SoftCo

The supplier control framework

A standard for active control across the supplier lifecycle.

AUTHOR

Robert Hickey

Chief Knowledge Officer, SoftCo

PUBLISHED

September 2026

CONTENTS

01

Why this framework matters now

For the last decade, the conversation about payables has been about speed. Throughput, automation rate, touchless processing, invoices per head, days to pay. Most finance teams have moved those numbers a long way, and they were right to. The efficiency gains were real.

But speed was never the thing that kept finance leaders awake. Ask a CFO what they worry about and the answer is rarely the volume getting through. It is the audit.

> “If an auditor asked how a payment was approved, could you explain it, end to end?”

The question that really matters

Throughput is a number to be managed; a failed audit is a conversation with the board. The person who signed off the process is the one who answers for it, often long after the people who ran it have moved on. So when external auditors examine how a particular, potentially fraudulent, payment came to be made, the explanation has to hold from start to finish, without anyone reconstructing it after the fact. That is the test this framework is built around.

The relevant question is not whether the invoice can be located. It is whether the full path can be traced, each step evidenced in sequence:

> Who the supplier is, and how that was verified.
>
> What they were approved to supply, and at what price.
>
> What the invoice was matched against.
>
> How the receipting was validated.
>
> Who released the payment, and whether that was the same person who entered it.

When that explanation comes together cleanly, the lifecycle is controlled. When it has to be pieced together across several systems, and there is a gap no one can quite account for, the lifecycle is not. That gap is the subject of this framework.

Why the gap exists

The cause is structural. For most of the last decade, the unit of control was the invoice: a document moving through the system, checked at the point it arrived. That model is no longer enough. The unit of control is now the supplier behind the invoice, its bank details, its tax status, its approval path, its inclusion on any sanctions list, and whether it is still the supplier that was onboarded or has since changed in ways no one recorded.

Trace almost any fraud, duplicate payment, or audit gap back to its origin and the root is seldom a bad invoice. It is a supplier whose details, status, or behaviour stopped being watched. This is compounded by a simple fact: automation has moved faster than oversight. Many controls in place today were designed for a manual, invoice-by-invoice era and validated once, on the day they went live. They still run. Whether they still hold is a question rarely revisited since.

The cost lands downstream

A weak control rarely fails where it was set. It fails downstream, at the most expensive possible point. A supplier changes its bank account and gives notice, but the record is never updated. Weeks later an invoice arrives, the details do not match, and a task that should take thirty seconds takes thirty minutes, corrected under pressure with a payment waiting. The control worked. It simply fired far too late to be cheap.

And what is true of one bank detail is true across the lifecycle: the longer a problem goes unseen, the more it costs to put right.

What a controlled lifecycle is

Most organisations treat control as a final gate, with checks accumulating toward the moment of payment. It is the wrong shape. By the time a payment is ready to be made, almost every decision has already been made, and reversing any of them is slow, expensive, and often impossible.

A controlled supplier lifecycle is not a gate. It is a continuous thread, running from the first commitment to the moment the books are reconciled. It is a bit like airport security, where the bag, the person, and the passport are each checked separately: no single check carries the whole load, and the strength of the system lies in the sequence, not in any one point of it.

> “A controlled lifecycle is not the absence of risk. It is the presence of evidence: the ability to stand over every step, in sequence, when asked to.”

This is a standard for what good looks like, not a description of any single system that delivers it. No vendor, SoftCo included, delivers every element today. It is offered as a reference point for finance leaders building toward continuous, supplier-centric control. What follows sets out each stage in turn. The process runs in a line, from contracting to post-payment, but the control model laid over it does not: the same kinds of control recur at stage after stage.

02

The stages of the supplier lifecycle

Act one: Commit

The first three stages. This is where the organisation commits money, before any invoice exists. Get these right and most of what follows takes care of itself.

STAGE 1

Contracting

The commercial baseline

"Is there a valid, current contract for this supplier and this spend, and are its terms structured well enough to be used downstream?"

WHAT GOOD LOOKS LIKE

- Terms are structured, not just filed, so later stages can check against them automatically
- The baseline is current, with amendments and renewals tracked
- The contract is linked to the supplier and the spend it governs

WHERE IT BREAKS

The contract exists but is locked in a PDF, so no downstream control can reach it

STAGE 2

Supplier onboarding

The golden source

"Is this supplier a verified, legitimate entity, set up by the right people, with bank details confirmed to belong to them?"

