The Essential Guide to SaMD and Medical Device Security

A Practical Roadmap for Market Access, Clinical Safety, and Regulatory Readiness.

CYBER ALCHEMY®

ASSESS·PROTECT·ENABLE

Contents

Foreword

Neil Richardson
Cyber Alchemy

I've spent years working with medical device companies. From early-stage clinical founders building their first SaMD product to established device manufacturers preparing for international expansion, one thing I see happen repeatedly. The companies that reach healthcare procurement fastest aren't the ones who bolt security on at the end. They're the ones who built it in from the start. They pass DTAC assessments without scrambling. They answer EU notified body questions with confidence. They demonstrate FDA readiness without months of rework.

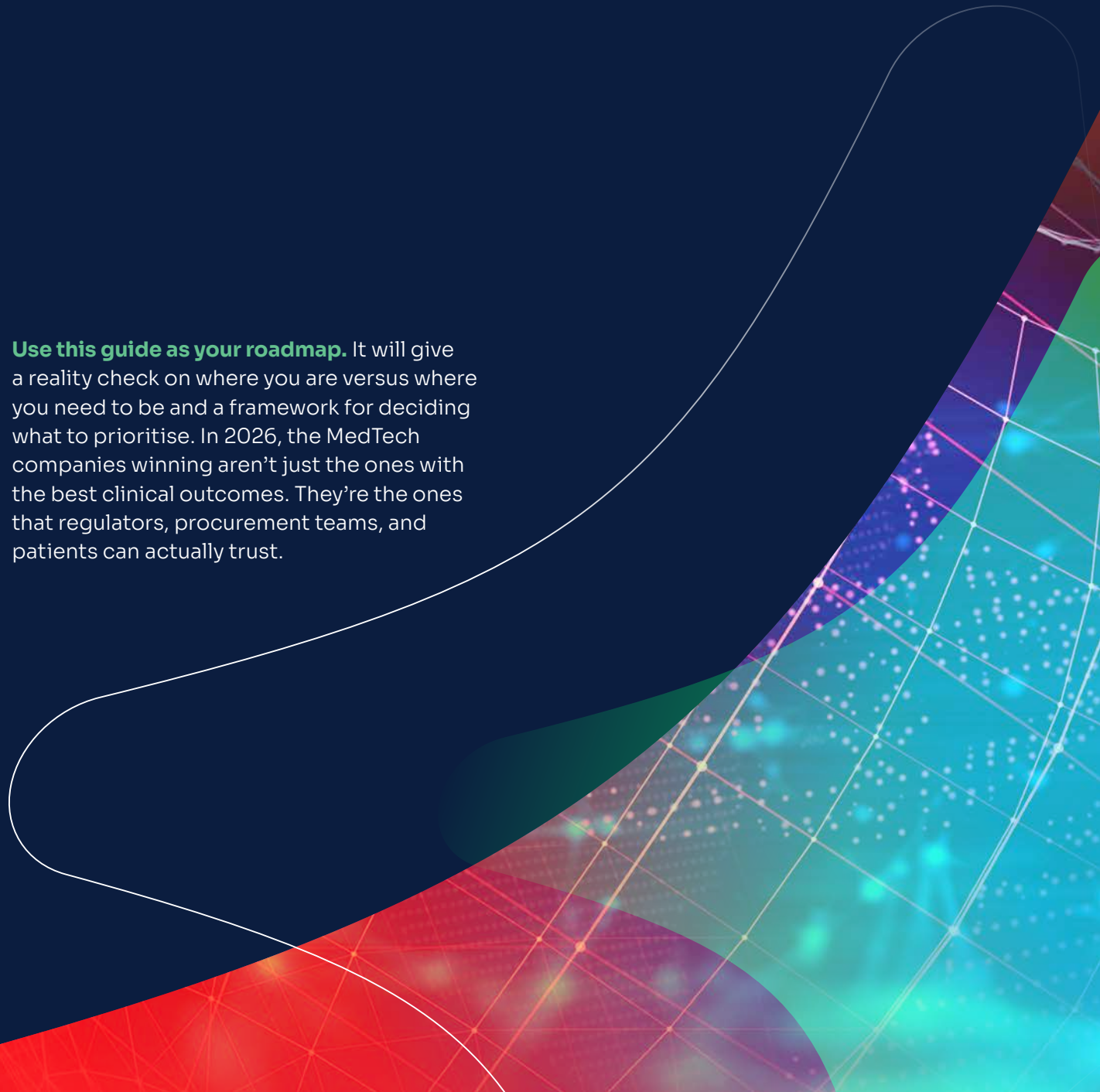
Security done right doesn't slow you down. It removes the friction from everything that matters. When you can demonstrate mature controls and clear governance, doors open faster.

The companies struggling are often the ones who treated cybersecurity as something to worry about later. 'Later' becomes 'now' the moment an NHS procurement team asks for your Cyber Essentials certificate and you don't have one. When your penetration test comes back with critical findings that need three months to fix. Or when you realise your SBOM doesn't exist (and it should have for months).

This guide exists because medical devices, including Software as a Medical Device (SaMD), are treated differently than technology in other sectors. You're building systems that directly impact patient safety, working under constant regulatory scrutiny from MHRA, notified bodies, and the NHS, and ultimately handling sensitive clinical data. The stakes are higher, and the evidence requirements are more demanding.

Inside, you'll find practical guidance on what DTAC (Digital Technology Assessment Criteria, the due diligence procurement assessment for digital health devices to access the NHS) actually requires. You'll find the specific evidence that medical device companies need to produce to get through procurement and regulatory approval. You'll also see where security adds genuine business value: (Faster DTAC assessments, smoother submissions and reduced review times).

Use this guide as your roadmap. It will give a reality check on where you are versus where you need to be and a framework for deciding what to prioritise. In 2026, the MedTech companies winning aren't just the ones with the best clinical outcomes. They're the ones that regulators, procurement teams, and patients can actually trust.



Medical Devices: Security is the Route to Market

Clinical performance gets you noticed. Security (and evidence) gets you deployed. That's the reality facing MedTech and Medical Device teams in 2026.

Whether you're accessing the UK, EU or USA, compliance reviewers are no longer asking whether your device works. They are asking whether you can prove it is **safe to deploy** in a connected clinical environment, and whether it will remain safe over its lifetime.

That shift to lifetime responsibility means medical devices are assessed across their entire deployed lifetime, not just at the point of approval, not one-time approvals. Security evidence is required at pilot stage, at procurement, and at every product update thereafter. It's an ever-present responsibility.

You might know you're secure, but **no evidence** means **no deployment**, regardless of how good your device is clinically. Security unlocks market access. It does not slow it down.

Cybersecurity Evidence: How it looks on the route to market

Pilot-ready

You can answer basic security questions and provide a lightweight evidence pack to partner organisations.

Procurement-ready (NHS tenders)

Full evidence pack with Cyber Essentials, independent test evidence, and post-market plan.

International-ready

Evidence pack adapted for EU MDR technical documentation or FDA 510(k) submission requirements.

A full international roll-out is beyond the scope of this guide. Instead, we'll focus on the fundamentals of accessing the UK market: DTAC. We'll cover exactly what evidence you'll need to produce and when to produce it, structured around the UK DTAC path.

We'll still include EU and USA (FDA) tips where relevant, but those will be covered in more detail in other guides (or you can **contact us now** if you need support).

The Threat Landscape

Medical Device compliance isn't just about everyday cybersecurity threats like phishing and ransomware. It's about understanding what healthcare providers and regulators now formally require for market approval based on the failures and breaches they see most frequently in medical devices.

Where attacks actually happen in MedTech

Understand these as repeatable failure patterns experienced by medical devices of all kinds. They are not theoretical scenarios, but real-world risks facing all healthcare suppliers.

- **Identity and access.**
  E.g. Unauthorised APIs, weak admin boundaries, missing MFA on deployment and maintenance routes.
- **Supply chain.**
  E.g. Vulnerable third-party libraries, unmanaged dependencies, no SBOM.
- **Update and maintenance gaps.**
  E.g. No secure update mechanism, patch policy commitments that do not hold in practice.
- **Operational disruption.**
  E.g. Ransomware affecting clinical services through connected devices.
- **External attack surface.**
  E.g. Exposed services, misconfigured cloud infrastructure, insecure APIs.
- **Remote access paths.**
  E.g. Abuse of legitimate deployment and maintenance channels, including exposed services, misconfigured cloud, and insecure APIs.
- **Organisational hygiene.**
  Baseline controls still matter, including MFA, least privilege, and secure admin (though procurement and regulators focus on product and system evidence).

If you are building AI into your product

Every MedTech company embedding AI or Machine Learning (ML) into their device faces an expanded security surface that **standard security practices might not automatically cover**. AI models are software artefacts: treat ML models as controlled release artefacts (versioned, traceable, monitored). Track ML frameworks/dependencies in your SBOM. Adversarial inputs, model drift, and supply chain risk for AI frameworks are threat categories your threat model must address explicitly that are then remediated through robust design and evidenced through validation.

The EU AI Act (covered in section 2.2) adds formal governance duties if your product is classified as high-risk AI. Section 2.2 covers both the product security implications and the regulatory overlay in full.

Post-market surveillance as a security requirement

Post-market surveillance is now a security expectation across the UK, EU and USA. Medical devices are assessed across their entire deployed lifetime, not just at the point of approval. Vulnerabilities may be discovered after deployment. Your evidence pack must include a credible plan for monitoring, triaging, and remediating issues in the field, not only at launch. Note, DTAC does not always ask for full postmarket cyber operations explicitly, but NHS buyers will often probe how you handle vulnerabilities and updates after go-live as part of their own due diligence.

