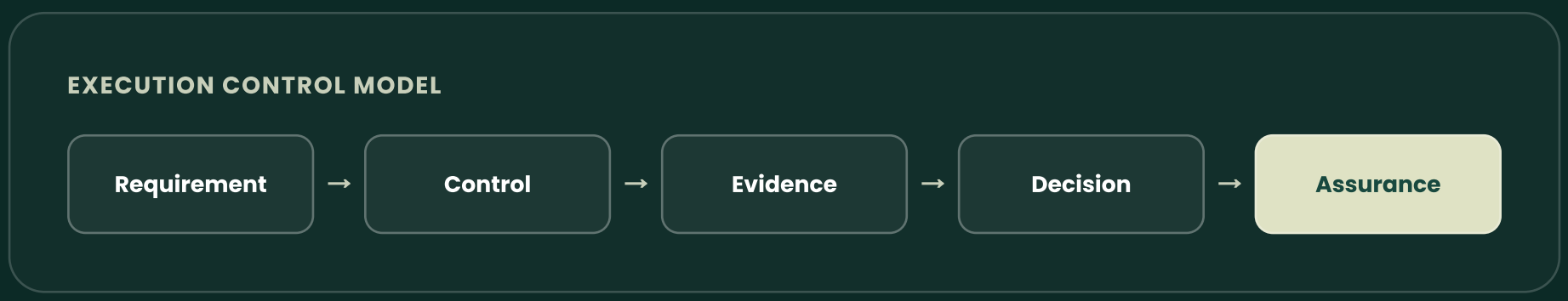
CORGENTA

Cyber Delivery Tax Brief

Why industrial organisations pay an invisible tax on OT cybersecurity delivery



A Corgenta Executive Insight Brief

01

Executive Summary

Industrial organisations invest heavily in OT cybersecurity, but many still struggle to prove that cybersecurity is being delivered consistently across projects, suppliers and operational environments.

The issue is rarely a lack of intent. It is usually a delivery problem. Cybersecurity work becomes fragmented across teams, spreadsheets, suppliers, emails, reports and approval routes. Each gap adds cost, delay and uncertainty.

> **Cybersecurity programmes rarely fail because organisations do too little. They fail because they cannot consistently execute, govern and prove what they are already trying to do.**

We call this hidden cost the Cyber Delivery Tax.

Why good programmes fail

Activity does not automatically create assurance.

Where the tax appears

Governance, engineering, supplier and audit friction.

Why GRC is not enough

Documentation alone does not govern execution.

How Execution Control works

Requirements, controls, evidence and decisions stay connected.

How to act

Recognise the pattern and assess the gap.

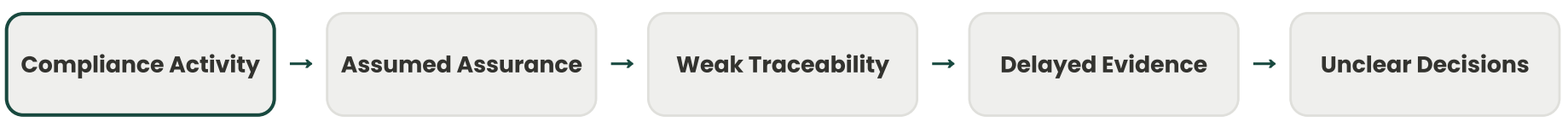
02 The Hidden Assumption Behind Most Cybersecurity Programmes

Many organisations assume that assurance follows naturally from compliance activity. The common belief is that if requirements are understood, assessments are completed, controls are assigned, evidence is collected and reports are produced, assurance will follow.

In industrial environments, that assumption is weak. OT cybersecurity is delivered through projects, engineering teams, suppliers, integrators, asset owners, contractors and governance bodies. Work moves across organisational boundaries. Evidence is produced by different parties. Decisions are made at different levels.

In that environment, compliance activity alone does not create assurance. Assurance requires controlled execution.