WHAT GOOD LOOKS LIKE

- Identity confirmed against external registries and screened against sanctions
- Bank details verified to belong to the supplier, the highest-risk field in the record
- The record built under segregation of duties, with every change approved and reasoned

WHERE IT BREAKS

Onboarding is manual and unverified, so the record exists but was never actually validated

STAGE 3

Purchasing

Commitment control

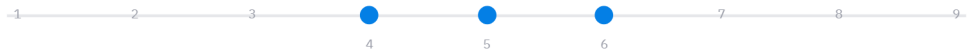
"Was this purchase authorised, made through an approved process, and placed with an approved supplier and contract?"

WHAT GOOD LOOKS LIKE

- Spend is directed to approved suppliers, enforced at the point of purchase
- Authority is checked before the commitment is made, not ratified after
- PO data is clean and detailed, so matching later has something precise to check against

WHERE IT BREAKS

Maverick buying: the approved supplier exists and someone orders elsewhere anyway



Act two: Process

The commitment is made. Now the work arrives and is checked against everything established upstream.

STAGE 4

Receipt

Delivery validation

"Were the goods or services actually received, recorded by someone authorised to confirm them, before the invoice was approved for payment?"

WHAT GOOD LOOKS LIKE

- Receipt is confirmed before approval, so payment rests on confirmed delivery
- The person confirming has the authority to do so, and the confirmation is real
- It enables a genuine three-way match against the PO and the invoice

WHERE IT BREAKS

Receipt is skipped under volume pressure, and the invoice is approved on trust

STAGE 5

Invoice capture and validation

The liability gateway

"Is this a valid, original invoice from a verified supplier, consistent with what was ordered, received, and agreed?"

WHAT GOOD LOOKS LIKE

- Every invoice is checked for duplication, the most reliable control in payables
- Validation is contextual, checked against the supplier, PO, receipt, and contract together
- Tax and compliance are validated at entry, before anything enters the ledger

WHERE IT BREAKS

The duplicate check is trusted into invisibility, until the one time it is missed

STAGE 6

Matching and approval

The decision engine

"Can this invoice be approved on a basis that can be explained and replayed for an auditor, by someone with the authority to approve it?"

WHAT GOOD LOOKS LIKE

- Matching is contextual and tolerant, distinguishing a rounding difference from a real discrepancy
- Decisions are deterministic and explainable, the same inputs giving the same result every time
- Authority is real and segregated: the person who processes is not the one who releases

WHERE IT BREAKS

Segregation of duties collapses under pressure, existing only in the policy document

Act three: Settle

Two stages. The cash leaves, and the books are closed and checked. The highest-stakes moment, and the safety net beneath it.

STAGE 7

Payment release

The final cash control

"Is this payment going to the right supplier, at the right account, for a validated and approved invoice, with nothing changed since it was approved?"

WHAT GOOD LOOKS LIKE

- The release is separated from the approval, carrying its own distinct control
- Bank details are re-checked against the verified record at the point of release
- Anomalies in the payment pattern are surfaced before the payment executes

WHERE IT BREAKS

Release is treated as a rubber stamp, so the one item that changed moves through unexamined

STAGE 8

Post-payment and reconciliation

The closed loop

"Did we pay the right amount, once, for everything we owed, and do our records reconcile against what suppliers say we owe them?"

WHAT GOOD LOOKS LIKE

- Payments are reconciled against an independent source, such as supplier statements
- Completeness is tested, looking for missing invoices and uncaptured accruals
- Recurring problems feed back upstream to strengthen the control that should have caught them

WHERE IT BREAKS

Recovery quietly becomes the strategy, instead of fixing the upstream gaps that cause the errors

Act four: Sustain

One stage. Everything before this point happens at a moment in time. Supplier lifecycle management happens continuously, maintaining control as suppliers, risks and circumstances change.

STAGE 9

Supplier lifecycle management

Continuous control

"Is this supplier still valid, compliant, and behaving as expected today, not only on the day it was first approved?"

WHAT GOOD LOOKS LIKE

- Suppliers are re-validated on a cadence and in response to risk, not just at entry
- A change to ownership, sanctions status, or bank details triggers re-verification rather than being absorbed silently
- Offboarding is a controlled act, so a dormant supplier cannot be used as a route to transact

WHERE IT BREAKS

Verified once, trusted indefinitely: the onboarding check is treated as permanent and never revisited

A supplier verified yesterday is not necessarily a supplier verified today.

A control that is never re-tested is, in the end, only an assumption.

03

How control runs across the supplier lifecycle

The previous section followed the supplier lifecycle one stage at a time. This section looks across it instead. The strongest controls are not confined to a single stage; they run throughout the lifecycle, recurring wherever they are needed. There are six types of control, each answering a different question. Together they provide a different way of reading the supplier lifecycle before the matrix maps where each one is most active.

