FRAMEWORK · COMPANION · V1.0

Supporting assurance towards a regime

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

What does it look like, structurally, for a framework to support assurance toward a regulatory regime — and how does the picture change when an organisation operates under several at once?

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

The situation

A mid-sized defence supplier in Sweden manufactures avionics subsystems. Their customer list includes prime contractors in the United States, the United Kingdom, and Canada, with occasional flow-downs from a French integrator on European programmes. The technical work the supplier does is the same regardless of who is buying — the same engineers, the same processes, the same configuration management, the same incident response. The assurance work is not the same.

For the US primes, the supplier is preparing for CMMC Level 2 assessment — practices drawn from NIST SP 800-171, evidenced against the assessment objectives in NIST SP 800-171A, conducted by a Certified Third-Party Assessment Organization. For the UK programmes, they operate under DEFSTAN 05-138 with its tiered risk profile and Cyber Essentials Plus underpinnings. For the Canadian programme, they are working through ITSG-33 controls in support of a Protected B handling environment. The French integrator's flow-downs reference both the EU NIS2 transposition and France's specific cybersecurity-for-defence requirements; ITAR may apply if certain components or technical data are involved, and that brings export-control regimes into the same envelope.

The technical reality is one set of systems doing one set of work. The assurance reality is four or five regimes each demanding evidence in their own form, against their own controls, classified under their own taxonomies, verified by their own assessment procedures, on their own audit cadences. Each regime has its own vocabulary; each regime's controls overlap with the others' partially but never identically; each regime's evidence requirements are specific enough that translation between them is not free.

Most suppliers in this situation manage the multi-regime burden by maintaining parallel assurance programmes. There is a CMMC programme with its own documentation, its own evidence repository, its own assessment readiness work; a DEFSTAN programme alongside it with its own documentation and evidence; a Canadian programme alongside that. The programmes share staff but little else. Each is reconstructed, each audit cycle, from the same underlying operational reality. The cost is significant and the duplication is structural — the same evidence is being prepared multiple times in multiple forms, against controls that are different in their letter but often the same in their substance.

This piece is about what changes when that reconstruction work is replaced by structural reuse — and specifically, what it takes for a framework to support assurance toward a regime in a way that genuinely composes across multiple regimes operating simultaneously. The leading question is precise: in what way does PDCA+ support assurance toward a regime? The answer, developed through this piece, also explains why the answer scales across regimes rather than fragmenting.

What assurance is, and what it is not

Assurance and compliance are often used interchangeably. They should not be. The distinction matters for what follows.

Compliance is the state of meeting the requirements a regime sets. A control is compliant when it is implemented as specified; an organisation is compliant when its controls collectively meet the regime's expectations. Compliance is a property of operations.

Assurance is the production and presentation of evidence that compliance holds, in a form a third party can accept as the basis for their own judgement. Assurance is a property of evidence, not of operations. An organisation can be compliant without being able to demonstrate it, and an organisation can present convincing assurance for compliance it does not actually have. The two are related but distinct concerns, and conflating them produces predictable failures — most commonly, organisations that have invested heavily in compliance work without investing comparably in the evidence apparatus that lets assurance be produced on demand.

The third party consuming assurance is the regime owner or their delegate — a CMMC assessor, a DEFSTAN auditor, a Canadian Communications Security Establishment authoriser, a prime contractor's supply-chain risk function. What they are doing structurally is not verifying the operations directly; they are evaluating the evidence the supplier presents about the operations. The evidence is the product. The operations underwrite the evidence, but it is the evidence that the assurance function delivers.

> **THE ASSURANCE PRODUCT**
>
> *Assurance is the evidence apparatus by which an organisation demonstrates, to a third party able to consume the demonstration, that its operations meet a regime's requirements. The operations matter; the evidence is what the regime owner reads.*

This framing has consequences for how a framework can usefully support assurance. The framework's contribution is at the evidence layer — making the right evidence available, in the right form, addressable to the right control reference, traceable to the operational artefacts that underwrite it, current as of the date the assurance is being produced. If the framework does this well, the assurance function becomes a function of selecting and presenting evidence that already exists in usable form. If the framework does this poorly, assurance becomes the reconstruction of evidence each cycle, regardless of how well the operations themselves are running.