ASSUMPTION GAP



03 Why Good Cybersecurity Programmes Still Fail

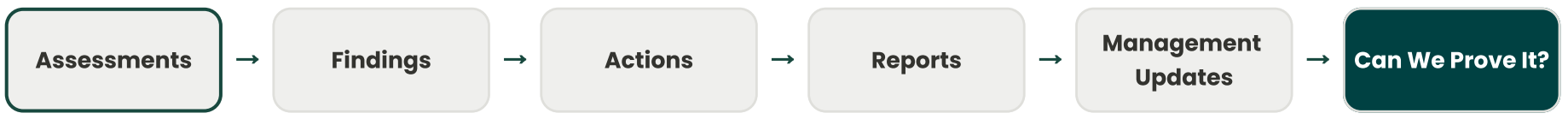
Many cybersecurity programmes are active, funded and staffed. The teams are often competent. The controls may be valid. The standards may be clear.

Still, executives struggle to answer simple questions:

- Which controls have been implemented?
- Who accepted the evidence?
- Which suppliers are late?
- Which risks remain open?
- Which decisions were made, and by whom?
- Can we prove this position now, without audit preparation?

When answers require meetings, manual checks or document searches, the programme does not have assurance. It has activity.

ACTIVITY WITHOUT ASSURANCE

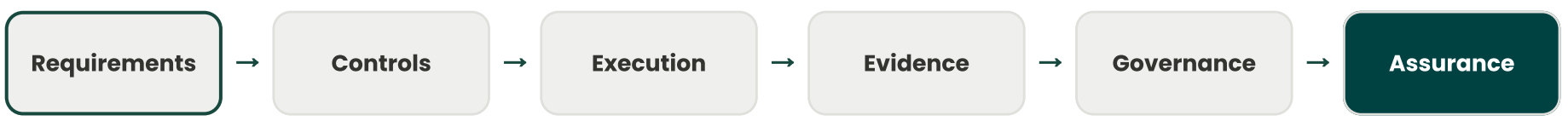


04 The Missing Layer: Execution

Most organisations can describe their cybersecurity requirements. Many can list their controls. Some can show evidence during an audit. The missing layer is execution.

Execution connects what must be done to how it is delivered, evidenced, validated and approved. Without this layer, organisations are forced to manage cybersecurity through coordination rather than control. That creates friction and uncertainty.

THE MISSING EXECUTION LAYER



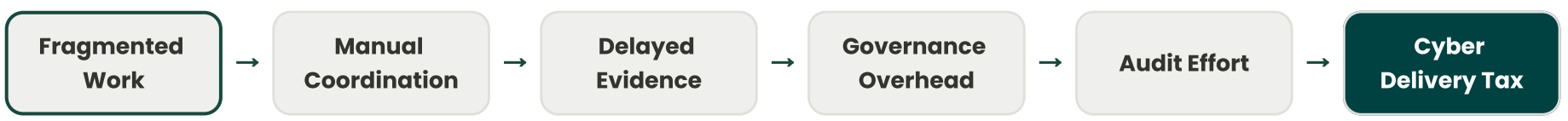
The issue is not whether cybersecurity work is happening. The issue is whether the work can be traced, governed and proven as it happens.

05 Introducing the Cyber Delivery Tax

Cyber Delivery Tax is the hidden operational cost created when cybersecurity delivery cannot be executed, evidenced and governed consistently across teams and organisations.

It is not a formal financial tax. It is paid through duplicated effort, repeated evidence requests, manual reporting, supplier coordination overhead, delayed approvals, audit preparation cycles, unclear ownership and low confidence in reported status.

CYBER DELIVERY TAX BUILD-UP



The tax grows when delivery becomes complex.

More projects, suppliers and approval routes mean more coordination friction.

The tax grows further when multiple organisations are involved.

Interface failures compound evidence, ownership and decision gaps.

