
FRAMEWORK · COMPANION · V1.0

Three modes of compliance

Bearing west · Third piece · PDCA+ v2.0 · Public Review

Compliance-check, continuous compliance, and strategic compliance are not stages in a maturity ladder. They are qualitatively different relationships between an organisation and the regimes it operates under. Most organisations operate in the first, aspire to the second, and do not know the third exists.

AUTHOR

Joacim Brandell

Written for practitioners working with regulatory regimes · worked example draws on defence supply-chain assurance across CMMC, DEFSTAN, and Canada Protected B

How to read this piece

“W.1 – Supporting assurance towards a regime” established how PDCA+ supports assurance toward a regime. “W.2 – The control-objective chain” elaborated the interior chain — Regime Intent through Stakeholder Entitlement, pivoting at the Control Objective Record — that holds the regime architecture in the substrate.

This piece elaborates a consequence of that chain that the practitioner may not yet have seen. Once the substrate holds the chain, three structurally different modes of compliance become distinguishable. Compliance-check is the mode most frameworks were designed for. Continuous compliance is the mode most organisations aspire to and most fail to actually achieve. Strategic compliance is a third mode that becomes operationally possible once continuous compliance is structurally real — and that most organisations do not yet know exists, because they have never had the substrate that makes it thinkable.

The three modes are not a maturity ladder. They are qualitatively different relationships between an organisation and the regimes it operates under. Moving between them is not just improvement; it is a change in what the compliance function is doing. This piece names the modes, distinguishes them precisely, and shows where PDCA+'s structural choices make each one possible — and why most organisations remain stuck between the first two for reasons that are framework-shaped, not effort-shaped.

Compliance-check, as the reference

Compliance-check is the mode every reader will recognise. The regime sets requirements; an audit window approaches; the organisation prepares evidence; an assessor examines the evidence and renders a judgement. Pass or fail, the cycle closes, and the next cycle begins when the next audit window approaches. The relationship between the organisation and the regime is gated by the check.

Compliance-check has been the default mode of regulatory compliance for as long as there have been regulatory regimes worth talking about. It works, in a limited sense. The mode is well-understood by both auditors and audited; the cadence is predictable; the evidence work, however expensive, is at least bounded in time. Organisations that have only ever operated in this mode have functioning compliance programmes by their own lights, and many of them pass their audits reliably.

The mode's structural cost is also well-understood, even when it is not named structurally. Audit preparation is reconstruction work — evidence is assembled from operational sources at the time it is needed, in the form the regime expects, against the controls the regime enumerates. Between audits, the work largely stops. The compliance function is busy in the run-up and idle in the trough; the operational systems continue to drift between checks; the organisation discovers what has gone wrong when it prepares for the next audit, often months after the wrongness began.

This piece takes compliance-check as the reference mode. It is the baseline against which the other two modes' contributions become visible. The mode persists not because it is good but because it is what most frameworks support. Replacing it requires a different framework, not a different work ethic.

Continuous compliance, and why most organisations fail at it

Continuous compliance is what most organisations now say they aspire to. The language is everywhere — "continuous controls monitoring," "always-on compliance," "audit-ready every day." The aspiration is correct. The execution is, in most organisations, structurally compromised, and the compromise is rarely named for what it is.

The trouble is that most organisations attempt continuous compliance by running compliance-check more frequently. Quarterly checks become monthly; monthly becomes weekly; weekly becomes a dashboard. The cadence shortens, the work load grows, the compliance function expands, and the organisation calls the result continuous compliance. It is not. It is high-frequency compliance-check, and the structural costs that compliance-check imposes do not go away when the cadence accelerates — they accumulate.

Genuine continuous compliance is something different. It is the mode in which the substrate holds operational reality continuously, in shapes that already address the regime's requirements, with evidence linked to obligations as operational artefacts are produced. The check, when it happens, is a snapshot of substrate state — not a reconstruction. The compliance function is doing the work continuously, but the work it is doing is substrate stewardship, not evidence assembly. Audit windows still exist, but they no longer trigger scrambles, because nothing needs to be assembled that was not already held.