What every regime asks for, structurally

Regimes differ in vocabulary, in scope, in stringency, in the specific controls they enumerate, in the evidence forms they accept, and in the assessment procedures they use. Beneath those differences, what they ask for is structurally similar across every regime worth taking seriously.

A regime asks the supplier to articulate the context within which controls are operating — what assets are in scope, what data classifications are handled, what environments are involved, what dependencies exist on third parties. It asks the supplier to demonstrate identification of risks, deviations, incidents, and changes relevant to the regime's concerns. It asks for evidence of analysis — that what has been identified has been examined for its properties. It asks for evidence of treatment — that responses have been committed where required. It asks for evidence of acceptance — that residual posture has been deliberately and authoritatively bound, with named accountability. And it asks for continuous evidence of monitoring and review against the criteria the regime specifies, with communication to whoever is authorised to consume the observations.

These are, recognisably, the strands of the organisational lifecycle as PDCA+ articulates them. The recognition is not coincidence. Regimes are written by people who have learned, often the hard way, what evidence is required to make a credible assurance judgement, and what they have learned has converged on roughly the same structural shape — because the structural shape is what credible assurance about a continuously-operating organisation requires.

Each regime then specialises this structural shape with its own substance. CMMC specifies which controls (the 110 practices drawn from 800-171), which evidence the assessment objectives expect for each, which assessment procedures are acceptable. DEFSTAN specifies its own risk-tier framework, its own profile of practices, its own evidence formats. Canada Protected B operates against ITSG-33's catalogue with the Canadian Centre for Cyber Security's specific guidance. The specialisations differ; the underlying structural ask is the same.

> **THE STRUCTURAL ASK, COMMON ACROSS REGIMES**
>
> *Every regime asks the supplier to evidence context, identification, analysis, treatment, acceptance, and continuous monitoring against criteria the regime specifies. The substance of the criteria differs; the structure of the evidence ask does not.*

This commonality is what makes structural reuse possible. If every regime asked for fundamentally different evidence in fundamentally different forms about fundamentally different aspects of operation, there would be no reuse to capture — the parallel-programme approach would be structurally correct, just expensive. The fact that regimes converge on the same structural ask is what makes multi-regime assurance a tractable engineering problem rather than an irreducible one.

Supporting assurance toward one regime

Take CMMC Level 2 as the worked example for the single-regime case. The supplier is preparing for a third-party assessment. They need to produce evidence that, for each of the 110 practices, the assessment objectives are met, in a form a C3PAO assessor can examine and judge. What does PDCA+ do for this assurance work?

Evidence shape

Every practice in 800-171 expects evidence of a particular shape — a policy reference, an implementation description, evidence of operation, evidence of effectiveness. The assessment objectives in 800-171A specify what the assessor will examine. PDCA+'s schemas hold these evidence shapes as structural definitions of what flows. When the configuration-management discipline produces evidence of its operations, that evidence enters the substrate in a schema that is already addressable to the practices it underwrites (CMMC practice CM.L2-3.4.1 establishment and maintenance of baseline configurations, CM.L2-3.4.2 enforcement, and so on). The evidence does not need to be prepared in a CMMC-specific form; it is prepared in the substrate's schema, and the schema's mapping to the regime is what makes the evidence regime-addressable.

Classification under the regime's taxonomy

Each regime has its own way of classifying what is in scope, what data is being protected, what risk tier applies to which system. CMMC distinguishes Federal Contract Information from Controlled Unclassified Information; DEFSTAN classifies by risk profile; Canada Protected B has its own protected-information categories. PDCA+'s taxonomies hold these classifications as conjunction-held capabilities. When an asset enters scope, its classification under the relevant regime's taxonomy is recorded in the substrate. Downstream consumers — risk assessments, change approvals, incident handling — can address findings to the right regime-specific class without each consumer needing to know the regime's taxonomy internally.

