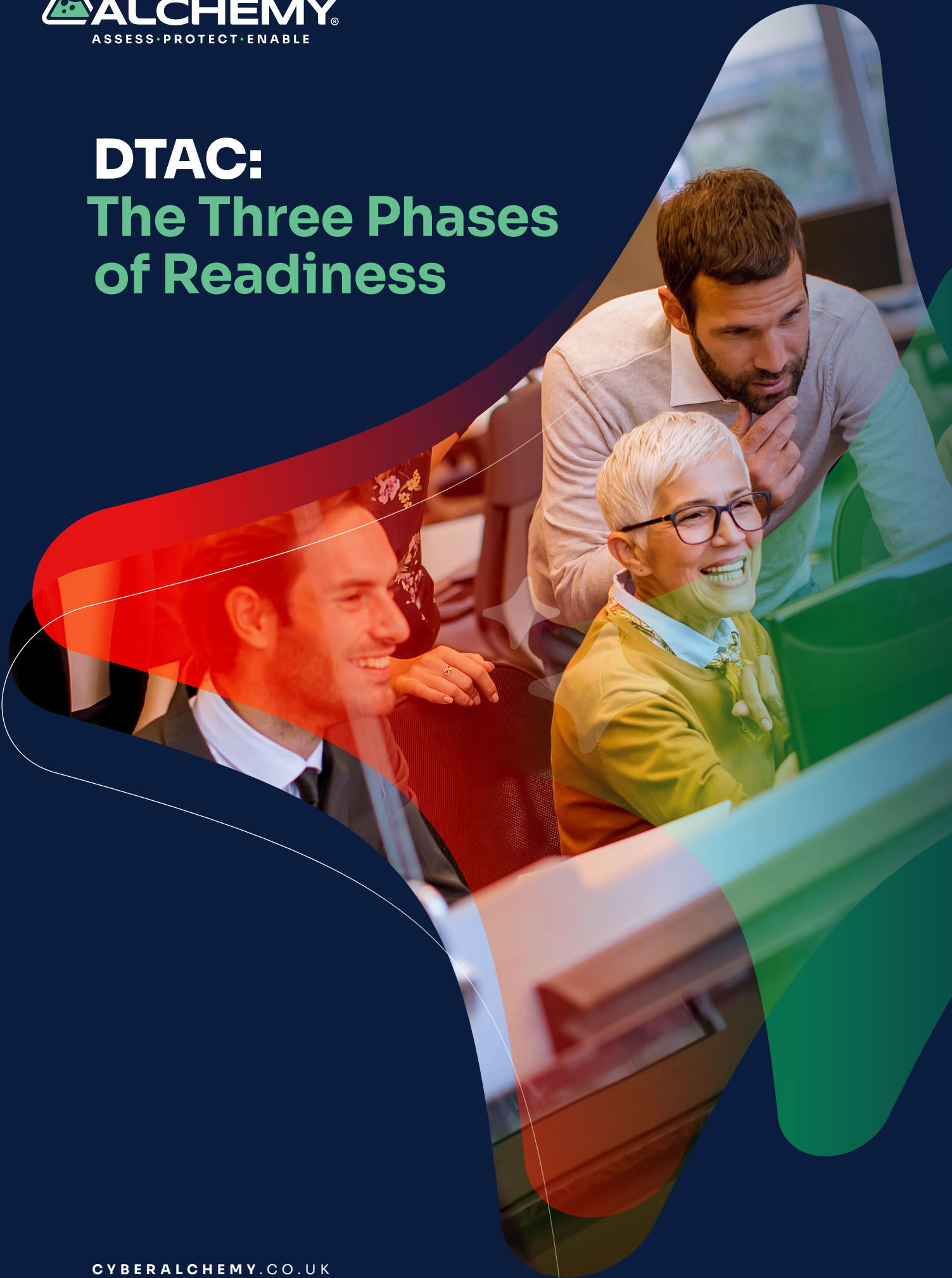


DTAC: The Three Phases of Readiness



DTAC: The Three Phases of Readiness

As should be clear by now, DTAC is used by NHS and social care organisations **during procurement and due diligence** for digital health tools, including pilots. You'll be expected to provide evidence and keep it current as your product changes. Each development phase requires you to produce evidence artefacts aligned to official DTAC guidance. Your aim is to be **assessable early**, produce objective proof, and run the pack as a **lifecycle process**.

The Phases		
1	Phase 1	Define and Organise. You are making yourself assessable early, before procurement pressure.
2	Phase 2	Implement and Prove Controls. You'll provide testable evidence that controls are in place and working.
3	Phase 3	Package for Review and Run as a Lifecycle Process. Ensure your product is procurement-ready and maintainable.