Financial control — *Is the number right?* Validates financial accuracy against the purchase order, contract or other agreed basis for payment.

Compliance control — *Are we within the rules?* Ensures supplier obligations, tax, sanctions and policy compliance remain current through continuous re-validation.

Fraud and risk control — *Is this supplier, invoice and behaviour genuine?* Combines prevention and detection to identify bad actors, bad data and suspicious activity before money leaves the business.

Governance control — *Was this action authorised?* Enforces approval authority and segregation of duties at every decision point, not simply through documented policy.

Data integrity control — *Can the underlying data be trusted?* Maintains a single source of truth against which supplier and transaction data can always be verified.

Operational control — *Is the process performing effectively?* Monitors throughput, exceptions and bottlenecks to identify where controls are becoming strained.

The matrix overleaf maps the six control types across the supplier lifecycle. Read each row from left to right to see where control is strongest, where it supports other controls, and where gaps begin to emerge.

See the control matrix ⟶

Mapping control activity across the supplier lifecycle

The matrix maps the six control types across the supplier lifecycle. It is a reference standard, showing where control should be strongest in a well-controlled organisation rather than the capability of any single system.

CONTROL TYPE	1 Contracting	2 Onboarding	3 Purchasing	4 Receipt	5 Invoicing	6 Matching	7 Payment	8 Post-payment	9 Lifecycle
Financial *Is the number right?*	●	○	◑	◑	●	●	●	●	○
Compliance *Are we within the rules?*	◑	●	◑	○	●	◑	●	◑	●
Fraud and risk *Is this real, and is it safe?*	○	●	◑	◑	●	◑	●	◑	●
Policy and governance *Was this allowed, and by whom?*	◑	◑	●	◑	○	●	●	○	◑
Data integrity *Can we trust what we are looking at?*	◑	●	◑	◑	●	◑	◑	◑	●
Operational *Are we getting through the volume?*	○	◑	◑	◑	●	●	◑	●	◑

Read each row from left to right. The pattern shows where each control type is strongest, where it supports other controls, and where it naturally thins across the supplier lifecycle.

04

Where control most often breaks

The matrix shows where control should be active. It cannot show whether that control actually holds. A circle on a grid says a check exists; it says nothing about whether the check still works, or whether anyone is watching it. This section is about the difference, the ordinary ways that controls which look sound on paper turn out to be hollow in practice.

None of what follows is exotic. These are not rare failures or sophisticated attacks. They are common precisely because each one is easy to miss. A control does not have to be absent to fail. It only has to be unwatched, untested, or quietly bypassed, sometimes by circumstance, sometimes by the organisation's own people. Five patterns account for most of it.

01

Master data drift

A supplier detail changes in the world before it changes in the system, and the gap between the two is where the damage sits. An invoice arrives, a control flags that something no longer matches the record, and the correction has to be made at the worst possible moment, under pressure, with a payment waiting. The control worked. It just fired far too late to be cheap, because the record it checks against was allowed to fall out of date. This is what happens when data integrity is treated as a one-time setup rather than something maintained, and it is the most frequent failure in payables.

02

Controls validated once

Onboarding passes on day one. The supplier is verified, the bank details confirmed, the sanctions screen clear. Six months later none of it has been looked at again, and the supplier is still treated as verified. But suppliers do not hold still. Ownership shifts, details change, status changes, and a verification that is never repeated slowly stops meaning anything. A control that is not re-tested is not really a control. It is a record that something was once true. The remedy is not constant manual review but re-checking that fires on its own: whenever a new document arrives, whenever master data is updated, and on demand, so that anyone can re-test a supplier before approving an invoice or a contract that depends on it.

03 Maverick buying

The right supplier was approved. Someone bought from a different one anyway, because it was quicker, or cheaper that week, or because they did not know the rule. The failure surfaces later and awkwardly: an invoice arrives with no contract, no purchase order, and no agreed price to check against, and the whole downstream apparatus has nothing to validate it with. The control was not weak. It was bypassed, and a bypassed control fails just as completely as a missing one. The discipline that prevents it can be as blunt as a firm no PO, no pay: if the commitment was never made through the proper channel, the invoice does not get paid until it is.

04 The duplicate that gets through

Duplicate detection is the most reliable control in payables, which is exactly why teams stop watching it. It works so consistently that it fades into the background, and a control nobody watches is a control nobody notices failing. The stakes are not small. Invoices run to millions, and a missed duplicate means paying one twice. What follows is not a system fix but a phone call, asking a supplier to return money it may have already spent. The control earns its keep on every ordinary day it appears to do nothing, and the one day it is skipped is the day that pays for all the rest, in money, and in confidence that the process can be trusted at all.