Key message: Regulators expect you to maintain security after deployment, not just at launch. That means having a documented process for monitoring new vulnerabilities, deciding how serious they are, and fixing them. Without this, your evidence pack is incomplete.

SBOM: Explainer

A Software Bill of Materials (SBOM) is a complete inventory of every third-party component your product uses (libraries, dependencies, frameworks) and the versions of each. Think of it as an ingredients list for your software. Regulators use it to check whether any components have known security flaws, and you need it to answer the question "are we affected by this vulnerability?" quickly and with evidence.

In 2021, a critical vulnerability was discovered in Log4j, a logging library embedded in thousands of products. Companies with a current SBOM could answer "are we affected?" within hours. Companies without one spent days or weeks just trying to find out. That gap is exactly what regulators are trying to close by requiring it.

Want Access to the UK Market? Time to Make Friends with DTAC

DTAC (Digital Technology Assessment Criteria) is the gateway to NHS and social care procurement for digital health tools. NHS and social care organisations use it during procurement and due diligence, including pilots, so if you have any chance of working with them, you need to be aware of DTAC requirements, provide evidence and keep it current as your product changes.

DTAC Simplified: The 5 Domains

DTAC assesses five domains. It is important to understand all five, because assessors review them together. This guide focuses on the technical assurance and cybersecurity elements because those are where MedTech companies most commonly stall.

	DTAC Domain	What is Assessed
1	**Clinical Safety**	Are clinical risk management activities in place? Is there evidence that clinical hazards introduced by the technology have been identified and mitigated?
2	**Data Protection** Supported by **Cyber Alchemy**	Does the device ensure privacy by design? (That means GDPR/ DPA 2018 compliance, DPIAs where required, and protection of individual rights).
3	**Technical Assurance** Supported by **Cyber Alchemy**	Is the product secure and stable, covering Cyber Essentials, penetration and vulnerability testing, access controls, patching, and incident handling.
4	**Interoperability**	Is data communicated and integrated accurately, quickly, and safely? (This covers APIs, HL7/FHIR standards, and integration security).
5	**Usability and Accessibility**	Does it conform with NHS service standards and good practice for usability and accessibility?

DTAC Readiness:
5 Questions to Ask Your Team

Note: These are self-check prompts, not official DTAC wording.
They'll help you identify gaps before you start.

	DTAC Readiness Self-check	
1	**Clinical Safety**	"Can we explain what new or changed risks our technology introduces in real clinical use, and show how we've assessed and controlled them?"
2	**Data Protection**	"Can we clearly describe what data we handle, the lawful basis/purpose, where it flows and is stored, and show the key privacy-by-design decisions we've made?"
3	**Technical Assurance**	"Can we demonstrate a robust security posture, show how we prevent common security failures and how we will operate safely after go-live (monitoring, vulnerability handling, updates/patching, and incident response) – with evidence, not intent?"
4	**Interoperability**	"Where we integrate with other systems, can we show that data exchange is accurate, secure, and well-bounded (interfaces, authentication, authorisation, and responsibilities) – and that we can support it reliably?"
5	**Usability and Accessibility**	"Can we show that real users can use the product safely and effectively, and that we've considered accessibility needs – with test results and documented decisions?"

It's not enough to answer 'yes' to these. You have to be able to show it with evidence.

DTAC Technical Security Requirements: Simplified Summary of DTAC C3

Within the technical assurance domain, the cybersecurity evidence most commonly required includes:

	Cybersecurity Evidence
1	**Cyber Essentials (C3.1).** Attach a valid Cyber Essentials certificate.
2	**Cyber Security Charter (C3.2).** Confirm whether you have signed the NHS Cyber Security Charter. If yes, you skip the remaining C3 questions.
3	**External Penetration Testing (C3.3).** For internet-based or internet-accessible products, provide a third-party pen test summary report from the last 12 months, covering OWASP Top 10.
4	**Secure Software Development (C3.4).** Confirm software is produced in line with the DSIT/NCSC Software Security Code of Practice.
5	**Operational Security Controls (C3.5–C3.6).** Confirm an MFA plan is in place, privileged supplier access uses MFA where applicable, and logging/reporting requirements are defined.

Note: individual NHS Trusts may apply DTAC differently, but the five domains and their core evidence requirements remain consistent. The DTAC question set and evidence map is the starting point. Pull it early and map your answers before you need to answer them under procurement pressure.

1 Cyber Essentials

Valid certificate covering systems and services supporting the product.

4 4 Secure Software Development

Confirm adherence to secure design, secure build, secure deployment and maintenance, and customer communication principles.

The new mandatory governance for some AI-driven clinical tools.

- Do you handle NHS patient data directly? DSPT may apply.
- Is your product used for clinical decisions? DCB0129/0160 may apply.
- Are you integrating with NHS systems? Additional integration testing may be required.

Approximate timeline from zero to DTAC-ready (assuming no major gaps): **4 to 6 months.**

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)

FSN template is available as **download via QR code**.

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.	Review the Cyber Security Charter for Suppliers to the NHS and decide whether signing it is the chosen route for DTAC C3.2.
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).

PHASE 2A

Action (what to deliver)	**Why it matters**	**Deliverable** (evidence output)
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).	Establish incident reporting route and response roles (including clinical safety escalation where relevant, e.g. for some products used in clinical decisions).	Ensures fast escalation and consistent comms during incidents; for some products used in clinical decisions, DCB0129/0160 may apply.
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.
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.
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.

Access to Markets:
Key Differences and Overlaps

Although the focus of this guide is DTAC, it's worth considering how much of DTAC can be reused as you seek to access other markets. Once your UK evidence pack is built, it serves as a platform to build upon to expand into EU or US markets as core documentation and evidence is reusable with minor tailoring.

What is the crossover?

Key:

- **Explicitly required/assessed**.
- **Conditional** (depends on product/scenario).
- **Expected evidence** (commonly needed to demonstrate conformity).
- **Not specified** as an explicit requirement.

Important scope note: FDA statutory 524B requirements apply to devices meeting the definition of a 'cyber device'. For other devices, FDA guidance provides nonbinding recommendations on what to include in a 510(k) submission when cybersecurity risk exists.

TABLE ONE

Cybersecurity Evidence Area (what to deliver)	**DTAC** (UK NHS)	**EU MDR** (with MDCG 2019-16 rev.1)	**FDA 510(k)** (with 524B for 'cyber devices')	**Overlap and Practical Notes**
Baseline Organisational Assurance (Certifications).	✓ Cyber Essentials certificate requested in DTAC (C3.1). ✓ Signed Cyber Security Charter for Suppliers to the NHS (C3.2). ✓ Software Security Code of Practice confirmation (C3.4).	✗ No specific organisational certification mandated by MDR; focus is device lifecycle risk management and evidence.	✗ No specific organisational certification mandated. ◻ QMS-linked cybersecurity processes expected in submissions; 524B focuses on device processes rather than org certification.	DTAC is uniquely prescriptive about Cyber Essentials. For EU/FDA, certifications can help procurement but are not the regulatory 'core'.
Secure Development Lifecycle (SDLC) and Governance.	◻ DTAC v2.0 does not prescribe a named SDLC framework, but C3.4 expects evidence across secure design/development, secure build, secure deployment/maintenance, and customer communication.	✓ MDR Annex I links state-of-the-art development life cycle, risk management including information security, verification and validation (MDCG highlights Annex I 17.2).	◻ FDA guidance recommends using a Secure Product Development Framework (SPDF) within the quality system; scaling with risk.	EU and FDA both emphasise lifecycle integration of cybersecurity. In practice, IEC 81001-5-1 can anchor your processes (if you adopt it).
System Security Architecture, Boundaries and Data Flows (Device/App/Cloud).	◻ Not a named DTAC upload, but strong supporting evidence for C3.4 because it underpins secure design, deployment, maintenance, and customer communication.	◻ Expected as part of technical documentation to demonstrate conformity and justify/verify security solutions; MDCG emphasises architecture as part of evidence.	◻ FDA guidance includes 'Security Architecture' and 'Architecture Views' as submission documentation (Appendix 2 provides diagrams/flows).	Strong overlap for submission-grade evidence: a clear boundary diagram + trust boundaries reduces assessor friction, especially for connected device + cloud.
Security Risk Management and Threat Modelling (Threats > Controls > Residual Risk)	◻ DTAC does not name a standalone threat model upload, but under C3.4 it is strong supporting evidence for secure-by-design development.	✓ Risk management system required (Annex I section 3) and cybersecurity risk should be included; MDCG discusses security risk assessment and threat modelling.	◻ FDA guidance includes Security Risk Management and Threat Modelling; for 524B, processes/procedures for reasonable assurance are required.	Common core: threat modelling + cybersecurity risk assessment that ties back to safety risk management (and stays maintained as the design evolves).