Translation between operational vocabulary and regime vocabulary

The supplier's operational teams use their own vocabulary — they speak of "servers," "applications," "engineers," "changes," "incidents." The regime speaks of "information systems," "organisational personnel," "system changes," "security incidents." The mapping is not free; the regime's terms have specific scoping that the operational terms do not always preserve. PDCA+'s translation rules hold these mappings explicitly. When evidence is being produced for the assessor, the substrate translates the operational vocabulary into the regime's vocabulary using the rules it already holds, with the rules' scope conditions and caveats traceable in case the translation is challenged.

Shared capabilities, including control management

Control management is the most prominent shared capability in PDCA+, and it is the one that does the most work for regime assurance. A single control inventory, held in the conjunction, holds the full set of controls the organisation operates. Each control has a specification, an

implementation description, evidence of operation, and a current effectiveness observation. The same control inventory is addressed by CMMC practice references, by DEFSTAN profile references, by Canadian ITSG-33 references. The control exists once; the regime mappings let multiple regimes consume evidence about it. This is the structural answer to the duplication problem named in §1.

Surfacing of assurance-relevant inadequacies

The conjunction's continuous observation surfaces inadequacies in what it holds. For regime assurance, the most consequential inadequacies are evidence gaps — a practice whose underwriting evidence has gone stale, a classification that no longer matches what the asset is doing, a translation rule whose scope conditions are being violated. The conjunction surfaces these as they arise, not at audit time. The assurance function then knows what evidence needs refreshing well before the assessor arrives, which is the difference between assurance as continuous readiness and assurance as periodic reconstruction.

Together these five functions — evidence shape, classification, translation, shared capabilities, and surfacing — are what PDCA+ contributes to assurance toward a single regime. None of them is exotic; each maps to a category of work that any assurance function does. What is structural is that the framework holds them as substrate rather than as documentation. The substrate is queried; the documentation is read. The difference between the two is the difference between assurance being computable and assurance being prepared.

> **THE SINGLE-REGIME CONTRIBUTION**
>
> *Toward one regime, PDCA+ contributes evidence shape, classification under regime taxonomies, translation between operational and regime vocabulary, shared capabilities consumed by the regime, and continuous surfacing of assurance-relevant gaps. The contribution is structural — substrate that the assurance function queries, not documentation it reads.*

Supporting assurance toward several regimes simultaneously

The structural contribution to a single regime is useful in itself, but the more interesting question — and the one that makes the difference between PDCA+ and any number of compliance platforms — is what happens when the same organisation operates under several regimes at once. The defence supplier in §0 is not preparing only for CMMC; they are preparing for CMMC, DEFSTAN, Canadian Protected B handling, and any flow-downs that arrive on top. The question is whether the framework composes across regimes or fragments under them.

The answer turns on what is held once in the substrate and what is held per-regime. The substrate is regime-agnostic where it can be, regime-specific where it must be, and the boundary between the two determines how much of the multi-regime burden becomes structural reuse and how much remains parallel work.

What the substrate holds once, across all regimes

The operational facts of the organisation are held once. There is one configuration baseline, one risk register, one incident record, one change history, one control inventory. These are operational realities; they are what they are regardless of which regime is consuming evidence about them. The substrate's schemas hold them in shapes that are not regime-specific, even though regime-specific mappings will be applied when evidence is produced.

Cross-cutting capabilities are held once. Control management lives in the conjunction, not in any one regime's programme. Measurement constructs — definitions of adequacy, severity, effectiveness — are conjunction-held, available to every regime that requires them. The shared capabilities accumulate substrate value: each new regime that binds gets to consume what is already there, rather than rebuilding it.

