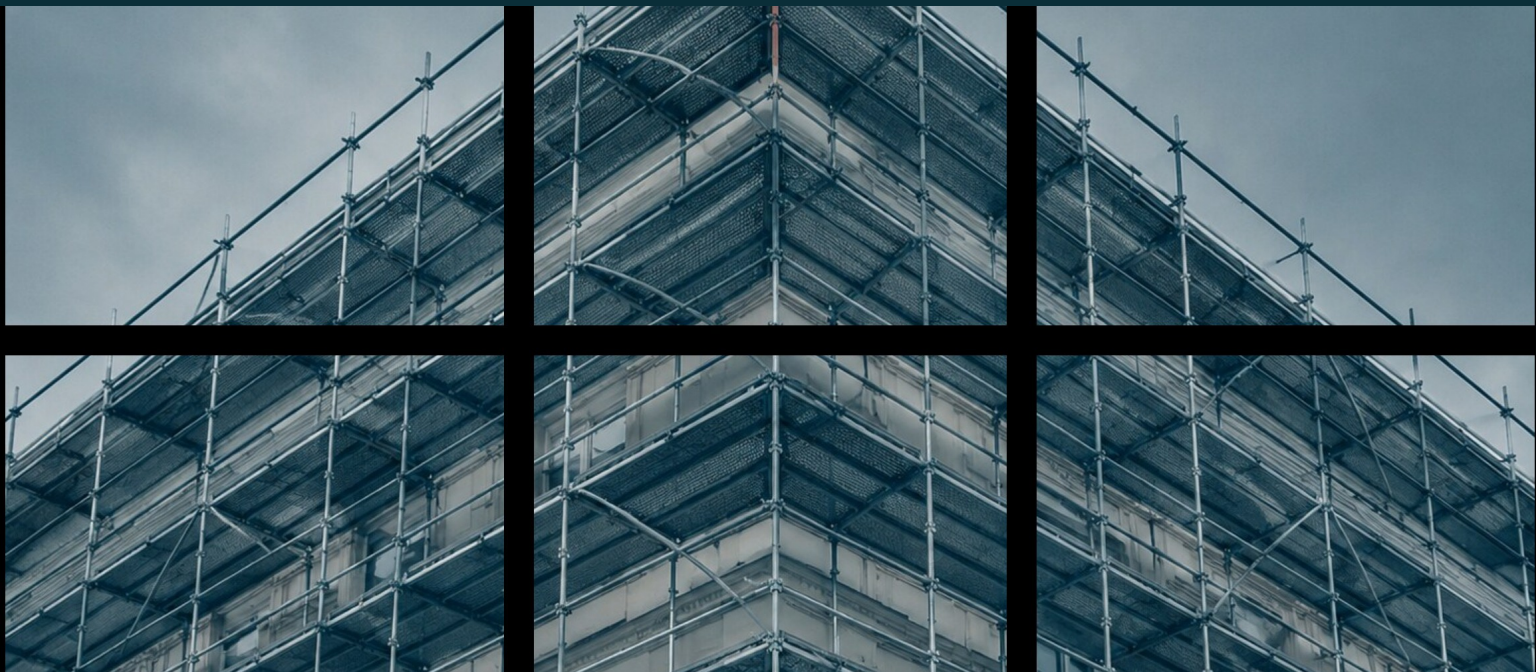


BEYOND THE DEADLINE

Sarbanes-Oxley Cannot Succeed as a Compliance Project

Why financial control reform must outlive the deadline that started it



Sarbanes-Oxley Cannot Succeed as a Compliance Project

Transformation · No. 29

Originally written April 2003 | Re-edited and re-rendered for the WhereBeyond Edition, 2025

“The programme has not discovered 684 sources of assurance. It has discovered 684 statements requiring judgement.”

1. The Sign-Off Meeting

The finance director places a twelve-page certification pack on the table. Every box is complete. The chief information officer confirms that access reports have been produced. Internal audit confirms that the required interviews took place. The programme manager confirms that all 684 documented controls have an owner.

Then the controller asks a simple question: which of those controls would prevent an unauthorised journal from entering the consolidation?

The room cannot answer without consulting three binders and four separate teams.

This is the central danger in the first wave of Sarbanes-Oxley work. Organisations are mobilising with appropriate urgency, yet many are treating compliance as a project whose product is evidence. The Act demands something more consequential: management must be able to understand, assess and stand behind the controls on which financial reporting depends.

A project can prepare an organisation for a deadline. It cannot, by itself, create a lasting control capability.

2. The New Transformation Mandate

Sarbanes-Oxley is frequently described as a finance or audit requirement. That description is too narrow. Financial statements are assembled through operational processes, enterprise systems, spreadsheets, batch interfaces, access permissions and manual adjustments. The reliability of the reported number depends on the reliability of that chain.

Section 302 has already made executive certification an immediate management concern. Section 404 points toward a more demanding obligation: management assessment of internal control over financial reporting, accompanied by external attestation. Whatever the final practical detail of implementation, the direction is clear. Assertions about control must be supported by an inspectable system of responsibility and evidence.

