continuous; from retrospective to preventative; from sampling behaviour to observing execution; from documenting failure to helping prevent it.

The best time to identify an operational failure is before it becomes one.

03. Knowing is not the same as doing.

For decades, organisations have attempted to improve execution by giving people more information: another policy, another SOP, another training module, another email, another SharePoint page, another town hall.

But information alone does not create behaviour change. People can know the correct process and still not follow it. They can understand a policy and still forget it at the moment it matters. They can complete mandatory training and behave differently six months later.

This is not simply a knowledge problem. It is a behavioural problem.

Operational Assurance therefore cannot only be built on technology and controls. It must also be built on an understanding of human behaviour.

How do we make the right behaviour easier, clearer and more likely at the exact moment it matters?

04. Assurance must live inside the flow of work.

The employee should not have to leave their work to become compliant. The assurance should come to them.

Inside the document. Inside the workflow. Inside the enterprise system. Inside the conversation. At the decision point. At the approval point. At the moment of uncertainty.

Operational Assurance creates intelligent checkpoints across the flow of work. Sometimes the right intervention is a warning. Sometimes it is a reminder. Sometimes it is a recommendation. Sometimes it is an explanation. Sometimes it is a requirement for human approval. Sometimes it is simply making the correct action easier than the incorrect one.

The objective is not to create more friction.

Introduce the right friction at the right moment - and remove unnecessary friction everywhere else.

05. AI changes the scale of the problem.

The arrival of enterprise AI makes Operational Assurance urgent.

Until now, organisations primarily needed to assure the behaviour of humans. Increasingly, work will be performed by a combination of humans, AI copilots, AI agents, automated workflows, and systems acting on behalf of other systems.

AI dramatically increases the speed at which organisations can operate. It also increases the speed at which they can make mistakes.

An employee might make ten consequential decisions in a day. An autonomous agent may eventually make ten thousand.

This creates a new enterprise question: Who assures the agents?

An AI agent should not be considered reliable merely because it successfully completes a task. It must complete that task within the organisation's policies, controls, permissions, procedures and operational intent.

AI therefore needs more than intelligence. It needs boundaries. Context. Checkpoints. Escalation paths. Evidence. Assurance.

In the AI enterprise, Operational Assurance becomes the control layer between intelligence and action.

06. Humans and AI should operate under the same operational truth.

We reject the idea that organisations should build one governance universe for humans and another for AI.

There should be one operational reality.

The organisation's strategy, policies, controls, procedures, responsibilities and obligations should define how work gets done - regardless of whether that work is being performed by a person or an agent.

The interface may differ. The intervention may differ. The level of autonomy may differ. But the underlying operational expectations should not.

An organisation in which humans and AI continuously operate against the same version of operational truth.

07. Governance should become executable.

For too long, critical organisational knowledge has remained trapped inside documents. Policies describe rules. SOPs describe processes. Control frameworks describe requirements. Job descriptions describe responsibilities. Strategy documents describe objectives.

But machines cannot reliably govern operations from documents designed only to be read by humans.

The next generation of organisations will transform this knowledge into something executable. Requirements become rules. Processes become observable workflows. Controls become checkpoints. Responsibilities become permissions and escalation paths. Policies become machine-readable operational context.

Governance moves from the bookshelf into the architecture of the enterprise.

The future of governance is not merely documented governance. It is executable governance.

08. Every operational initiative should become measurable.

Operational Assurance should not merely enforce. It should learn.

Every intervention creates information. Where are employees struggling? Which policies generate the most confusion? Which processes are regularly bypassed? Where are unnecessary bottlenecks occurring? Which teams need additional support? Which interventions actually change behaviour? Where are AI agents repeatedly encountering ambiguity? Which controls are creating value - and which are simply creating friction?

This turns assurance into something more powerful than oversight. It becomes an organisational learning system.

Observe. Compare. Intervene. Measure. Learn. Improve. Repeat.

Every operational initiative becomes an experiment in making the organisation better.

09. Leaders should be able to influence behaviour, not merely measure it.

Enterprise dashboards have given leaders unprecedented visibility. But visibility without agency has limits.

It is not enough to tell a leader: "Your team has a compliance problem."

Operational Assurance should allow them to do something about it: identify the behaviour, understand why it is occurring, design an intervention, deploy it into the flow of work, measure the response, and adapt.

This creates a fundamentally different relationship between leadership and operations.

The dashboard stops being merely a place where leaders observe the organisation. It becomes a mechanism through which they can continuously improve it.

10. Transformation should not require replacing everything.

Organisations have already invested billions in enterprise technology: Microsoft, SAP, Oracle, Salesforce, ServiceNow, Google, custom applications, data platforms and AI platforms.

The answer cannot always be another massive transformation programme.

Operational Assurance should sit across the existing enterprise. It should connect systems rather than unnecessarily replace them. It should observe work wherever it occurs. It should provide intelligence where it is needed. It should strengthen the technology organisations already own.

Evolution, not revolution.

The objective is not another system of record. It is a system of assurance across the systems of record.

11. Assurance should enable ambition, not constrain it.

The purpose of Operational Assurance is not bureaucracy. It is confidence.

Confidence to move faster. Confidence to delegate. Confidence to automate.
Confidence to deploy AI. Confidence to transform. Confidence that increased speed does not require abandoning control.

The organisations attempting the world's most ambitious transformations should not have to choose between innovation and assurance. They should be able to have both.

In fact, the more ambitious the organisation becomes, the more important Operational Assurance becomes.

Control should not be the enemy of speed. Done correctly, control is what makes speed possible.

WE BELIEVE.

We believe Strategy without execution is aspiration.

We believe Governance should exist where work happens.

We believe Assurance should prevent failures, not merely document them.

We believe Policies should become executable.

We believe Compliance should become easier for employees, not harder.

We believe Behavioural science belongs inside enterprise technology.

We believe Leaders should be able to influence operational behaviour continuously.

We believe AI agents must be assured just as rigorously as human employees.

We believe Humans and AI should operate against the same organisational truth.

We believe Every intervention should generate learning.

We believe Organisations should improve continuously through the evidence created by everyday work.

We believe Assurance should increase the speed at which organisations can safely operate.

We believe A new enterprise capability is required to make this possible.

OPERATIONAL ASSURANCE

The continuous process of ensuring that human and AI activity remains aligned with an organisation's policies, processes, controls, responsibilities and strategic intent - during the execution of work, not merely after it.

It is the layer between governance and execution.

Between strategy and behaviour.

Between intelligence and action.

Between what the organisation says should happen and what actually happens.

As AI transforms the enterprise, this layer will become fundamental. Because the defining question of the next generation of organisations will not simply be:

"How intelligent are our people and our systems?"

It will be:

"Can we trust them to act as intended?"

That is the problem Operational Assurance exists to solve.

THE AGE OF OPERATIONAL ASSURANCE HAS BEGUN.