The translation rules between operational vocabulary and regime vocabularies are held once each. There is one translation between operational terms and CMMC vocabulary, one between operational terms and DEFSTAN vocabulary, one between operational terms and Canadian Protected B vocabulary. The rules accumulate; they do not interfere. When ITAR or a NIS2 flow-down arrives, a new translation rule is added; the existing rules continue to work.

What the substrate holds per-regime

Each regime brings its own taxonomy of in-scope categories, its own control-set mapping, its own evidence-form expectations, its own assessment-objective references. These are regime-specific by construction and cannot be made generic without distorting what the regime actually asks for. The substrate holds them as regime-bindings: a regime-specific overlay that addresses the regime-agnostic operational facts through the regime-specific lens.

A regime-binding looks structurally similar to a discipline-binding (in the whitepaper's sense): it declares which strands it consumes (typically all of them, because regimes ask for all strands to be evidenced), which conjunction services it relies on (typically the shared control inventory, the relevant translation rules, the measurement constructs), and how its specific evidence-form expectations are met by the substrate's regime-agnostic content. Adding a new regime is binding work, not rebuilding work.

The matrix view

Looking at the same evidence elements across three regimes makes the reuse structure concrete. The following matrix shows how a small set of evidence elements maps across CMMC Level 2, DEFSTAN 05-138, and Canada Protected B handling. The point is not the specific control references — those will vary by version and profile — but the pattern of overlap.

Evidence element	CMMC L2	DEFSTAN 05-138	Canada Protected B
Configuration baseline	CM.L2-3.4.1	5.2.2 (baseline mgmt)	ITSG-33 CM-2
Change authorisation	CM.L2-3.4.3	5.3.1 (change control)	ITSG-33 CM-3
Risk acceptance, named	RA.L2-3.11.1	4.4 (risk treatment)	ITSG-33 RA-3
Incident response	IR.L2-3.6.1–3.6.3	7.1 (incident mgmt)	ITSG-33 IR-4
Audit logging	AU.L2-3.3.1	6.2 (logging)	ITSG-33 AU-2
Personnel screening	PS.L2-3.9.1	3.1 (vetting)	ITSG-33 PS-3

The underlying operational artefacts are the same across columns. The configuration baseline that satisfies CMMC CM.L2-3.4.1 is the same configuration baseline that satisfies DEFSTAN 5.2.2 and ITSG-33 CM-2. What differs is the regime-specific addressing — the control reference, the evidence-form expectation, the assessment objective — not the operational reality being addressed. The substrate holds the operational reality once and the addressing per regime; evidence production becomes selection and presentation, not reconstruction.

> **THE MULTI-REGIME ANSWER**
>
> *Operational reality is held once. Regime-specific addressing is held per-regime. Each new regime adds a binding, not a parallel programme. The structural reuse is what lets multi-regime assurance scale where parallel-programme approaches fragment.*

Flow-downs and cascading regimes

Defence supply chains have a particular dynamic that makes the multi-regime case more demanding than it first appears: flow-downs. A prime contractor's regime obligations propagate to subcontractors through contractual flow-down clauses. A subcontractor's regime obligations propagate to their own subcontractors. Each link in the chain inherits some subset of its customer's regime requirements, often modified by what the link does for the customer, often with timing and stringency that depend on the contract.

In practice, this means a supplier may face simultaneous obligations under regimes they have not themselves signed up to — CMMC obligations because the US prime requires them, DEFSTAN obligations because the UK prime requires them, Canadian Protected B handling because the Canadian programme they are subcontracting on requires it. The regimes were not chosen by the supplier; they arrived as flow-down conditions on contracts the supplier wanted. The compliance and assurance burden, however, is the supplier's to bear.

Flow-downs also have time dynamics that make parallel-programme approaches especially brittle. A new prime contract may bring a new regime with a short timeline to assurance readiness. An updated standard version (CMMC 2.0 to CMMC 2.1, DEFSTAN revisions, ITSG-33 catalogue updates) may arrive with revised practices that flow down to existing subcontracts. The supplier's assurance apparatus has to accommodate change continuously, not just at planned audit cadences.