Why this requires more than effort

The reason most organisations fail at genuine continuous compliance is that their underlying frameworks were not built for it. Compliance-check frameworks treat evidence as a per-audit product to be assembled. Their data architectures hold operational records adequate for operations but not addressable to regime requirements. Their control inventories live in spreadsheets that are reconciled to regimes by hand. Their risk registers are separate artefacts that the compliance function consults but does not connect to evidence structurally. The framework's seams are exactly where continuous compliance needs structural reuse to live.

These are the conditions PDCA+ was built to address. The whitepaper named them in operational terms — duplicated work at every cycle, gaps at the seams, alignment held in people's heads, learning closed within silos. Each of these is a continuous-compliance failure mode, even when the organisation has not yet named what continuous compliance would have to look like to genuinely work. The substrate that holds schemas, taxonomies, translation rules, and shared capabilities is precisely the substrate that makes continuous compliance structurally possible rather than aspirational.

THE FAILURE MODE, IN ONE SENTENCE

Most organisations attempting continuous compliance are running compliance-check faster — without the substrate that would let evidence be held continuously, classifications propagate between disciplines, and obligations link to operational artefacts as they arise. The framework, not the work ethic, is what is holding the aspiration short.

What genuine continuous compliance buys

When the substrate is in place and the chain is held, continuous compliance changes the compliance function's relationship to time. Audit windows stop being scrambles. Evidence freshness becomes a property of the substrate rather than a project. Findings surface continuously rather than at quarterly review forums. The function spends its time on stewardship — maintaining the regime bindings, updating translation rules as regimes revise, closing inadequacies the conjunction surfaces — rather than on reconstruction. The organisation's compliance posture becomes a property it has at any given moment, queryable on demand, not a state it achieves periodically and lets drift between.

This is what W.1 described, and what most organisations want when they talk about continuous compliance. Getting there requires the substrate, the chain, and the framework's structural choices working together. Without them, the aspiration produces high-frequency compliance-check at best, and audit-cycle exhaustion at worst — which is where many compliance functions currently live.

Strategic compliance, the third mode

Most organisations do not know strategic compliance exists. The reason is structural: it is invisible from compliance-check mode entirely, and only barely visible from genuine continuous compliance. It becomes thinkable only once the substrate is in place and the chain architecture is held — at which point the organisation has, often without realising it, acquired a capability it did not have before.

Strategic compliance is the mode in which the organisation's compliance posture is treated as a managed strategic variable. The organisation does not just respond to the regimes it is under; it deliberates about which regimes it will be under, which obligations it will commit to, which risks it will accept, and which controls it will operate — and recomputes the consequences across the substrate when those strategic decisions change.

What strategic compliance includes that continuous compliance does not

Continuous compliance keeps the organisation's posture current relative to the regimes it is operating under. Strategic compliance adds the dimension of choosing which regimes those are, and what posture is being held within each.

Control discontinuation. When a regime no longer applies — because a contract has ended, a market has been exited, a programme has wound down — the controls that existed solely

to satisfy that regime can be retired. Strategically, this means actively recovering the cost of operating them. Operationally, it means walking the chain from the retired Regime Intent Record downward, identifying which obligations now have no upstream requirement, which evidence links no longer underwrite anything in scope, which controls can be cleanly decommissioned, and which remain because other regimes still depend on them. The substrate computes the propagation. Without the chain, this work cannot be done coherently and most organisations leave retired-regime controls in place indefinitely, paying their cost without their benefit.

Deliberate risk-appetite shift. Risk appetite is supposed to be a strategic choice, but in most organisations it is articulated abstractly and then reconnected to actual treatment decisions ad hoc. Strategic compliance attaches risk-appetite changes directly to the Control Objective Records they affect, propagates through the obligations and evidence those objectives generate, and surfaces which residual postures the organisation is now choosing to operate with. The decision becomes traceable and the consequences computable. An organisation deciding to accept more risk in one domain (perhaps to free resources for another) can do so deliberately rather than by accident.