06

Where the Tax Appears

The Cyber Delivery Tax is usually not visible as a single budget line. It is spread across operational friction.

Governance Tax

- Approval decisions made through email
- Inconsistent decision records
- Steering meetings used to find status
- Repeated questions about ownership

Engineering Tax

- Duplicate evidence requests
- Manual evidence packaging
- Repeated spreadsheet updates
- Engineers preparing status slides

Supplier Tax

- Inconsistent supplier evidence formats
- Weak traceability across contracts
- Late or incomplete submissions
- Assurance gaps at handover points

Audit Tax

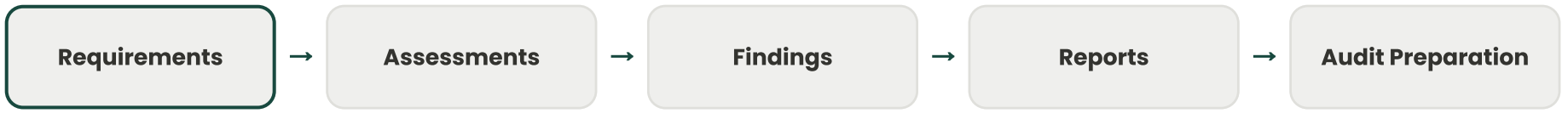
- Audit preparation takes weeks
- Evidence is collected before review
- Findings are debated due to weak traceability
- Historical decisions are difficult to defend

07 A Different Operating Model

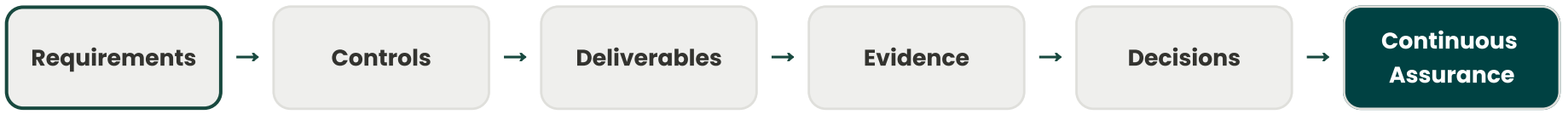
Traditional approaches often manage cybersecurity through assessments, reports and periodic audit preparation. That model can document activity, but it does not reliably govern execution.

A stronger model connects requirements, controls, deliverables, evidence and decisions as work is performed.

BEFORE: COMPLIANCE DOCUMENTATION MODEL



AFTER: EXECUTION-BASED ASSURANCE MODEL



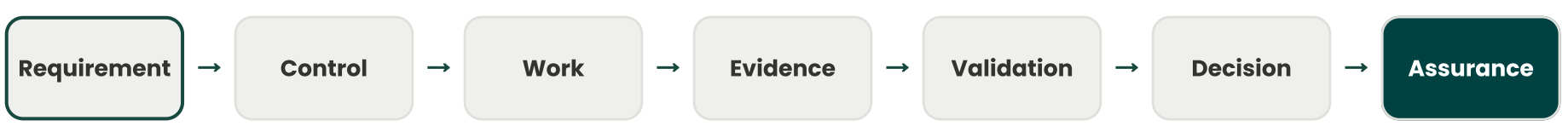
Instead of preparing assurance later, the organisation produces assurance as delivery happens.

08 Execution Control: The Corgenta Approach

Execution Control is the way Corgenta manages OT cybersecurity delivery. It connects requirements, controls, work, evidence, validation and decisions into one controlled execution model.

Governance is not treated as a separate reporting layer. Evidence is not treated as a late-stage audit task. Approvals are not treated as disconnected emails. They become part of the delivery process.

CORGENTA EXECUTION CONTROL MODEL



Execution Control helps organisations:

- maintain traceability from requirement to decision
- make evidence part of delivery
- control supplier and contractor submissions
- strengthen governance accountability
- reduce manual coordination
- improve readiness for audit and regulatory review

09

What Changes When Execution Is Controlled

When execution is controlled, the operating model changes. Standards, policies and audits remain important, but they become executable.