What the substrate does for flow-downs

The structural answer is the same as for static multi-regime operation, applied dynamically. When a flow-down arrives, it brings a new regime-binding or a revision to an existing one. The binding declares what the regime requires; the substrate already holds the operational reality; the regime-specific addressing is what is being newly declared. The work is bounded: define the new binding, validate that the existing operational substrate underwrites it, identify the gaps where the substrate does not yet hold what the regime requires, and address those specific gaps rather than rebuilding the whole.

This bounding matters because flow-downs would otherwise have multiplicative cost. A supplier with three primes and four regimes each, with each regime revising every few years, would face an unbounded reconstruction burden under parallel-programme management. Under structural reuse, the cost of each new flow-down is the cost of binding work plus the cost of closing any specific operational gaps the new regime exposes — which is bounded, and predictable.

Export-control regimes as a special case

ITAR and other export-control regimes introduce a complication worth naming: they regulate not just operational conduct but who can access what technical data, with consequences that propagate through the supplier's information architecture. ITAR compliance is not just a set of controls; it is a regime that classifies technical data and gates access by personnel nationality, system location, and storage architecture. These classifications cascade through the rest of the assurance picture — an ITAR-controlled artefact is also a CMMC-relevant asset, also subject to DEFSTAN protections if it touches a UK programme, also potentially Canada Protected B if it touches a Canadian programme.

The substrate handles this through composition rather than special-casing. ITAR brings its own classification taxonomy, its own access-control schema, its own translation rules between the export-control vocabulary and the supplier's operational vocabulary. These are held alongside the other regime-bindings; their cross-cutting effects (an ITAR-controlled artefact also being subject to CMMC, etc.) are computed by the substrate as it would compute any other cross-binding interaction. The architecture of the substrate is what lets export-control regimes participate in the multi-regime picture without forcing the rest of the picture to be restructured around them.

What changes for the assurance function itself

If PDCA+ supports assurance toward a regime in the way described, the work of the assurance function changes substantially. The change is worth naming directly, because it reframes what the assurance function is and what its practitioners are doing.

Under parallel-programme management, the assurance function is largely a reconstruction function. Each audit cycle, each regime, each flow-down event triggers work to assemble the evidence the regime expects, in the form it expects, from operational sources that were not designed with the regime in mind. The function consists in significant part of translation work

done by humans at the time evidence is needed. The skill it requires is regime-specific expertise applied to operational reality each time.

Under structural reuse, the function changes character. The translation work has been pre-done, structurally — the rules are held in the substrate, and evidence production becomes querying. The function's skill becomes substrate stewardship: ensuring the regime-bindings are correct, that the translation rules accurately reflect the regimes' current asks, that the evidence shapes still align with what assessors expect, that gaps surfaced by the conjunction are closed in the operational substrate before they affect assurance readiness.

This is not less work. It is different work, and it requires different skills. A substrate steward needs to understand both the operational reality and the regimes' formal requirements precisely enough to maintain the mappings between them. They need to know when a regime revision changes the addressing without changing the underlying ask (a substrate-binding update is sufficient) and when it changes the underlying ask itself (operational change may be required). They need to know what the conjunction is telling them when it surfaces an inadequacy, and where in the substrate or the operations the inadequacy lives.

What disappears, mostly, is the audit-cycle scramble. Evidence that lives in the substrate is current by construction; evidence that does not is surfaced as gaps before assessors arrive. The function spends less time assembling and more time maintaining — which is, structurally, the right balance for a continuously-operating organisation in a multi-regime environment.

> **THE FUNCTION TRANSFORMS**
> *The assurance function changes from regime-specific reconstruction at audit time to substrate stewardship continuously. The skill shifts from translation-on-demand to maintaining the structural reuse that makes translation pre-done. The audit-cycle scramble largely disappears; substrate stewardship is what fills the time it freed.*

Limits and honest framing

Three things PDCA+ does not do for regime assurance are worth naming, because pretending otherwise would undermine the cases where it genuinely helps.