Response to environmental change. Wars, sanctions, regulatory shocks, market exits, supply-chain disruptions — major environmental shifts change which regimes apply, which obligations are reasonable, which risks have moved. Compliance-check organisations absorb these shocks chaotically, often re-papering controls to fit the new reality long after operations have already shifted. Continuous-compliance organisations keep up reactively. Strategic-compliance organisations make the posture changes deliberately — adding regimes that have become applicable, retiring regimes that have not, shifting risk acceptances that the new environment warrants, communicating the changes through the substrate to all bound disciplines and stakeholders.

Selective regime entry. Strategic compliance also includes the decision to take on new regime obligations as a strategic choice rather than a contractual requirement. An organisation may decide to seek certification under a regime its current contracts do not require, because the certification opens new markets or signals capability. The substrate makes this decision computable: bind the new regime, see what additional obligations attach, identify which already-held objectives satisfy the new regime's requirements, scope the gap precisely. The strategic case becomes evaluable against operational reality rather than against guesses.

The conditions strategic compliance requires

Strategic compliance requires both pieces of structure that the W.1 and W.2 together establish.

It requires the substrate — without it, the regime architecture is reconstructed by hand each time, and strategic moves are too expensive to contemplate. An organisation cannot strategically retire a control if the cost of properly retiring it (identifying its dependencies, retiring its evidence collection, updating regime mappings, communicating the change to bound disciplines) exceeds the cost of just letting it run. The substrate makes retirement cheap enough to be strategic.

It requires the chain — without it, regime requirements are not linked to control objectives in a way that makes strategic moves propagate coherently. Retiring a Regime Intent Record without the chain leaves orphaned Requirement Records, orphaned Obligations, orphaned Evidence Links scattered through whatever artefacts the organisation happened to associate with the regime. With the chain, retirement is a structured operation: walk the chain downward, identify what loses upstream support, compute the consequences, present the changes for authority decision, propagate the changes through the substrate.

And it requires the deliberate framing — without it, the capability exists but is not used strategically. An organisation can have the substrate, have the chain, and still operate in continuous-compliance mode indefinitely if the compliance function and the leadership do not recognise that they now have a strategic instrument. This recognition is rare, which is why strategic compliance is rare even where the substrate makes it possible.

THE THIRD MODE, IN ONE SENTENCE

Strategic compliance treats the organisation's compliance posture as a managed strategic variable: which regimes to be under, which controls to operate, which risks to accept, all recomputable through the substrate when strategic decisions change. It is invisible from compliance-check, barely visible from continuous compliance, and unfamiliar to most organisations even when they already have the substrate that makes it possible.

The three modes, side by side

The differentiation becomes concrete when the three modes are compared across dimensions that matter operationally. The following table maps the modes against axes a practitioner working in any of them will recognise.

Dimension	Compliance-check	Continuous compliance	Strategic compliance
Cadence	Periodic, gated by audit windows	Continuous, evidence held in the substrate	Continuous, with strategic intervention points
Relationship to time	Scramble–trough–scramble	Steady stewardship	Steady stewardship plus deliberate posture moves
Posture	Reactive — meet the regimes as they ask	Sustained — meet the regimes continuously	Deliberate — choose which regimes, choose how
Response to change	Re-paper after the fact	Keep up reactively as change arrives	Recompute posture deliberately and propagate
Control discontinuation	Rarely happens; cost outweighs benefit	Possible but expensive without chain	Routine; substrate computes the propagation
Risk appetite	Articulated abstractly; loosely connected to controls	Connected to controls through register reconciliation	Attached to objectives; propagates through chain
Substrate dependency	None required	Required for genuine version (not high-frequency)	Required plus the control-objective chain
Recognition	Universal — every organisation knows this mode	Aspirational — most claim it; few actually have it	Rare — most organisations do not know it exists

The progression across columns is not just "more of the same." Each move changes what the compliance function is structurally doing. The first move (check to continuous) requires the substrate. The second move (continuous to strategic) requires the chain plus the deliberate framing. Organisations stuck between the first two are almost always stuck for substrate reasons; organisations that have the substrate but not the third mode are typically stuck for framing reasons — they have the instrument and have not yet recognised what it can be used for.