EU MDR and FDA 510(k) phased plans are available as **download via QR code**.

Phase 1: Define and Organise (Be Assessable Early)

PHASE 1	Action (what to deliver)	Why it matters	Deliverable (evidence output)
	Download the current DTAC question set and identify which parts apply to your product.	Avoid late rework and “we didn’t realise this applied” blockers.	DTAC applicability notes + question-to-evidence map (v1).
	Create a DTAC evidence index (single source of truth).	Prevents evidence drift and makes adopter review faster.	Evidence index with owners and review dates.
	Define system boundary, data flows, and trust boundaries (device/app/cloud/integrations).	Clarifies scope and responsibilities; underpins security testing and procurement answers.	Boundary and data flow diagram (1 page).
	Security risk assessment and threat model.	Shows risks have been identified and mitigations are traceable. Underpins secure development.	Threat model + risk register (owned and current).
	Define ‘we control’ / ‘customer controls’ / ‘shared responsibilities’.	Adopters need to understand what you require from their environment and how you will integrate.	Responsibility matrix and minimum environment assumptions.
	Plan external assurance activities (if needed) and book lead-time items.	Pen testing and certification lead-times can block procurement timelines.	Assurance plan and scoped statements of work.
	Plan to obtain a valid Cyber Essentials certificate and review the requirements for the certification.	DTAC C3.1 requires a valid Cyber Essentials certificate to pass.	Project plan of requirements to achieve Cyber Essentials and shortlist of providers for certification.
	Review the Cyber Security Charter for Suppliers to the NHS and decide whether signing it is the chosen route for DTAC C3.2.	DTAC C3.2 asks this question; a “Yes” answer changes the rest of the C3 path.	Cyber Security Charter decision note + owner and internal approval plan.
	Review the DSIT/NCSC Software Security Code of Practice requirements and map current practice against them for DTAC C3.4.	Early gap analysis prevents late rework and shows what evidence you need across secure design/development, secure build, secure deployment/maintenance, and communication with customers.	C3.4 gap assessment + phased implementation plan + evidence checklist.

Phase 2: Implement and Prove Controls (Produce Proof)

2A – Implement Controls (Build what the Regulation and Threat Model Requires).



Phase 1 gives you your threat model and risk register.

Phase 2 is where you turn that analysis into implemented, operational controls and evidence-ready ways of working.

PHASE 2A

Action (what to deliver)	Why it matters	Deliverable (evidence output)
Convert the Phase 1 threat model into security requirements and a prioritised backlog.	Ensures security is engineered into the product rather than added late; makes controls traceable.	Security requirements list + mapped backlog epics (risk > control).
Implement identity and access controls (MFA, least privilege, admin boundaries, break-glass, joiner/mover/leaver basics).	Adopters will probe who can access production, data, and remote support; this is a common blocker.	Access control record + admin account inventory + JML checklist.
Implement secure-by-default configuration baselines (cloud, APIs, dashboards) and change control.	Prevents misconfiguration incidents; provides evidence of operational discipline.	Baseline configuration standard + change/review workflow (e.g., IaC/peer review rule).
Implement secure development controls aligned to your lifecycle (code review, protected branches, CI/CD access controls, secrets management).	Provides assurance that security risks are controlled during build and release.	SDLC control summary + CI/CD access policy + secrets handling approach.
Implement dependency management (approved sources, version pinning, update policy) to support SBOM and vulnerability response.	Underpins vulnerability handling and reduces supply chain risk.	Dependency intake rules + release checklist items (SBOM generation handled in 2B evidence).
Implement the required mitigations identified in the threat model.	This is the “so what” of threat modelling; reviewers expect the top risks to have concrete mitigations.	“Top mitigations implemented” register (risk > mitigation > status).
Implement secure update/patch capability (or compensating controls if updates are constrained).	Procurement teams want to know you can remediate issues after deployment.	Patch/update approach summary (mechanism + constraints + compensating controls).
Implement the organisational and technical controls needed to meet Cyber Essentials requirements across the supported systems and services.	Planning alone is not enough; the certification depends on the controls being in place before assessment.	Cyber Essentials controls implementation log + remediated gaps + readiness checklist.
Implement logging and operational visibility for security-relevant events (admin actions, auth failures, key workflow changes).	Enables detection, investigation and evidence of control operation over time.	Logging specification (what/where/retention/access) + alerting/high-risk events list.
Establish incident reporting route and response roles (including clinical safety escalation where relevant).	Ensures fast escalation and consistent comms during incidents; for some products used in clinical decisions, DCB0129/0160 may apply.	Incident roles/escalation map + reporting route + draft comms templates.
Prepare the internal approvals and organisational commitments needed to sign the Cyber Security Charter, if this is the chosen route for DTAC C3.2.	Ensures the answer to C3.2 is supportable and aligned to named owners and organisational commitments.	Internal approval record + charter readiness note + named signatory.
Implement the controls and working practices needed to support DTAC C3.4 across secure development, secure build environment, secure deployment/maintenance, and communication with customers.	Turns the Phase 1 gap assessment into implemented controls and evidence-producing ways of working.	Implemented C3.4 control set + owners + evidence locations.
Publish a vulnerability disclosure route and define intake handling.	Supports C3.4 because the Software Security Code of Practice expects an effective vulnerability disclosure process and a confidential reporting route.	Published vulnerability disclosure policy / security contact + triage workflow.
Establish remediation governance (triage rules, severity model, decision records, retest triggers).	Turns findings into closure with an audit trail; avoids “we have a report but no process”.	Remediation workflow + decision/retest record template.
Implement third-party and contractor access boundaries (named accounts, MFA, least privilege, offboarding).	Supplier access is a common weak point; adopters ask how it's controlled.	Supplier/contractor access standard + offboarding checklist.