05 Collusion-shaped gaps

Segregation of duties keeps the person who processes an invoice apart from the person who releases the payment. On paper the separation is clean. In practice it bends under exactly the conditions where it should hold firmest: volumes spike, someone is on leave, and the two roles collapse into one set of hands to keep the queue moving. The separation still exists in the policy document. It has stopped existing in the work. Because it happens for practical reasons, with no ill intent, it is rarely noticed, and a defence against fraud is only a defence while it is maintained.

These five have something in common. In every case the control was present. None of this is a story about an organisation with no controls. They are stories about controls that worked in isolation, were validated once, and were not connected to anything that kept them honest over time. That is the gap the next section sets out to close.

05

The seven principles of a controlled supplier lifecycle

A controlled supplier lifecycle is not the product of individual controls. It is the result of seven principles, applied consistently.

1 **Push controls upstream.**

Fix problems where they are cheapest to resolve—close to the supplier, not at the point the cash leaves.

2 **Control the supplier, not the invoice.**

Most fraud, duplicate payments and audit failures begin with the supplier record, not the invoice itself.

3 **Validate, don't assume.**

A control that passed yesterday says nothing about today. Re-validation keeps control honest.

4 **Make every decision explainable.**

Every decision to pay should be supported by evidence that can be understood and replayed.

5 **Segregate duties, especially under pressure.**

Controls matter most when workloads increase. Authority should never collapse when the business is busy.

6 **Treat evidence as a by-product, not a task.**

Strong controls generate their own audit trail as they operate.

7 **Connect the controls.**

Individual checks do not create control. Connected controls create a controlled supplier lifecycle.

Control is not a series of checks.
It is a connected system of evidence.

06 SECTION SIX

Automated does not always mean controlled

A word, finally, on the technology that sits behind all of this now. Most payables operations are automating faster than ever, and the next wave of automation is driven by AI: faster, more complex, and able to make far more decisions without a person involved. The temptation is to read that as control solved. It is the opposite.

Automation moves the work. It does not remove the need to govern it. It changes where the control has to sit. A faster process makes more decisions in less time, which means more decisions to account for, not fewer. An automated check that cannot explain itself is not a control. It is a guess made at speed.

> **AI changes the scale, not the standard.**
>
> AI can make more decisions, more quickly, than any human process. That increases the importance of explainability, evidence and continuous control. It does not reduce it. The same standard applies whether a decision is made by a person or by a machine.

This is why everything in this framework matters more as automation advances, not less. The same standard applies to a machine decision as to a human one: it must be explainable, it must be reviewable, and it must be reproducible for an auditor after the fact. The faster and more capable the system, the more it has to show its working, because the cost of an ungrounded decision now scales with the speed of the system making it.

Sophisticated automation does not reduce the need for grounded control.
It raises it.

07 SECTION SEVEN

Towards greater control across the supplier lifecycle

The last decade of payables was about speed. The efficiency was won, the processes were automated, and the numbers moved a long way. The next phase will be about control, underpinned by business intelligence, reporting, auditing, and normalisation. Anything outside the norm should be flagged. Not because speed stops mattering, but because automation has quietly outpaced the controls built to govern it, and that gap is now the thing worth closing.

This is the direction the industry is moving in, and the organisations that move early will find it far easier than those that wait until an auditor, a duplicate payment, or a diverted account forces the question.

> Behind every control is a person who will, one day, be asked to account for a payment.
>
> A controlled supplier lifecycle makes the answer simple.

The framework in these pages is a map of where control needs to run and where it tends to thin out. The most useful next step is to hold your own lifecycle up against it.

That is rarely a solo exercise. A structured review with someone who has seen how control succeeds and fails across many environments will surface more, and surface it faster, than an internal audit working from first principles.

A NOTE ON WHAT THIS FRAMEWORK DOES

The goal of this framework is to establish a consistent best-practice approach to managing risk and control across the supplier lifecycle. It is intended as a reference point for finance leaders building towards continuous control, and who are intent on keeping pace with the rate of change.

It is a standard, not a product description. No vendor delivers every element of it today.

RH

ABOUT THE AUTHOR

Robert Hickey

Chief Knowledge Officer, SoftCo

Robert Hickey has spent his career close to how finance teams process invoices, across hundreds of customer environments. The examples in this document are drawn from that experience, not from theory.

Financial control
begins long before the invoice.
It begins with the supplier.

SoftCo

THE SUPPLIER CONTROL FRAMEWORK