TABLE TWO

Cybersecurity Evidence Area (what to deliver)	**DTAC** (UK NHS)	**EU MDR** (with MDCG 2019-16 rev.1)	**FDA 510(k)** (with 524B for 'cyber devices')	**Overlap and Practical Notes**
Third-party Software Components and Dependency Management.	Not explicitly named in the DTAC form, but strong supporting evidence for C3.4 because the Code expects component identification, integrity checks, testing, and update management.	Commonly needed to show control of vulnerabilities in libraries, OS components, and other third-party software across the lifecycle.	FDA guidance includes 'Third-Party Software Components'; for 524B cyber devices, SBOM is explicitly required.	EU/FDA are more explicit on software supply chain; DTAC is lighter, but NHS procurement often still asks. Aligning with SBOM practice reduces rework.
Cybersecurity Testing Evidence (what was tested and how often).	For internet-based / internet-accessible products, must provide an external penetration test summary report from the previous 12 months, including OWASP Top 10 coverage (C3.3).	MDCG states technical documentation should include methods/results of security testing as justification/verification of adopted solutions.	FDA guidance includes 'Cybersecurity Testing' and expects evidence scaled with risk.	All three benefit from a simple 'test evidence index': scope, method, results summary, and follow-up actions.
Minimum IT Requirements, Secure Configuration and User-facing Security Information.	DTAC asks about APIs, interoperability standards, open API practice/documentation, and integration with NHS/local systems where relevant (C4.1–C4.2.6).	MDR Annex I includes minimum IT requirements and protection against unauthorised access; MDCG references minimum IT requirements (Annex I 17.4/23.4).	FDA guidance contains labelling recommendations for devices with cybersecurity risks (secure setup, configuration, maintenance information).	Overlap: publish a one-page 'Secure deployment and operation' note: prerequisites, ports/ protocols, roles, update approach, logging expectations.
Post-market Surveillance (PMS) and Ongoing Cybersecurity Monitoring	DTAC does not impose a full PMS regime, but C3.4 strongly supports a lightweight post-release process for vulnerability triage, update decisions, customer communications, and evidence refresh.	MDR includes pre- and post-market aspects; MDCG states technical documentation should be updated with PMS information related to handling/remediation of incidents and vulnerabilities.	For 524B cyber devices: must submit a plan to monitor, identify and address postmarket vulnerabilities/exploits. For other devices: postmarket management is strongly recommended by FDA guidance.	EU MDR is strongest here as a formal lifecycle regime. DTAC is lighter, but no longer silent because C3.4 clearly points to ongoing maintenance and communication.
Coordinated Vulnerability Disclosure (VDP) /Intake Channel	Not a standalone DTAC upload, but strong supporting evidence for C3.4 because the Code expects a published vulnerability disclosure process and confidential reporting route.	Not an explicit MDR requirement as a named artefact in MDCG, though handling vulnerabilities/ incidents is part of lifecycle expectations.	For 524B cyber devices: postmarket plan must include coordinated vulnerability disclosure and related procedures.	Cross-market best practice: publish a VDP contact channel and triage process. Mandatory for many FDA 'cyber devices' and widely expected by enterprise buyers.

TABLE THREE

Cybersecurity Evidence Area (what to deliver)	**DTAC** (UK NHS)	**EU MDR** (with MDCG 2019-16 rev.1)	**FDA 510(k)** (with 524B for 'cyber devices')	**Overlap and Practical Notes**
Patching, Updates and Remediation Capability.	Not explicitly required within DTAC but C3.4 now asks suppliers to confirm adherence to the Software Security Code of Practice, including secure deployment and maintenance.	MDCG describes modifying risk control measures/corrective actions/ patches and updating technical documentation through PMS.	For 524B cyber devices: must make available postmarket updates and patches; processes/ procedures for reasonable assurance are required.	Cross-market: a clear 'secure update/patch policy' (delivery method, prioritisation, emergency vs routine cadence) is high leverage.
Software Bill of Materials (SBOM).	Not explicitly named in DTAC v2.0. Practical way to evidence component control and vulnerability management under C3.4.	Not explicitly required as a named MDR/IVDR artefact, though often useful for component transparency and vulnerability management.	For 524B cyber devices: SBOM is explicitly required in premarket submissions.	Treat SBOM as: FDA-required (when applicable), EU-helpful, DTAC/procurement-friendly. Maintaining SBOM per release reduces late-stage submission pain.
Interoperability and Secure Integration Controls.	DTAC interoperability section asks about APIs, applicable interoperability standards, open API practice/ documentation, and integration with NHS/local systems (C4.1–C4.2.6).	MDR Annex I includes interaction between software and the IT environment and interoperability/compatibility requirements; MDCG highlights these areas.	FDA guidance includes interoperability considerations and expects interface/ connection risks addressed.	Overlap: define scope boundaries and shared responsibilities (device vs app vs cloud vs hospital IT) to avoid gaps in threat modelling and procurement questionnaires.
Privacy/Data Protection Controls (Cyber-adjacent).	DTAC data protection criteria require ICO registration evidence, product DPIA, transparency materials and fair data-use terms, where personal data is processed (C2.2.1–C2.2.6)	MDCG notes privacy/ confidentiality may be governed by other legislation (e.g., GDPR) and not explicitly in MDR; cybersecurity connects to confidentiality/ integrity/availability.	FDA 510(k) cybersecurity focuses on safety/ effectiveness; HIPAA compliance is separate from 510(k) submission requirements.	Include privacy evidence when handling patient data, but keep it distinct from device cybersecurity evidence to avoid conflating regulatory scopes.

Sources (official): NHS England DTAC assessed section C; MDCG 2019-16 rev.1 (EU); FDA Cybersecurity FAQs (524B); FDA guidance "Cybersecurity in Medical Devices…", issued 3 Feb 2026.

The "One Evidence Pack, Three Markets" Principle

It would be an oversimplification to say accessing all three markets is straightforward. But there are efficiencies.

- **UK DTAC.** The gateway to the NHS. Cyber Essentials, independent testing, core artefacts, post-market basics.
- **EU MDR.** Contains deeper risk management documentation, MDR/IVDR mapping, and PMS integration.
- **US FDA.** Contains detailed SBOM, formal VDP/PSIRT, documented patch/update approach and postmarket processes, and TPLC plan.
- **Approximately 70% of core evidence is reusable with minor tailoring** across all three markets.

Emerging Regulations

Cyber Resilience Act (CRA) and NIS2

CRA reflects a tightening of security and regulations around software and hardware products. NIS2 is concerned with the operational resilience of critical services. The scope for medical devices is nuanced, so treat these as a watchlist item and confirm applicability for your specific product. Contact us now if you're unclear whether they apply to you.

For companies at an early stage, focus on becoming UK pilot-ready first (DTAC).

The EU AI Act: (High-risk AI in MedTech)

If your product uses AI to support diagnosis, treatment decisions, triage, or clinical decision support, the EU AI Act may classify it as high-risk.

If your AI is a medical device (or a safety component) and your route to market requires third-party conformity assessment, you should assume you will need AI-specific governance and evidence alongside your cybersecurity programme.

Here's a quick primer:

Step 1: Confirm Whether you are High-risk

An AI system is high-risk when either: (a) it is a safety component of a regulated product or is itself a regulated product, and that product must undergo third-party conformity assessment; or (b) it falls into one of the high-risk use case categories listed in the Act.

Step 2: The Six Governance Requirements for High-risk AI

1. Risk management that is AI-specific: bias, failure modes, misuse, performance drift, and cybersecurity threats across the lifecycle.
2. Data governance you can defend: provenance, representativeness, bias assessment, train/test separation.
3. Technical documentation that stands up to scrutiny: intended purpose, limitations, performance claims, validation approach.
4. Human oversight designed into the workflow: clinicians must be able to understand when to rely on, challenge, or override the AI.
5. Logging, traceability and auditability: operational records to reconstruct what happened and to detect issues early.
6. Accuracy, robustness and cybersecurity as ongoing duties: maintain performance and resilience in real-world conditions over time.

Naturally you'll be expected to provide evidence that you can meet these requirements.

The AI Act entered into force in 2024, with a general date of application of 2 August 2026 and an extended transition for some products expected by 2027. Treat this as a roadmap item now, but don't get blind sided.

Five Questions to Ask About AI Security.
(if Your Product uses AI)

1. What is the AI doing, and what clinical decision does it influence?
2. Where does the data come from, and can you defend representativeness and bias controls?
3. How do you keep performance stable? (monitoring, drift detection, update triggers)
4. How does a clinician stay in control? (oversight, override, instructions, boundaries)
5. What evidence pack will you hand to an assessor or procurement team without scrambling?

What do you Actually Need to Produce?

The artefacts in this section represent the full evidence picture across DTAC, EU MDR, and FDA. For DTAC, many of these are best practice rather than hard requirements, but building them early means you are not starting from scratch when you move to MDR or FDA. The artefacts table (section 2) indicates the requirement level for each standard.

1) Secure Software Development Lifecycle (SSDLC)

In MedTech, “secure at the end” is too late. A Secure Software Development Lifecycle (SSDLC) builds security into **every** stage of delivery, from requirements to post-market support. That means vulnerabilities are found early, fixed cheaply, and documented with evidence as you go.

EU MDR and FDA 510(k) do not explicitly require a named SSDLC, but both expect evidence of secure lifecycle development and risk management. For DTAC, it is not mandated by name, but the evidence it produces (documented threat model, traceability, test records) build a strong security foundation that leads to robust security and an efficient security program. Companies that build to SSDLC standard from the start find DTAC straightforward; companies that do not often struggle to evidence decisions they made informally.

In practice, we start by defining **security requirements** alongside **clinical and functional requirements**, then design the system with clear **trust boundaries, data flows and threat scenarios**.

During build: developers follow secure coding practices backed by automated checks (static code analysis and dependency/supply-chain scanning) and disciplined peer review.