First, the framework does not substitute for regime-specific expertise. Knowing what CMMC actually requires, what DEFSTAN's risk tiers mean in practice, what Canadian Protected B handling demands in specific operational contexts — these are regime-specific competencies that have to live somewhere in the organisation. The substrate holds the mappings between operations and regimes, but the mappings have to be authored by people who understand both sides. PDCA+ makes the expertise more leveraged; it does not make it unnecessary.

Second, the framework does not relieve the supplier of regime authority decisions. Whether a particular system is in scope, whether a particular data element is CUI or FCI, whether a residual risk is acceptable for a Protected B environment — these are judgements that have to be made by people with the authority to make them. The substrate makes the judgements

traceable, queryable, and consistent across regimes, but the judgements themselves remain human work. The framework keeps authority where it belongs and surfaces what authority needs to act on; it does not act for authority.

Third, the framework's value is most visible when more than one regime is in play, or when regime change is frequent. A supplier operating under exactly one stable regime can probably maintain parallel-programme assurance acceptably well; the duplication cost is real but bounded. The value of structural reuse compounds with the number of regimes, the frequency of flow-down events, the rate of regime revision, and the complexity of cross-regime interactions. A supplier with one regime and stable contracts may not see the framework's full value; a supplier in the situation described in §0 will see it acutely.

None of these limits is a defect. They are the conditions under which the framework does its work, and being honest about them is what allows the work to be done well. The framework supports the assurance function; it does not replace it. The function is more leveraged with the framework than without it, and the difference becomes the larger the more demanding the multi-regime environment is. That difference, in the supply-chain assurance environment described in §0, is substantial.

Returning to the leading question

In what way does PDCA+ support assurance toward a regime? The piece has assembled the answer in pieces; it is worth restating directly.

It holds the evidence shapes the regime expects, as schemas the operational disciplines produce evidence into. It holds the regime's classifications as taxonomies the operational artefacts are classified under. It holds the translation rules between the operational vocabulary the supplier actually uses and the regime vocabulary the assessor will read. It holds cross-cutting capabilities — control management above all — as shared substrate every regime can address. It surfaces, continuously, the inadequacies in any of these that would otherwise become assurance gaps at audit time.

These are the contributions to a single regime. The structural form of the contribution is what lets it compose: each new regime added is a binding to the same substrate, not a new programme alongside existing ones. The operational reality is held once; the regime-specific addressing accumulates. Flow-downs become binding work rather than reconstruction work. Regime revisions become substrate maintenance rather than programme rewrites. Export-control regimes integrate through composition rather than special-casing.

The supplier in §0 is not in a situation that scales under parallel-programme management. The cost of maintaining four or five regime programmes in parallel, each reconstructed at each audit cycle, each updated independently as regimes revise, with each new flow-down adding a new programme — that cost grows faster than the supplier's capacity to absorb it. The structural reuse PDCA+ enables is what lets the situation become workable. The framework does not eliminate the regimes' demands; it changes the structural cost of meeting them, from multiplicative to additive.

That is what supporting assurance toward a regime looks like, structurally. The framework's contribution is not in any one regime's substance — the regimes own their substance, and the supplier's substantive work has to meet it. The framework's contribution is in how the evidence apparatus is held, so that meeting one regime's substance does not require rebuilding for the next. The single-regime answer is useful; the multi-regime answer is what makes the framework's structural choices visibly worth the abstraction. The supplier in §0 needs the multi-regime answer. The framework provides it.

> **THE ANSWER, STRUCTURALLY**
>
> *PDCA+ supports assurance toward a regime by holding the evidence shapes, classifications, translation rules, and shared capabilities a regime requires, and by continuously surfacing the inadequacies that would otherwise become audit-time gaps. The same machinery supports the next regime, and the next, because the operational reality is held once and the regime-specific addressing is what accumulates. Multi-regime assurance becomes additive work rather than multiplicative.*

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.