A worked example: environmental shift

To make the differentiation concrete, consider a defence supplier — the same Swedish avionics supplier from W.1's §0 — when a major environmental shift occurs. The shift, for the purposes of this example, is a significant escalation in regional security tensions. Several things change simultaneously.

- New emergency cybersecurity directives from the supplier's national authority impose additional obligations on defence supply-chain participants, effective immediately.
- The organisation's risk appetite is deliberately tightened by the board — risks that were acceptable six months ago are no longer acceptable in the current environment.

- A planned market exit from a non-aligned jurisdiction is accelerated; contracts there will be wound down within ninety days, and the regime that governs information handling for those contracts (a national data-protection regime) will no longer apply to the supplier's operations.
- An existing prime contractor adds a flow-down requirement for a new export-control category that was not previously in scope.

How does the organisation respond in each compliance mode?

In compliance-check mode

The organisation absorbs the changes operationally — the operational teams respond to the new directives, scale back work in the exited jurisdiction, accommodate the new flow-down — but the compliance function does not engage structurally until the next audit window approaches. When it does, it discovers that several months of operational change need to be re-papered against the regimes. The retired-jurisdiction's controls remain in place because nobody has authority or budget to retire them cleanly. The new directives are documented hastily for the upcoming audit. Risk appetite changes are noted in board minutes but not connected to specific controls. The organisation appears compliant at the next audit, with significant residual confusion about which obligations actually apply to which operations.

In continuous-compliance mode

The substrate continuously surfaces what is changing — new directives appear as new requirements to be addressed; the exited-jurisdiction obligations begin surfacing as inadequacies (controls being operated against a regime that no longer applies); the new flow-down arrives as a new binding to be added. The compliance function keeps up. Evidence remains current; the substrate reflects the new reality within weeks rather than months. But the function is reactive: it is responding to changes as they arrive, not deciding which changes to accept, which to anticipate, which to reposition against.

In strategic-compliance mode

The compliance function and leadership use the environmental shift as a decision point. The new directives are evaluated for what they require beyond what the substrate already holds; the gaps are scoped precisely. The exited-jurisdiction obligations are deliberately retired — the Regime Intent Record is marked for retirement, the chain propagates downward, controls and evidence that exist solely for that regime are identified and decommissioned cleanly. The board's risk-appetite tightening is attached to specific Control Objective Records, propagating through the substrate to surface which residual postures are now no longer within appetite — and what would have to change for them to come back within appetite. The new flow-down is bound as a regime; the substrate identifies which already-held objectives satisfy its requirements and which gaps remain to be closed.

The strategic-compliance organisation has done more work than the continuous-compliance one, but the work is leveraged: every move is deliberate, every consequence is computed, every decision is traceable. The organisation emerges from the shift with a deliberately reconfigured compliance posture, lower ongoing cost (retired controls genuinely retired), clearer accountability for residual risks, and earlier signal on the new directives' implications. The compliance posture has become a strategic asset rather than a reactive overhead.

WHAT THE WORKED EXAMPLE SHOWS

Compliance-check absorbs the shift chaotically. Continuous compliance keeps up reactively. Strategic compliance reconfigures the posture deliberately. The structural difference is not effort — it is whether the substrate and chain make deliberate moves cheap enough to be worth making at all.

Why the third mode is rare

Strategic compliance is rare even in organisations that have the substrate, and understanding why is worth a moment.

First, the recognition problem. Organisations that have spent years climbing toward continuous compliance often experience reaching it as the destination. The capability they have now — sustained evidence, manageable audit cycles, no more scrambles — is so much better than what they had before that the question of what else the capability makes possible does not arise. The substrate is being used to do continuous compliance well. It is not being used for anything beyond that, because nothing beyond that has been imagined.

Second, the framing problem. Compliance has been culturally framed for decades as a constraint to be satisfied — "what does the regime require, and how do we meet it?" — rather than as a posture to be managed. The framing makes the strategic dimension invisible. A compliance function that thinks of itself as "meeting requirements" will not naturally extend to "choosing which requirements to be under," even when the substrate makes the choice operationally tractable. The framing has to be deliberately changed, usually by someone at executive level who sees the strategic dimension and names it.