For many organisations, this is their first mandatory technology transformation. The trigger is regulatory, but the work crosses finance, operations, information technology, internal audit and external audit. It requires common definitions, traceable process maps, rationalised access, dependable records and repeatable testing.

That combination explains why conventional compliance management is insufficient. Legal interpretation can define the obligation. Audit can test control design and operation. Only management can make the control environment workable every day.

A control that exists only when the compliance team asks for evidence is not an operating control. It is a rehearsal.

3. What the Project Model Gets Right

The strongest argument for a project-led response deserves serious weight.

The obligations are new. Timetables are tight. The organisation needs clear scope, dedicated resources, named deliverables and disciplined escalation. A central programme can impose a common method where business units otherwise interpret the Act differently. It can build an inventory quickly, coordinate advisers, manage dependencies and give the audit committee a visible line of sight.

Without this mobilisation, the response may fragment. Each division may document different things at different levels of detail. Information technology may remediate access without understanding which financial assertions matter. Finance may describe controls without identifying the systems that execute them. External audit may receive inconsistent evidence too late to resolve disagreements.

A project is therefore necessary. The mistake is assuming it is sufficient.

Projects optimise for a defined end-state and a closure date. Controls operate through recurring accounting cycles, staff changes, system releases, acquisitions, reorganisations and changes in accounting treatment. The work does not become stable merely because the first assessment is complete.

If the project owns the control inventory, the testing calendar and the evidence files, the organisation becomes compliant through temporary machinery. When that machinery is dismantled, the capability leaves with it.

4. The Anatomy of the Failure

The pattern usually develops through five steps.

1. The control universe expands without a governing logic. Teams document everything that appears relevant because omission feels riskier than excess. The inventory grows faster than anyone can challenge it.
2. Documentation substitutes for design. A narrative states that a reconciliation occurs, but does not specify the threshold, evidence, reviewer or treatment of exceptions.
3. Technology is treated as a supporting workstream. System access, program changes, interfaces and computer operations are recorded separately from the financial controls that depend on them.
4. Testing is organised as an annual event. Samples are gathered in a concentrated exercise, frequently after the people who performed the control have forgotten the circumstances.

5. Remediation is measured by closure. An issue is considered complete when a new procedure is approved, not when the control has operated reliably through a reporting cycle.

The mechanism is cumulative. An oversized inventory consumes testing capacity. Weak specifications create inconsistent evidence. Separation between finance and technology hides dependencies. Late testing leaves little time to correct defects. Administrative closure then protects the timetable while preserving uncertainty.

The result may look industrious and still fail the management test: can the organisation explain, with confidence, why its reported numbers are controlled?

5. A Composite Diagnostic

Consider a composite manufacturing group with six divisions, eleven principal financial applications and more than forty feeder systems. Its first inventory contains 684 controls. The programme reports 91 per cent documentation complete after four months.

A closer review of the revenue process finds 73 controls. Twenty-one describe reports produced by systems but do not identify who verifies that the reports are complete. Fourteen are variations of the same divisional reconciliation. Nine merely restate job responsibilities. Six depend on spreadsheets whose formulas are neither protected nor independently checked.

Only 23 controls directly address a financial reporting risk with a specified owner, frequency, evidence standard and exception route.

The programme has not discovered 684 sources of assurance. It has discovered 684 statements requiring judgement.

A risk-led redesign reduces the revenue set from 73 controls to 31. Common reconciliations are standardised. The six spreadsheet-dependent controls receive protected templates, version control and independent review. Report completeness is tied to record counts and control totals from the feeder systems. Divisional exceptions are logged and resolved before consolidation.

Testing effort falls, but assurance increases. Instead of sampling a broad catalogue of vague activity, management can test a smaller set of controls whose purpose and operation are explicit.

This is not control reduction for convenience. It is the removal of duplication and ambiguity so that attention reaches the points where a material error could enter, pass undetected or remain uncorrected.

6. Three Responses Available to Management

The choices can be stated plainly.

Approach	Immediate advantage	Structural weakness	Likely result
Documentation project	Fast inventory and visible progress	Ownership remains with the project team	A large evidence archive that decays after first use
Audit-led compliance	Strong testing discipline and independence	Management may defer judgement to the testers	Findings are identified, but operating capability remains external
Management control capability	Connects risk, process, technology, evidence and accountability	Requires harder changes to roles and routines	Compliance becomes repeatable and informs better management

The first option is attractive when the deadline dominates every conversation. The second is attractive when executives want assurance from specialists. Both contribute essential elements. Neither should be the operating model.

The recommended position is a management control capability, established through a time-bound transformation programme but transferred into normal finance, technology and operational governance before the first full assessment cycle is complete.

7. The Recommended Control Capability

The capability has six connected components.

7.1 A Risk-to-Account Map

Begin with significant accounts, disclosures and relevant assertions. Trace the risks that could cause material misstatement, then identify the processes and systems through which those risks arise.

This direction matters. Beginning with departments or existing procedure manuals produces an inventory of activity. Beginning with financial reporting risk produces a defensible scope.