In testing: we combine automated and manual security testing to confirm the system behaves safely under realistic attack conditions.

Before release: security gates confirm the build is deployable in a controlled, repeatable way.

After deployment: monitoring, vulnerability intake and patch processes keep the product safe over its lifetime (because connected devices are “living products”, not one-off releases).

For regulated products, SSDLC also provides a clean standards backbone:

IEC 62304. Software lifecycle processes: planning, requirements, design, implementation, verification, maintenance.

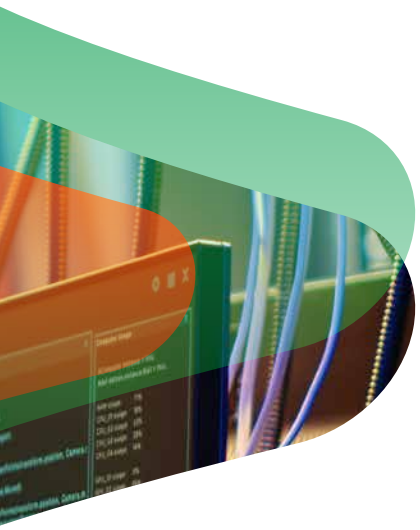
ISO 14971. Risk management across the device lifecycle: identify hazards, evaluate/control risks, monitor effectiveness.

IEC 81001-5-1. Security lifecycle activities for health software: a framework of processes, activities and tasks to increase cybersecurity across the product lifecycle.

ISO 13485. QMS discipline: design controls, documentation, change control, and verification culture.

ISO 27001. Information security controls that commonly underpin secure development environments and practices.

The outcome: security that scales, and (most importantly) evidence created as you go that accelerates procurement and regulatory conversations with no impact on delivery.



Secure Development Lifecycle for MedTech

Concept and Planning

- Define intended use and environment
- Set security and safety objectives
- Map data flows and interfaces
- Agree evidence and acceptance criteria

Risk Management

- Build risk file to ISO 14971
- Threat model (STRIDE, attack trees)
- Define mitigations and residual risk
- Derive security requirements and controls

Design and Development

- Secure architecture and trust boundaries
- Implement secure coding standards
- SBOM and dependency governance
- Hardening, crypto, key management
- Secure CI/CD and code reviews

Verification and Validation

- SAST, SCA, secrets scanning
- Security test cases and traceability
- Penetration testing and fuzzing
- Validate privacy and encryption
- Remediate findings and retest

Regulatory Approval

- Compile cybersecurity documentation package
- Evidence for IEC 62304 and 81001-5-1
- Support FDA and IMDRF expectations
- Prepare vulnerability disclosure plan
- Supplier and third-party assurance

Launch and Post Market

- Secure deployment and configuration guidance
- Continuous monitoring and telemetry
- Vulnerability intake and triage
- Patch releases and advisory cadence
- Post market surveillance and incident response

1 → 2 → 3 → 4 → 5 → 6

Security activities and evidence mapped to each stage.

2) 10 Core Procurement Artefacts

These are the artefacts most commonly requested by procurement teams, Notified Bodies, and regulators. Build them incrementally. The early ones unlock pilot conversations; the later ones unlock formal submissions.

Key:

- **Mandatory** / will cause delays if missing.
- **Expected** / commonly asked.

TABLE ONE

Artefact	What it is and Why	Minimum Standard	DTAC	EU MDR/ IVDR	FDA 510(k)	Update Cadence
1 **Security Architecture and Boundaries**	Diagram and narrative showing device/app/cloud/integrations and trust boundaries. Shows what you control vs what the customer controls and where data flows.	One diagram (data flows and trust boundaries) plus 1–2 pages on responsibilities.	✓	✓✓	✓✓	On significant design change.
2 **Threat Model and Risk Register**	Top threat scenarios with risk ratings, mitigations, and residual risk rationale. Shows systematic identification and treatment of device-specific threats.	Top scenarios, risk rating (likelihood/impact), mitigations, residual risk rationale, named owners.	✓	✓✓	✓✓	Per major release.
3 **Risk-control Traceability Matrix**	Single table linking threats, controls, verification, and evidence location. Proves controls actually address identified risks with test evidence.	Risk/threat, control, verification method, evidence link, status.	✓	✓✓	✓✓	Quarterly review.

TABLE TWO

Artefact	What it is and Why	Minimum Standard	DTAC	EU MDR/ IVDR	FDA 510(k)	Update Cadence
4 **SBOM and Vulnerability Monitoring**	Software Bill of Materials per release plus documented CVE monitoring workflow. Shows what third-party components you use and how you handle vulnerabilities.	SBOM stored with each release plus documented CVE monitoring/triage process with decision records.	✓	✓	✓✓	Every release; monitoring ongoing.
5 **Vulnerability Disclosure Policy (VDP/ PSIRT)**	Public reporting route, triage process, severity model, escalation. Shows how you handle security issues discovered after deployment.	Public reporting contact, triage steps, severity model, decision owners, comms triggers.	✓	✓	✓✓	Quarterly review.
6 **Secure Update/ Patch Policy**	How you deliver updates: signing, rollback, routine vs urgent timelines. Ensures vulnerabilities can be patched without breaking devices.	Signed updates, rollback/ fail-safe behaviour, routine vs urgent patch timelines, supported versions.	✓	✓✓	✓✓	Annual plus on platform change.

TABLE THREE

Artefact	What it is and Why	Minimum Standard	DTAC	EU MDR/ IVDR	FDA 510(k)	Update Cadence
7 **Security Test Evidence**	Automated scans plus independent testing scoped to system boundary. Verifies controls work in practice.	SAST/DAST/dependency scans with triage logs plus scoped independent testing across system boundary.	✓✓	✓✓	✓✓	Continuous (automated); annually or major change (independent).
8 **Logging/ Monitoring Approach**	What events are logged, alerting triggers, retention, access controls. Shows you can detect and investigate security incidents.	Events logged (admin actions, auth failures, key workflows), alerting, retention, access controls.	✓✓	✓	✓	Per environment change.
9 **Supplier Security Controls**	Vendor due diligence, access boundaries, onboarding/ offboarding, contracts. Covers third-party risk from cloud, manufacturers, and contractors.	Supplier list, access boundaries, onboarding/offboarding, minimum security requirements, incident notification expectations.	✓	✓	✓	Per supplier; annual review.
10 **Incident Response Playbook and Rehearsal**	Roles, escalation, containment steps, evidence you have tested it. Shows you can handle incidents quickly without improvising.	One-page roles/escalation/ comms/containment checklist plus evidence of rehearsal (tabletop exercise minimum).	✓	✓	✓	Rehearse at least annually.

Note: The artefacts above are the core set. There are additional artefacts that may apply depending on your product type, deployment model, and target market. Use this table as a starting reference.

3) System Boundaries: Who Controls What

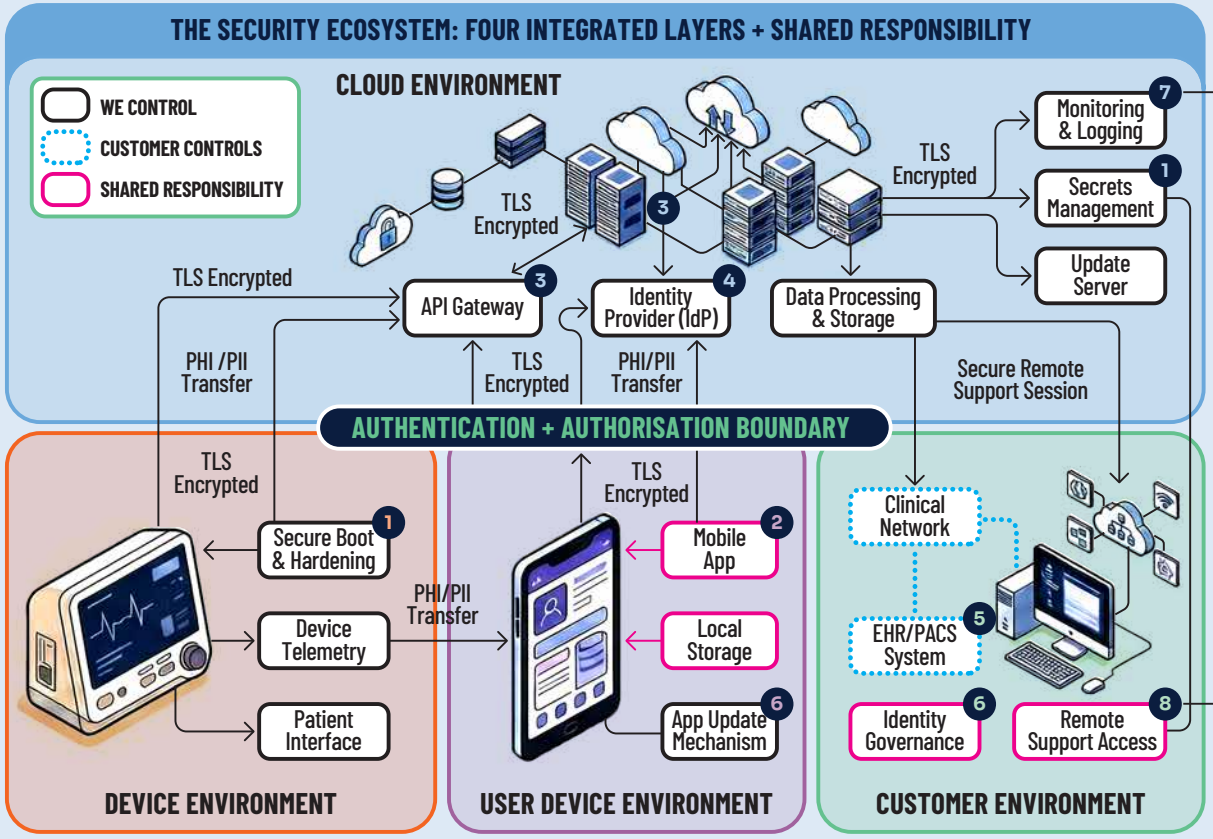
Medical device security covers far more than the physical device. It covers the entire connected system: device, companion app, cloud backend, APIs, and clinical integrations. Defining boundaries early prevents late-stage disputes, procurement confusion, and gaps in your threat model.