Third, the political problem. Strategic compliance involves making explicit decisions about risk appetite, regime entry and exit, and control retirement. Each of these is a decision that compliance-check organisations have implicitly avoided — controls accumulate because retiring them is politically expensive; risk appetite stays abstract because making it concrete requires owning specific residual decisions; regime entry happens through contract obligations because anything else would require strategic deliberation the organisation has not been resourced to do. Strategic compliance asks the organisation to make these decisions explicitly, and explicit decisions have explicit owners. Some organisations are not ready for that.

Fourth, and most consequential, the substrate problem. Most organisations have not yet achieved genuine continuous compliance. They are in high-frequency compliance-check, accumulating work and exhaustion, and the substrate that would make strategic compliance possible has not yet been built. From inside that situation, strategic compliance is not just invisible — it is unimaginable. The framework would have to be in place first; the practitioner would have to have time to think about what the framework makes possible beyond its first-order use; the organisation would have to be open to recognising a strategic capability where it was previously seeing only an operational improvement. Each of these is a separate condition, and the combination is rare.

The argument of this piece is not that every organisation should reach for strategic compliance immediately. It is that strategic compliance exists, is operationally definable, and becomes available once the substrate and the chain are in place. Organisations that recognise the third mode early — even before they have fully arrived in the second — can plan for it. Organisations that do not recognise it will reach continuous compliance, take stock, and conclude they are done. Some of them will be doing themselves out of a capability they already structurally possess.

Closing

Three modes, qualitatively distinct. Compliance-check is the reference, the mode every framework was originally designed for and the mode most organisations still operate in. Continuous compliance is the aspiration, achievable only when the substrate makes evidence-as-substrate-state structurally real — without which the aspiration produces high-frequency compliance-check and exhaustion. Strategic compliance is the third mode, operationally possible once the substrate and the chain are in place, and structurally invisible to organisations that have not yet built them.

PDCA+ supports each mode at exactly the level the mode requires. For compliance-check, the framework is overkill — the mode runs on any framework, however brittle. For continuous compliance, the framework is necessary, because without the substrate, continuous compliance reduces to its high-frequency-check cousin and fails for the structural reasons PDCA+ was built to address. For strategic compliance, the framework is necessary plus sufficient — the substrate plus the chain plus the deliberate framing produce a capability the organisation can use strategically, and PDCA+'s structural choices were made in a way that supports all three.

Most readers of this piece will be working somewhere between the first two modes, with various combinations of substrate maturity and aspirational language. The offer is not a prescription — get to the third mode immediately — but a recognition: the third mode exists, it is structurally definable, and the work you are doing toward continuous compliance is also, whether you have framed it that way or not, work toward making strategic compliance possible. Naming what is being built is part of how it gets built.

THE THREE MODES, IN ONE SENTENCE

Compliance-check is reactive and gated. Continuous compliance is sustained and steady. Strategic compliance is deliberate and reconfigurable. The first works on any framework; the second requires substrate; the third requires substrate plus chain plus the recognition that the compliance posture is now a strategic variable.

References

- U.S. Department of Defense. Cybersecurity Maturity Model Certification (CMMC) 2.0 Programme documentation, 32 CFR Part 170.
- NIST Special Publication 800-171 Rev. 3. Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations.
- NIST Special Publication 800-171A. Assessing Security Requirements for Controlled Unclassified Information.
- UK Ministry of Defence. Defence Standard 05-138 (Cyber Security for Defence Suppliers).
- Government of Canada. ITSG-33 IT Security Risk Management: A Lifecycle Approach.
- Government of Canada, Treasury Board Secretariat. Directive on Security Management — Protected B handling requirements.
- U.S. Department of State. International Traffic in Arms Regulations (ITAR), 22 CFR §§120–130.
- Directive (EU) 2022/2555 — NIS2 Directive, and national transpositions thereof.