The output is a map linking:

- financial accounts and disclosures;
- assertions such as existence, completeness, valuation and presentation;
- material risks;
- process stages and applications;
- key preventive and detective controls.

The map becomes the organising spine for documentation, testing and change assessment.

7.2 Precisely Specified Controls

Every key control should answer seven questions.

1. What risk does it address?

2. Who performs it and who reviews it?
3. How often does it operate?
4. What information is used?
5. What constitutes satisfactory performance?
6. What evidence remains?
7. What happens when an exception is found?

This specification distinguishes a control from a good intention. "Management reviews monthly results" is not testable. "The divisional controller compares actual gross margin with budget and prior month, investigates movements above an agreed threshold, records explanations and signs the review before consolidation closes" is.

7.3 Integrated Technology Control

Financial controls and technology controls should not be maintained as separate worlds. The organisation must know which applications support each key control, which interfaces feed those applications and which general technology controls underpin their reliability.

The practical focus should include:

- user access and segregation of duties;
- program change approval and testing;
- scheduled processing and failed-job recovery;
- backup and restoration;
- interface completeness and accuracy;
- privileged access to data and programs.

The purpose is not to label every technology procedure as financially significant. It is to identify the small number of technology conditions without which key financial controls cannot be trusted.

7.4 Evidence by Design

Evidence should be generated as part of performing the control, not reconstructed when testing begins.

A reconciliation template should show preparer, reviewer, date, source totals, difference, explanation and resolution. An access review should retain the population reviewed, the decision made for each exception and proof that removals occurred. A program change should link approval, test result and production movement.

Paper records will remain appropriate in many places. Shared network folders and controlled intranet repositories can improve retrieval. The medium matters less than the chain of evidence and the discipline of retention.

7.5 Distributed Ownership with Central Standards

Finance owns the integrity of financial reporting controls. Process owners operate the controls. Information technology owns the reliability of supporting systems and general controls. Internal audit provides independent evaluation. The programme office sets the method, coordinates remediation and reports readiness.

External audit should challenge and attest, not design the organisation's controls or become the repository of management knowledge.

A small central control office should remain after the initial programme. Its role is to maintain standards, coordinate the annual assessment, monitor significant changes and advise owners. It should not perform controls on behalf of the business.

7.6 Change-Triggered Reassessment

Annual testing alone is too slow for an environment that changes throughout the year. The organisation should require control reassessment when specific events occur:

- a major system implementation or release;
- a process centralisation or outsourcing decision;
- an acquisition or disposal;
- a significant accounting policy change;
- a reorganisation affecting responsibility;
- a serious control failure or unexplained adjustment.

Each event should trigger a review of scope, risk, control design, documentation and test plans. This prevents the control inventory from describing last year's organisation.

8. From Programme to Operating Rhythm

The transition should be planned from the beginning, not attempted at project closure.

In the first stage, the programme establishes scope, method, governance and the initial risk-to-account map. In the second, process and technology owners document and redesign controls with central challenge. In the third, controls operate through real reporting cycles while defects are corrected. In the fourth, internal testing confirms readiness and unresolved issues reach accountable executives. In the fifth, ownership transfers into normal management routines.

The transfer gate should require more than completed documents. It should demonstrate that:

- owners can explain the risk and purpose of each key control;
- evidence has been produced through at least one genuine operating cycle;
- technology dependencies are mapped;
- deficiencies have named remediation dates and responsible executives;
- changes to systems and processes trigger reassessment;
- the audit committee receives a concise view of significant risks, failures and management decisions.

The central programme can then shrink because the organisation, not the project, owns the work.

9. Governance and Measures

The audit committee needs a view that separates volume from significance. Hundreds of control counts obscure judgement. Reporting should distinguish:

- key controls designed and operating;
- significant deficiencies by financial risk;
- overdue remediation by accountable executive;
- controls affected by current system or process change;
- repeated exceptions indicating that a control is poorly designed;
- unresolved disagreements over scope or evidence.

Completion percentages are useful for mobilisation, but dangerous as the principal measure of readiness. A programme can be 95 per cent complete while the remaining five per cent contains the only controls preventing a material error.

The governing question is not how much documentation exists. It is whether management has credible grounds for its assessment.

10. Prescription

Sarbanes-Oxley should be used to create a permanent management discipline linking financial risk, operational process, technology and evidence.

The immediate prescription is therefore:

1. Mobilise as a transformation programme, because urgency and coordination are real.
2. Scope from financial reporting risk, not from existing procedure catalogues.
3. Reduce vague activity statements to a defensible set of specified key controls.
4. Integrate financial and technology dependencies in one control model.
5. Generate evidence during operation and test through genuine reporting cycles.
6. Transfer ownership to finance, process and technology leaders before programme closure.
7. Retain a small central capability to maintain standards and respond to change.

This approach is more demanding than a documentation exercise. It requires management to make choices about risk, responsibility and the design of work. It also produces something more valuable than a successful filing season.

Regulation may have created the deadline, but management must create the capability that survives it.