Component	Your Security Responsibilities	Customer/ Hospital Responsibilities
1 **Device / Firmware**	Hardening, secure communications, device identity, secure update mechanisms (signing and rollback), tamper considerations (risk-based).	Physical security of device, network segmentation.
2 **Mobile App**	Authentication/authorisation flows, secure local storage, API request integrity, session management, security-relevant logging.	Device OS updates, application installation, user access governance.
3 **Cloud / Backend**	Tenancy isolation, secrets management, encryption boundaries, audit logging, infrastructure-as-code controls, vulnerability scanning (images/dependencies).	Network firewall rules (if private cloud), user identity management integration.
4 **Integrations (EHR, APIs)**	Supported configurations documented, minimum TLS/ auth requirements, API security standards, integration testing scope.	Network controls (firewalls, VPNs), identity governance, endpoint protection, access provisioning/deprovisioning.
5 **Shared Responsibilities**	Vulnerability intake process, incident response co-ordination, patch communications, evidence maintenance.	Reporting suspected incidents, applying patches within agreed timeframes, reviewing security advisories.

Note: Include explicit assumptions in your documentation. For example, “customer manages network segmentation” and “shared responsibility for cloud applies (config, IAM, logging)”. Assumptions left undocumented become disputes.

Bringing it to Life: An Example System Boundary Diagram

MedTech Security: End-to-End System Boundary and Services



Cyber Alchemy Consultancy Services

Technical Security Hardening

- 1 System hardening,
- 3 verification testing, penetration testing, and system architecture.

Clinical Access, Identity & Support Security

- 5 Identity governance,
- 6 IAM/PAM, SSO, privileged access,
- 8 secure remote support.

Lifecycle Security Engagement

- 2 Secure SDLC, CI/CD security, SBOM assurance,
- 4 compliance support,
- 7 vCISO guidance, and post-market security activities.

Data Table: Service Mapping

Service Area	Focus Highlights
Device, App & Endpoint Security	System hardening, secure update implementation, system verification testing plan development and execution.
Application, API & Cloud Security	AuthN/Z, Application, infrastructure and cloud penetration testing, cloud architecture hardening.
Identity, Access & Operational Security	IAM/PAM, SSO, secrets management, privileged access, secure remote support.
Threat Validation, Monitoring & Response	Red/purple teaming, adversary simulation, logging maturity, vulnerability assessment, and incident readiness.
Secure Delivery, DevSecOps & Training	Secure SDLC, CI/CD security, developer enablement training, SBOM assurance and awareness training.
Governance, Compliance & Post-Market Security	DTAC/EU MDR/ FDA510(k) compliance support, vCISO strategy, AI governance, and Cyber Essentials certification.

10 Most Common Failures across DTAC, EU MDR and FDA 510(k): Lessons Learned from Real Product Launches

These failure patterns come directly from real submissions across all three standards. They are not edge cases, and most of them apply regardless of which market you are targeting.

1 Missing Documentation: You built it but cannot prove it

The best security in the world provides zero procurement or regulatory value if it's not documented. If a procurement team asks "show us your architecture" and you have nothing to share, the conversation ends very quickly.

Lesson: Build your evidence index from day one. Document as you build, not after.

2 The "Show Your Working" Failure

Having the right controls is necessary but not sufficient. Regulators and procurement teams need to see the entire documented chain: threat identified, control selected, control implemented, verification tested, evidence filed.

A company that cannot show this chain is indistinguishable from one that has done nothing, even if their actual security is excellent. The chain is the evidence. Procurement teams see through documentation that shows conclusions without reasoning.

Lesson: Update your evidence clearly and promptly when issues are resolved

3 Risk Analysis Done in Reverse

Teams document the security controls they have already built, then work backwards to construct a risk analysis that justifies those controls. Reviewers can see the order of events: the threats are too convenient, the controls too perfectly matched, and the gaps too clean.

Lesson: Build threat-first. Identify threats systematically using STRIDE or a similar framework. Then select controls. Then verify. This produces the traceability chain that regulators expect, and it tends to surface genuinely missed risks rather than confirming what you already built.

4 Treating Threat Modelling as a one-off Activity

Sometimes a threat model is done once during initial development, then never updated. So after a new software release, a new cloud integration, or a new API, the threat model is stale (and assessors notice). Threat models must be living documents, updated on every major release or system change.

The same failure applies to your SBOM. Teams generate one during initial development and never update it. When a new vulnerability is published (a CVE - a publicly disclosed security flaw in a specific software component) they have no reliable way to check whether their product is affected.

Lesson: Treat your threat model as a living document: update it on every major release or system change. Do the same with your SBOM: regenerate it per release, with a logged process for checking new CVEs against it.

5 External Developer Misalignment

External development teams are usually hired to add specific features. Security documentation, (including threat models, SBOM, and traceability matrices) is typically not in their contract, their sprint reviews, or their commercial priorities.

The gap often only becomes visible at procurement. By then, the developers have usually been paid and moved on.

Lesson: Include security documentation requirements in developer contracts. Review evidence artefacts at sprint milestones, not only at submission time and brief security evidence as a deliverable.

6 Patch Policy Commitments not kept in Practice

If your policy documents state “we will patch critical vulnerabilities within 14 days”, expect procurement teams to ask for proof. If in practice it has been taking months, that policy becomes a liability.

One thing companies consistently underestimate: deploying a patch to a fleet of live devices is not the same as pushing an app update. If your devices are in clinical use, air-gapped, or subject to high uptime requirements, every patch needs clinical safety validation before it goes out. That validation time needs to be built into your patch SLAs from the start, not discovered when you’re trying to respond to a critical vulnerability.

Lesson: Set realistic SLAs you can actually demonstrate evidence for. An honest shorter commitment you can back up is more credible than an aspirational one you cannot.

7 Unclear System Boundaries

Your company is probably laser-focused on the physical device. Yet reviewers will ask about the companion app, cloud backend, APIs, and clinical integrations. If your scope documentation is ambiguous, reviewers fill in the gaps themselves (usually unfavourably).

Lesson: Draw the full boundary. Define who owns security at each layer. Be explicit about what you assume the customer manages. Ambiguity in boundaries means ambiguity in your threat model, your testing scope, and your evidence pack.

8 SBOM Exists once but is not Release-tied

Sometimes a team generates an SBOM during initial development, or keeps a "best effort" list, but does not store it with each release or run a consistent monitoring and triage workflow. This means they cannot answer "are we affected by this CVE?" quickly, and cannot demonstrate the post-market capability that regulators expect.

Lesson: Treat SBOM as a release artefact. Define monitoring ownership and document triage decisions and timelines.

9 Evidence Pack Built for One Tender, then Left to Drift

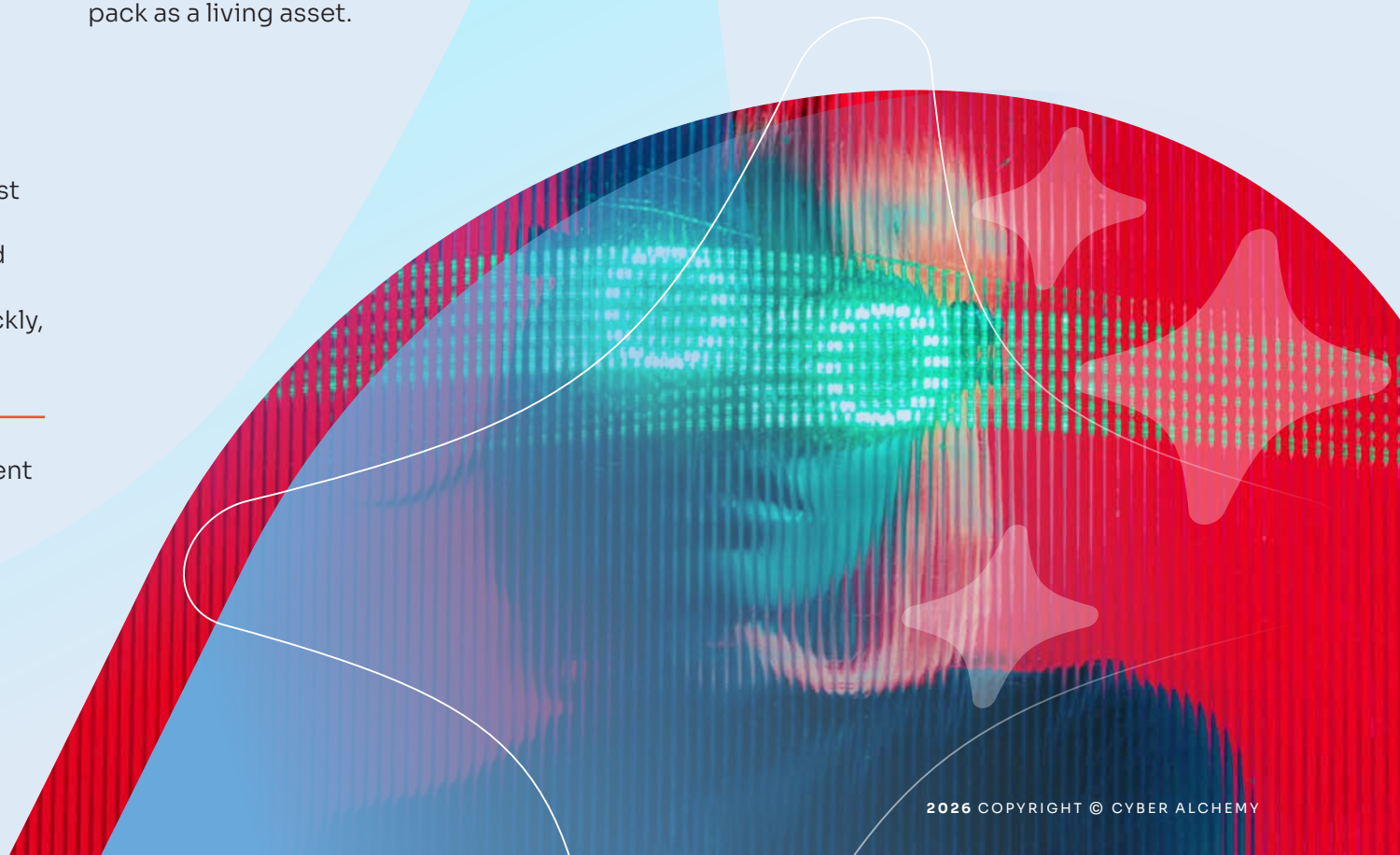
An evidence pack might be produced for a specific procurement opportunity, then left unchanged. Product owners might leave, documents might go out of date, so the next procurement cycle becomes slow and painful again. This is often where inconsistencies appear.