Phase 2: Implement and Prove Controls (Produce Proof)

2B – Generate Objective Evidence (What you can Show).

PHASE 2B

Action (what to deliver)	Why it matters	Deliverable (evidence output)
Engage a cybersecurity provider to obtain Cyber Essentials certification for DTAC C3.1.	DTAC C3.1 requires a valid Cyber Essentials certificate to pass.	Cyber Essentials certificate + certificate ID + expiry date.
Sign the Cyber Security Charter for Suppliers to the NHS, if this is the chosen route for DTAC C3.2.	DTAC C3.2 asks this question, and a “Yes” answer changes the remainder of the C3 path.	Signed Cyber Security Charter evidence + date + owner.
Compile the C3.4 Software Security Code of Practice evidence pack and final confirmation.	DTAC C3.4 asks for confirmation against the Code and needs evidence across secure design/development, secure build, secure deployment/maintenance, and communication with customers.	C3.4 evidence pack + confirmation statement ready for review.
Run security testing aligned to the system boundary (internal and independent where appropriate).	Objective testing evidence is often requested during DTAC technical assurance conversations.	Test scope statement + report(s) + remediation tracker.
Produce resilience/performance evidence where relevant (availability, load/performance limits).	Some DTAC technical assurance approaches include resilience/performance evidence for deployed services.	Load/performance test summary (where applicable).
Document External Penetration Testing Evidence (C3.3): provide an external penetration test summary report for internet-based products or internet-accessible services, completed within the previous 12 months and covering OWASP Top 10 vulnerabilities.	DTAC v2.0 explicitly requests an external penetration test summary report for applicable internet-facing products.	External penetration test summary report: scope, date, third-party supplier, OWASP Top 10 coverage, and remediation status/CVSS outcomes.

Phase 3: Make it Reviewable and Maintainable (Procurement-ready)

-  **Phase 2** gives you implemented controls and objective proof.
Phase 3 turns that work into a pack adopters can review quickly
 – and a process you can keep current as the product changes.

PHASE 3

Action (what to deliver)	Why it matters	Deliverable (evidence output)
Assemble the DTAC review bundle: cover sheet, evidence index, and “how to read this pack”.	Reviewers need orientation and a single entry point; reduces back-and-forth.	DTAC pack cover sheet + evidence index + pack navigation notes.
Complete DTAC responses with direct evidence links (architecture, controls, tests, policies, records).	Adopters decide readiness based on evidence, not statements.	Completed DTAC response pack with stable evidence links.
Close high-risk findings and record re-test outcomes or residual risk rationale.	Unresolved critical findings undermine credibility and can stall adoption.	Remediation log + re-test note(s) / residual risk decision record.
Freeze an “evidence pack release” (v1.0) and run an internal adopter-style review.	Prevents contradictions and broken links; improves readability.	Evidence pack v1.0 + internal review checklist + review log.
Define refresh triggers that match Phase 2 activities (new release, new integration, supplier change, major config change, new vuln class) and set a review cadence.	Reviewers often ask “what changed since last review?”; stable links prevent rework.	Change log (date, change, artefacts updated, version) + link integrity check record.
Schedule recurring assurance activities (risk-based testing, vulnerability monitoring reviews, incident tabletop).	Ensures “controls remain effective” beyond the initial review.	Annual/quarterly assurance calendar + outputs referenced in pack.