Before	After
Evidence is collected late	Evidence is generated during delivery
Status is reconstructed manually	Status is linked to execution records
Approvals sit in emails	Decisions are traceable
Suppliers report differently	Suppliers work against a common model
Audit readiness is prepared	Audit confidence is continuously produced
Governance reacts to issues	Governance controls the delivery path

10

Is Your Organisation Paying the Cyber Delivery Tax?

Most organisations pay some level of Cyber Delivery Tax. The key question is whether it is visible, understood and actively managed. Use the following questions as a quick recognition check.

Question	Yes	No
Can you trace each cybersecurity requirement to implemented controls?	☐	☐
Can you identify who owns each control and evidence item?	☐	☐
Can you prove current control status without manual evidence collection?	☐	☐
Can supplier evidence be assessed consistently?	☐	☐
Are governance approvals linked to the evidence available at the time?	☐	☐
Can executives see delivery risk without waiting for a report cycle?	☐	☐
Can audit evidence be produced without a separate preparation exercise?	☐	☐
Are project, supplier and governance records connected?	☐	☐

If several answers are "No", the organisation is likely paying a material Cyber Delivery Tax.

11 Why This Matters Now

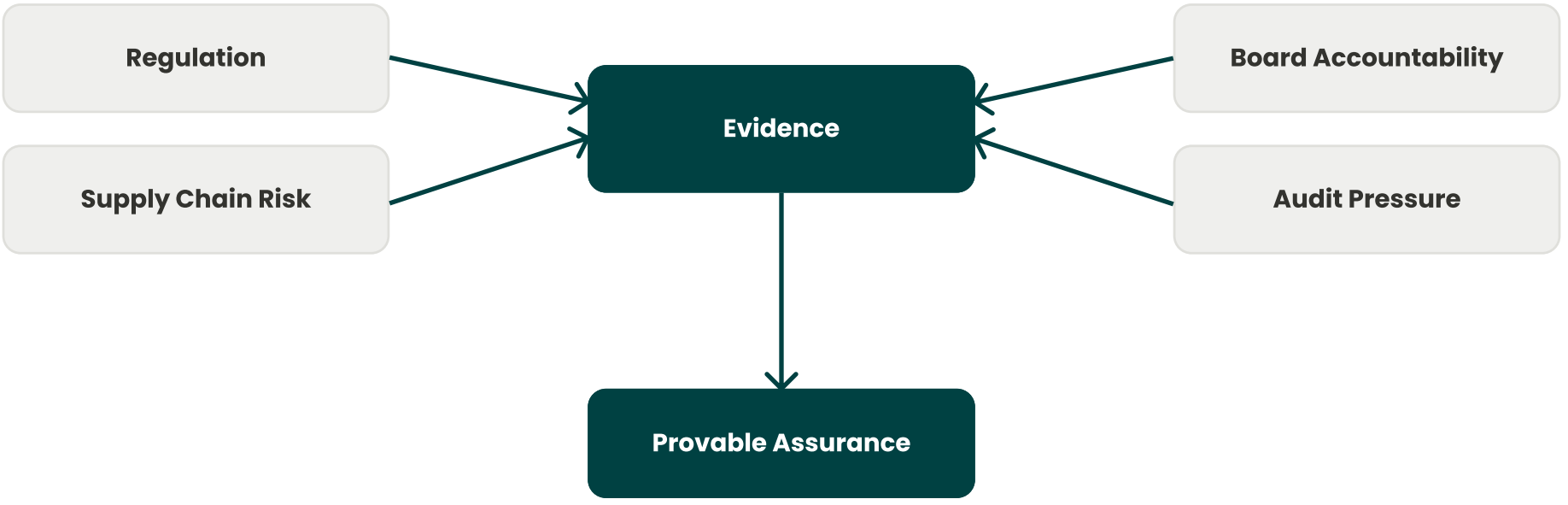
The pressure on OT cybersecurity is changing. Regulators, boards, insurers, customers and supply-chain partners increasingly expect organisations to demonstrate more than intent.