Lesson: Use the evidence index to track owners and review cadence. Update "last updated/next review" whenever a change ships. Treat the evidence pack as a living asset.

10 Over-claimed Capabilities

It's a cliché, but sometimes true: Marketing language often describes capabilities the documentation does not support. If that happens, credibility immediately suffers when reviewers ask for evidence.

Lesson: Use precise language: "aligned to", "informed by", "based on" unless you hold the formal certification. A credible, honest picture of your security posture is always more effective than an inflated one.



Your Medical Device Compliance Toolkit: Free Templates

The tools below are structured around the full submission picture. The threat modelling guide is the most widely used way to evidence cybersecurity risk management in EU MDR and FDA510(k). Building it early benefits your DTAC positioning. The patch playbook and FSN template apply across all three markets once your product is operational. Each tool indicates which standards it most directly supports.

Threat Modelling for MedTech (STRIDE): A Practical Guide

Most directly supports EU MDR, FDA 510(k). Recommended for DTAC.

Threat modelling is a structured way to answer one question:

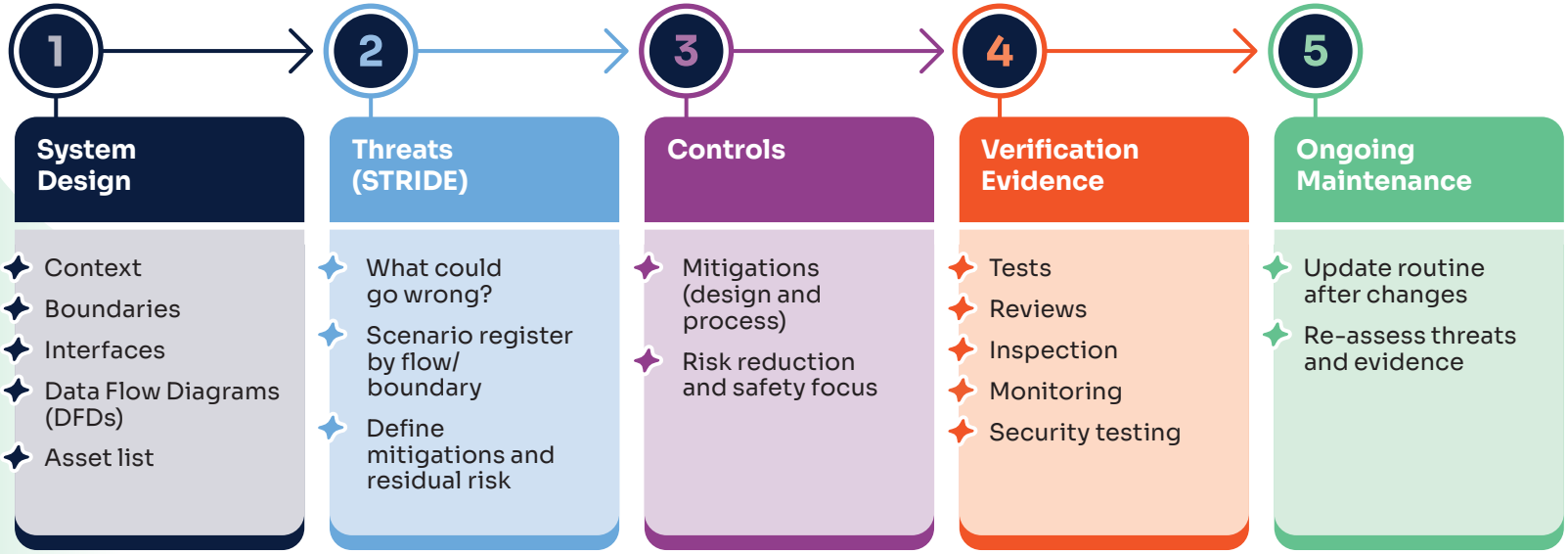
"What could go wrong, how bad would it be, and what are we doing about it?"

In MedTech, the "how bad" part is not only data loss. It can include patient harm, multi-patient harm, and clinical service disruption. Good threat modelling produces evidence you can use for DTAC (and reuse for EU MDR and FDA submissions) because it links:

System Design > Threats > Controls > Verification Evidence > Ongoing Maintenance

Secure Development Lifecycle for MedTech

Linking design decisions to cybersecurity evidence across the product cycle.



What you will Produce
(The Outputs)

By the end, you will have:

1. **A System & Data Flow Diagram** showing boundaries and interfaces.
2. **An Asset List** (what must be protected).
3. **A Threat Register** using STRIDE categories.
4. **A Risk View** (patient impact and exploitability/likelihood) and priorities.
5. **A Mitigation Plan** (controls chosen).
6. **A Verification Plan** (how you prove controls work).
7. A simple **"keep it current"** routine so the threat model stays valid after updates.

Tip for non-technical teams:
You're not expected to invent attack techniques. Your job is to capture realistic "what if" scenarios, then prove the design prevents harm or reduces risk.

The STRIDE Method
(in Plain English)

STRIDE is a checklist that helps you think of different types of security problem:

- **S** **Spoofing:** pretending to be someone/ something trusted.
- **T** **Tampering:** altering data, settings, software, or signals.
- **R** **Repudiation:** actions that can't be proven later (weak/no logs).
- **I** **Information disclosure:** data seen by people who shouldn't see it.
- **D** **Denial of service:** making the device/ service unavailable or unreliable.
- **E** **Elevation of privilege:** gaining higher access than intended.

We apply STRIDE **to each data flow and trust boundary** (i.e., each place information crosses between components or organisations). This is consistent with structured threat registers used in medical device cybersecurity workbooks (e.g., STRIDE columns in a threat model sheet).

The MedTech Threat Modelling Process
(3 Stages, 7 Steps)

Most directly supports EU MDR and FDA 510(k) submissions.
Not a formal requirement for DTAC, but the evidence it produces maps directly to what technical assurance assessors look for in practice.