They expect evidence of:

- accountability
- decision-making
- operational resilience
- supplier control
- risk treatment
- continuous assurance

The organisations that improve fastest will not be those that create more reports. They will be those that make cybersecurity delivery executable, evidenced and governable.

ASSURANCE PRESSURE



12 If You Recognised It, Act on It

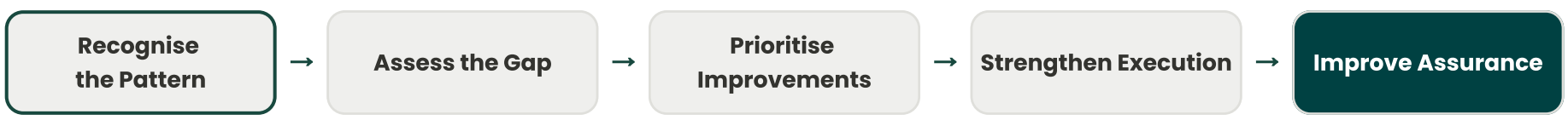
If the situations described in this brief reflect your own experience, the issue is worth examining before it becomes more expensive.

Many organisations only discover the scale of the problem during an audit, a project delay, a supplier dispute or a regulatory review. By then, the Cyber Delivery Tax is already being paid.

A structured review helps make the issue visible earlier. It can help your organisation:

- identify hidden delivery friction
- understand where governance slows or weakens execution
- find evidence gaps before they become audit findings
- expose supplier and contractor handover weaknesses
- clarify where accountability is strong or weak
- prioritise improvements based on risk and business value

FROM RECOGNITION TO ACTION



13 Request a Cyber Delivery Gap Review

A Cyber Delivery Gap Review provides a structured assessment of how cybersecurity is executed across your organisation, programmes and projects.

It examines where execution friction, governance overhead, supplier interface gaps and assurance weaknesses are accumulating.

- Governance and decision-making
- Execution workflows
- Control ownership
- Evidence lifecycle
- Supplier and contractor interfaces
- Approval traceability
- Continuous assurance capability

REVIEW OUTCOME

14 About Corgenta

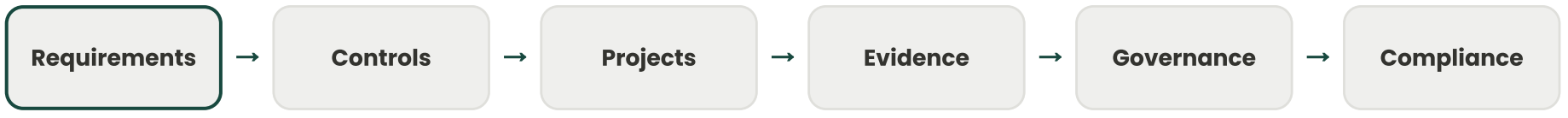
Corgenta is an OT Governance, Risk and Compliance execution platform.

It helps organisations manage cybersecurity delivery across requirements, controls, projects, evidence, governance and compliance.

Corgenta is designed for industrial environments where assurance depends on controlled execution across multiple teams, suppliers and delivery organisations.

Its purpose is to help organisations move from fragmented cybersecurity activity to governed, evidenced and decision-ready assurance.

CORGENTA PLATFORM SPINE



If cybersecurity cannot be executed, governed and proven consistently, the organisation pays for the gap one way or another.

The practical question is whether that cost remains hidden or becomes actively managed.

Next step: Request a Cyber Delivery Gap Review to identify where execution friction, governance gaps and assurance weaknesses are accumulating.