Stage A: Understand the System

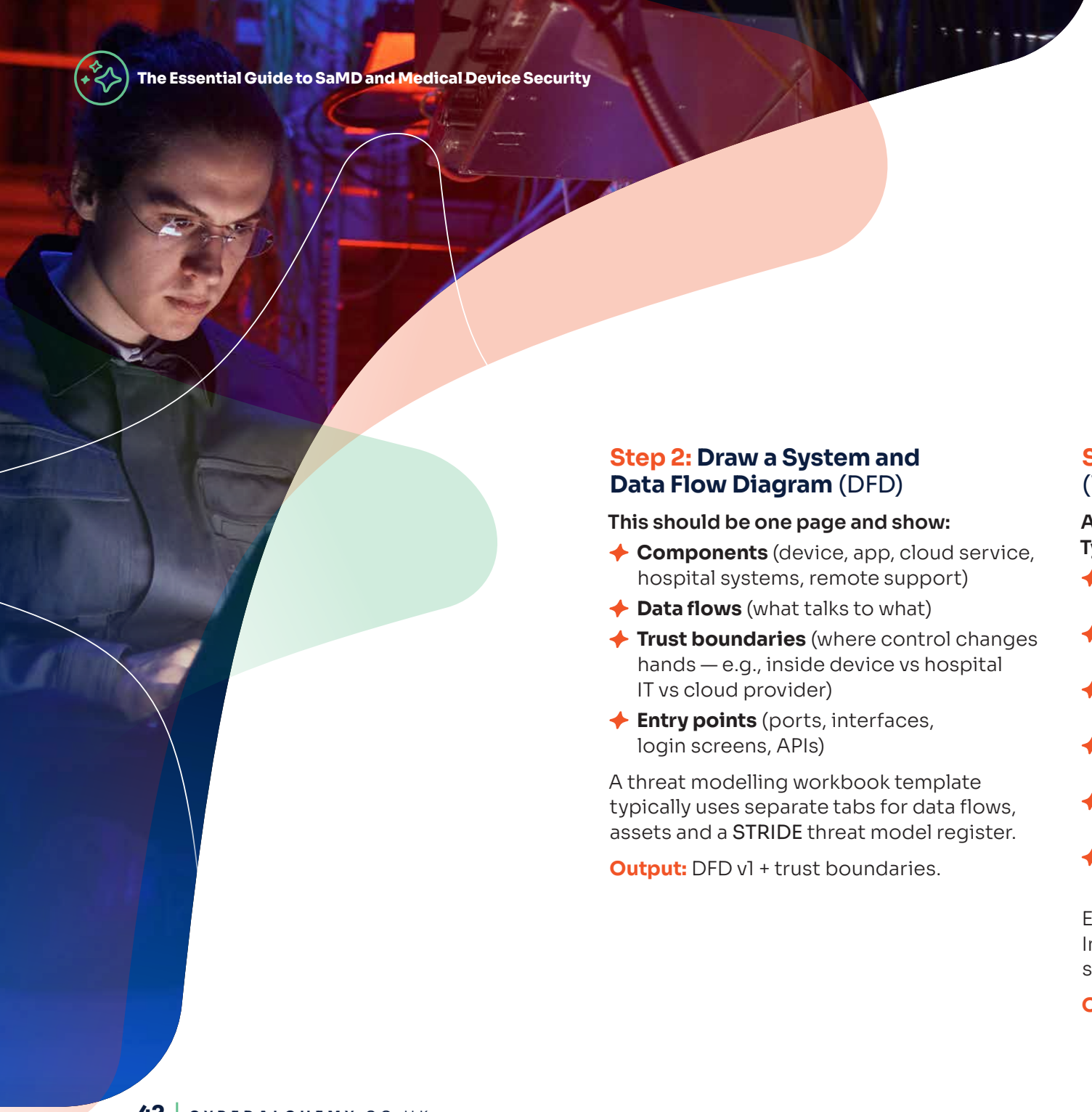
Step 1: Define the Scope and Assumptions Showing Boundaries and Interfaces.

Write down, in plain English:

- What the product is and what it does (intended use)
- Where it runs (hospital network, home Wi-Fi, cloud, mobile, on-device)
- Who uses it (clinician, patient, admin, service engineer)
- What connections exist (USB, Bluetooth, APIs, VPN, remote support)
- How updates happen (local update, cloud update, service engineer)
- The most important "safety-critical" outcomes (what could cause harm)

This matters because EU guidance explicitly frames cybersecurity around intended **operational environment, foreseeable misuse**, and **operating environment expectations** (e.g., segmentation, access control, patching, malware protection).

Output: "System context & assumptions" (½–1 page)



Step 2: Draw a System and Data Flow Diagram (DFD)

This should be one page and show:

- **Components** (device, app, cloud service, hospital systems, remote support)
- **Data flows** (what talks to what)
- **Trust boundaries** (where control changes hands — e.g., inside device vs hospital IT vs cloud provider)
- **Entry points** (ports, interfaces, login screens, APIs)

A threat modelling workbook template typically uses separate tabs for data flows, assets and a STRIDE threat model register.

Output: DFD v1 + trust boundaries.

Step 3: Identify Assets (What must be Protected)

Assets in MedTech are not just "data". Typical asset groups:

- **Patient safety / clinical function:** accurate readings, correct therapy delivery
- **Clinical integrity:** configuration/ calibration, algorithms, decision outputs
- **Availability:** device/service uptime for care delivery
- **Patient data:** identifiable data, clinical records, telemetry
- **Security anchors:** credentials, keys, certificates, update signing keys
- **Evidence & traceability:** logs needed for investigations

EU guidance emphasises CIA (Confidentiality, Integrity, Availability) and ties it to patient safety impacts.

Output: Asset list (with IDs).

Stage B: Find Threats (STRIDE Workshop)

Step 4: Apply STRIDE to each Data Flow and Boundary

Write down, in plain English:

- For each data flow on your diagram, ask six questions (one per STRIDE letter).
- Keep answers high-level (no exploit steps). You're writing scenarios like:

  "If the wrong person could access X, what could they do and what harm could result?"

Output: Draft threat scenarios tagged with STRIDE categories.

Step 5: Score and Prioritise (MedTech Lens)

Your scoring needs two dimensions:

1. **Safety severity** (patient harm potential; include multi-patient harm).
2. **Likelihood/exploitability** (how plausible in the real environment)

EU MDR cybersecurity guidance defines risk as probability × severity and ties cyber issues into risk management and lifecycle updating.

FDA guidance similarly positions cybersecurity as part of safety/effectiveness and includes risk management and threat modelling as part of the recommended approach.

Output: Ranked threat list (high/med/low).

Stage C: Decide Controls, Prove them, Keep it Current

Step 6: Choose Mitigations and Create Traceability

Once the threats have been assessed against your risk acceptance criteria you will know what needs to be fixed and what can remain. For each unacceptable threat:

- **Write the control(s)** you will implement (design or process)
- **Link it to verification evidence** (test, review, inspection, monitoring)

A threat model workbook template explicitly supports traceability from threat scenarios to mitigations and evidence.

FDA guidance includes "Implementation of Security Controls" and "Cybersecurity Testing" as submission documentation components.

Output:
Threat **>** Control **>** Verification mapping

Step 7: Keep it Current

Update triggers: new major feature or architecture change; new integration; new third-party component; new CVE affecting your system; significant change in operating environment; security incident or near-miss.

Output: threat model version history and update log.

72-hour Security Patch Playbook (Safety-impacting Cyber Issues)

Relevant to DTAC, EU MDR and FDA 510(k)

Customise timelines and roles to your product and regulatory context before an incident occurs.

When this Playbook Applies

Use a two-tier trigger so you never miss a relevant issue, but you only escalate when it matters.

Output: Clear understanding of when you need to patch and how to perform it safely.

Here's what that looks like:

1) Start Triage (Always)

Start triage when any vulnerability, weakness, or suspicious security report is identified that could relate to your device/app/cloud service or its components (including third-party libraries and suppliers).

Goal: confirm relevance, scope exposure, and decide next steps with an auditable record.

2) **Escalate** (When Impact or action is likely)

Escalate to the full playbook when any of the following is true:

- **Safety or clinical impact is suspected or confirmed:** patient safety, clinical performance/essential performance, or clinical service continuity could be affected.
- **Credible exploitation is possible in the intended environment:** e.g., hospital network, remote support path, update channel, typical configurations and user behaviours.
- **Mitigation requires action beyond "note and monitor":** a patch/update, configuration change, disabling a feature, compensating controls, or customer communications.

Practical rule: Triage everything. Escalate fast when safety, credible exploitation, or customer action is on the table.

Roles (Assign names before an incident)

Role	Responsibility
Incident Lead	Owns timeline and decision-making; chairs checkpoints.
Engineering Lead	Owns technical fix, testing, build/release.
Clinical Safety / Patient Safety Lead	Assesses patient safety impact; reviews user guidance.
Regulatory/ QA Lead	Owns FSN wording, submissions, evidence pack, DHF updates.
Support Lead	Owns customer comms, deployment coordination, confirmation tracking.

72-hour Timeline Checklist

Timebox	Objective	**Key actions** (tick)	**Outputs** (evidence)
T0–T4 (0–4h)	**Triage and Stabilise**	○ Open incident record ○ Confirm scope (products/versions/configs) ○ Assess safety impact and worst-case harm ○ Decide immediate containment (disable feature, restrict access, block IOC) ○ Identify who must be notified internally	✦ Triage note (impact, scope, initial controls) ✦ Containment decision record
T4–T24 (4–24h)	**Build Fix Plan and Draft Comms**	○ Root cause analysis (high-level) ○ Choose remediation approach (patch vs config vs compensating) ○ Define test plan (incl. safety/regression) ○ Draft FSN (v0.1) in plain English ○ Prepare deployment approach and rollback criteria	✦ Remediation plan ✦ Test plan ✦ FSN draft v0.1
T24–T48 (24–48h)	**Implement, Validate, Prepare Release**	○ Implement fix ○ Run security tests + regression tests ○ Validate clinical/safety impacts are not worsened ○ Prepare release artefacts (signed build, versioning) ○ Update SBOM for the patch release	✦ Test results ✦ Release notes ✦ Updated SBOM
T48–T72 (48–72h)	**Notify, Deploy, Verify**	○ Finalise FSN (v1.0) + approval ○ Distribute FSN to targeted users ○ Deploy patch/config change ○ Verify adoption (telemetry or confirmations) ○ Record effectiveness + residual risk ○ Schedule follow-up comms	✦ FSN v1.0 ✦ Deployment record ✦ Customer confirmations ✦ Post-action review

Quality bar (what makes this defensible)

✦ **A reviewer should be able to follow a clear chain:** vulnerability **>** safety/clinical impact rationale **>** decision **>** fix **>** verification **>** communication **>** evidence of deployment. Keep all artefacts versioned and link them to the affected product release(s).

Field Safety Notice (FSN) Template – Cybersecurity Patch

Structure aligns with MHRA guidance for clear and effective FSNs (traceability, UDI inclusion, targeted distribution, and follow-up) and commonly-used FSN layouts in industry templates.

A. Cover Letter (Page 1)

URGENT – FIELD SAFETY NOTICE (FSN) / FIELD SAFETY CORRECTIVE ACTION (FSCA)

Company Name
Company Address
Phone
Email
Website

Date of issue: [DD/MM/YYYY]

FSN reference: [FSN-YYYY-XXX]
FSCA reference: [FSCA-YYYY-XXX] (if applicable)

Recipient: [Hospital/Organisation Name],
[Department],
[Address]

Subject: Cybersecurity update for [Product Name] – action required

Dear [Name/Role],

We are issuing this Field Safety Notice to inform you of a cybersecurity issue affecting certain versions/configurations of [Product Name]. This notice explains (1) what the issue is, (2) what the potential risk is, and (3) what actions you must take.

Please: (a) circulate this notice to all relevant users, IT, and clinical engineering teams, (b) complete the required actions by [DATE/TIMELINE], and (c) confirm completion using the acknowledgement section on Page 3 (or the attached reply form).

If you have questions or require support, please contact: [Support Contact Name/Team], [Email], [Phone].

Sincerely,

[Name],
[Title] (e.g., Regulatory/Quality Responsible Person)

[Signature]

B. FSN Details (Page 2)

1) Affected Product(s)

Field	Details
Product Name	Owns timeline and decision-making; chairs checkpoints.
[Product Name]	Owns technical fix, testing, build / release.
Software/Firmware Versions	[Affected versions]
UDI / UDI-DI (if applicable)	[UDI / UDI-DI]
Serial / Batch Range	[Serial numbers / batch / lot]
Geographic Scope	[Countries / regions affected]

2) Affected Product(s)

Describe the issue in 3–5 sentences, avoiding technical jargon. Include the conditions under which it may occur, and how it may be triggered in real operating environments.

Issue summary:
Write here...

3) Risk to Users/Patients

Risk category	Describe what could happen
Patient Safety	[e.g., delayed diagnosis, incorrect output, therapy interruption, etc.]
Clinical Service Impact	[e.g., device unavailable, workflow disruption]
Data Confidentiality	[e.g., patient data exposure risk, if applicable]
Integrity	[e.g., risk of altered configuration/records, if applicable]

4) Actions Required by Customers/Users

Please complete ALL actions below:

Actions by customers/users:

- ○ Identify all affected devices and versions in your environment (see Section 1).
- ○ Apply the update / patch: [Patch ID / Version] by [deadline].
- ○ If you cannot patch by the deadline, apply the interim mitigations in Section 5 and contact [Support].
- ○ Confirm completion using the acknowledgement section (Page 3).

5) Interim Mitigations (If Patch cannot be Applied Immediately)

Provide specific, actionable interim steps that reduce risk without creating unsafe clinical workarounds.

Examples (select as applicable):

- ✦ Restrict network exposure (segmentation, allow-listing)
- ✦ Disable non-essential remote access paths
- ✦ Increase monitoring / log review for specific events

Interim mitigations for this issue:

Write here...

6) Actions Taken by the Manufacturer

Actions by manufacturer:

[Company Name] has:

- ○ (a) investigated the issue,
- ○ (b) developed a remediation.
- ○ (c) validated the remediation,
- ○ (d) prepared deployment support.

Remediation provided:
[Patch/Config/Other]

Version:
[X].

Availability:
[Where/how to obtain].

Support:
[Support channels/ hours].

7) Distribution and Targeting

This FSN should be forwarded to: IT/security teams, clinical engineering/biomed teams, department leads, and any third parties who manage the device on your behalf.

C) Customer Acknowledgement (Page 3)

Use this page as the return/confirmation record to support traceability and effectiveness monitoring.

Field	Customer to Complete
Organisation / Site	
Department / Unit	
Contact Name / Role	
Email / Phone	
Number of Affected Devices	
Patch Applied?	◯ Yes ◯ No ◯ Not applicable
Date Patch Applied	
If not Applied, Interim Mitigations Implemented?	◯ Yes ◯ No ◯ Not applicable
Comments	
Signature and Date	

To download Excel versions of these sheets, check out our resources: **download via QR code**.

5. SBOM + CVE Triage Tracker
(Spreadsheet Template)

Required for FDA 510(k) Cyber Devices.
Recommended for EU MDR & DTAC

Designed to pair each product release SBOM with an auditable vulnerability triage and remediation record. Capture minimum SBOM fields and record decisions consistently.

A) Release SBOM index (one row per release)

Release ID	Product/ Component	SBOM Format	SBOM file Location	Generated by	Signed/ Attested?	Notes
R-YYYY-MM-XXX	[Product / Module]	[CycloneDX/ SPDX]	[Path/URL]	[Tool + Version]	◯ Yes ◯ No	

B) SBOM Minimum Fields Checklist (Baseline)

Use this page as the return/confirmation record to support traceability and effectiveness monitoring.

Field	Example	Captured?
Supplier Name	R-YYYY-MM-XXX	○
Component Name	R-YYYY-MM-XXX	○
Version	R-YYYY-MM-XXX	○
Unique Identifiers	R-YYYY-MM-XXX	○
Dependency Relationship	R-YYYY-MM-XXX	○
Author of SBOM Data	R-YYYY-MM-XXX	○
Timestamp	R-YYYY-MM-XXX	○

C) **CVE Triage Log** (One row per vulnerability finding)

Tip: Treat this as your auditable decision record. If a vulnerability is not applicable/exploitable, record the justification clearly.

Finding ID	Release ID	Component (name@ version)	CVE/ Advisory	Severity	Exploit-ability	Affected?	Decision	Fix Version / ETA	Owner	Verification Evidence	Notes / Justify-cation
V-0001	R-YYYY-MM-XXX	[comp@ver]	CVE-YYYY-NNNN	[Low/ Med/ High]	[Low/ Med/ High]	◯ Yes ◯ No ◯ Unknown	[Fix/ Accept/ Defer/ Mitigate]	[Low/ Med/ High]	[Name]	[Test/Report Link]	[Low/ Med/ High]

D) Decision Guide
(Keep this consistent)

Use these standard decision labels in the triage log:

- **Fix:** patch is required and scheduled; include target version and verification evidence.
- **Mitigate:** A compensating control reduces risk; record the control and how it is verified.
- **Defer:** Fix is planned but not immediate; record why and what triggers escalation.
- **Accept:** Risk accepted; record explicit justification and approver.
- **Not affected:** Vulnerability does not apply to your use; record the technical reason in plain English.

Operational Tip

Run triage on every new release and whenever new vulnerabilities are disclosed against components in your SBOM. Keep the triage log tied to release IDs so you can answer: 'Am I affected right now?'

Next steps with Cyber Alchemy

Most MedTech companies face the same problem: they understand the clinical value of their device, but security evidence requirements block market access. Building evidence packs in-house diverts engineering resources from core product development and often results in incomplete or non-compliant documentation.

Our Approach:
Assess > Protect > Enable

1) ASSESS (Clarity)

We map your exact position against UK (DTAC), EU (MDR/IVDR), and US (FDA) requirements. No generic audit – we tell you specifically what's blocking revenue versus what can wait.

Output: Prioritised roadmap of what matters now.

2) PROTECT (Safety)

We help implement the controls that matter. From threat modelling to SBOM generation to incident response capabilities, we build the security architecture that protects patient safety and passes procurement review. We work alongside your team – this isn't outsourced, it's collaborative.

3) ENABLE (Capability)

We transfer knowledge and capability into your organisation so you can become self-sufficient. We teach your team the methods, build their confidence with regulatory evidence, and set you up for internal success. Our goal is to do the difficult foundational work with you, then enable your team to carry it forward.

Book a Strategy Session

We offer a no-obligation strategy session to discuss where you are in development and deployment, what is blocking your progress, and the practical steps to accelerate approval, procurement, and scale.

What you will gain:

- Clarity on your current security and regulatory posture.
- A prioritised roadmap focused on your specific deployment blockers.
- A realistic route to UK/EU/US deployment without rework.

Book your strategy session:

Mail: sales@cyberalchemy.co.uk
Call: 0114 4000377
Click: cyberalchemy.co.uk

CREST | Crown Commercial Service Supplier | CYBER ESSENTIALS | CYBER RUNWAY by plexal

Three Questions to Ask Your Team Today

Before we speak, ask your development lead these three questions:

1 The Commercial Test

If a hospital procurement team asks for our Security Evidence Pack today, is it ready to send?".

If the answer is "**no**" or "**mostly**" – you have a market access blocker.

2 The Safety Test

Have we explicitly mapped our cybersecurity risks to clinical patient safety outcomes?

If the answer is "**not formally**" – regulators will ask and expect documented answers.

3 The Supply Chain Test

Do we have a live, monitored Software Bill of Materials (SBOM) for every third-party component we use?

If the answer is "**what's an SBOM?**" – you're not ready for FDA and increasingly not ready for UK/EU either.

These aren't trick questions – they're the foundation of procurement readiness. **If you can't answer confidently, we can help.**

Digital safety isn't the obstacle to MedTech deployment – it's the bridge. The companies that cross it early will lead the market.

Cyber Alchemy
Advanced Manufacturing Park
Brunel Way
Catcliffe
Rotherham S60 5WG

Mail: sales@cyberalchemy.co.uk
Call: 0114 4000377
Click: cyberalchemy.co.uk

CYBER ALCHEMY®
ASSESS·PROTECT·ENABLE