EXECUTIVE MANAGEMENT BRIEF

From Static Compliance to Continuous Cyber Assurance

CRA-Capable Digital Product Passports for Connected Products, Critical Infrastructure and Resilient Supply Chains

Dr. Carsten Stöcker
Spherity GmbH

23 August 2026

Audience: CEOs, CISOs, CTOs, policymakers, national cybersecurity authorities and senior DPP / industrial cybersecurity leaders
Evidence status: EU legal and standards status checked to 23 August 2026

MOTIVATION The Cyber Resilience Act (CRA) establishes lifecycle cybersecurity requirements for most commercially supplied hardware and software products with digital elements, including connected products and product-integrated remote data-processing services, subject to defined exclusions. It complements NIS2: NIS2 governs organisational cyber risk, while the CRA governs product security and market access. For product OEMs, secure design, vulnerability handling, updates, support and post-market evidence become enduring lifecycle disciplines. A **CRA-capable DPP** connects the resulting evidence to the correct product, release, customer deployment and accountable decision. It can also establish a governed, bidirectional communication channel between the OEM and the product owner or operator: the OEM can issue product-specific vulnerability information, advisories and update notifications, while customers can retrieve authentic OEM information, authorised updates, support status, and current operating and safety documentation for secure product operation. The DPP thereby supports efficient conformity work, trusted customer communication and secure lifecycle operations; it does not itself secure the product or determine legal conformity [1, 2].

OEM regulatory milestones

- 11 September 2026 — Article 14 reporting obligations apply. OEMs need assigned roles, Single Reporting Platform readiness, evidence preservation and coordinated customer communications.
- By August 2027 — complete a scoped product-service pilot, independent control verification and scale decision, preserving an industrialisation window before full application.
- 11 December 2027 — the CRA applies generally. Applicable products placed on the EU market must meet the essential requirements and the relevant conformity-assessment obligations [1].

Why it matters for the C-Suite

- **Cybersecurity resilience.** The CRA institutionalises disciplines that reduce real operating risk: secure-by-design engineering, faster affected-product analysis, supported updates and accountable vulnerability handling.
- **OEM product strategy and economics.** Lifecycle security becomes a designed product capability rather than a late compliance retrofit; supporting portfolio decisions, service models, critical-sector market access and lower evidence-reconstruction costs.
- **Customer trust leadership and OEM credibility.** Precise affectedness, authentic updates and transparent support horizons help customers operate safely and demonstrate that the OEM stands behind the product throughout its supported life.

Five decisions to take now

1. **Appoint one accountable executive owner.** Unify product security, engineering, legal, quality, safety and post-market operations under one evidence-governance mandate.
2. **Fund a digital evidence backbone for CRA conformity, DPP infrastructure, evidence and secure product operations.** Treat persistent identifiers, versioning, provenance, access policy and retention as reusable product infrastructure.
3. **Adopt the five-subject model.** Separate product type, build, instance, deployment state and remote service so that risk and evidence resolve to the right scope.
4. **Bound automation explicitly.** Automate integrity and policy checks, but retain attributable legal and safety decision authority.
5. **Prove and scale the model before full CRA application.** Establish Article 14 reporting readiness by 11 September 2026; complete a scoped high-risk product-service pilot and scale decision within 12 months, leaving time for industrialisation before 11 December 2027.

These decisions are deliberately sequenced around the legal timetable. The immediate test is reporting readiness; the 12-month pilot must then prove traceability, governed evidence access and operational closure early enough to support product-line industrialisation before the CRA applies generally.

Contents

1. Why the operating model must change

The Cyber Resilience Act (CRA) is valuable because it corrects a structural market failure: connected products have historically entered the market with uneven security baselines and weak incentives for sustained vulnerability handling. Regulation (EU) 2024/2847 makes cybersecurity a horizontal market-access discipline across design, development, production and the support period. It requires risk-based secure design, vulnerability handling, security updates, user information, technical documentation and post-market corrective action [1].

The lifecycle logic is the important part. Article 14 reporting obligations for actively exploited vulnerabilities and severe incidents apply from 11 September 2026; the Regulation applies generally from 11 December 2027 [1]. A product that was secure at release can become exposed through a component disclosure, configuration drift, a changed cloud dependency or an unsupported version. Point-in-time certification cannot, by itself, manage that reality.

The CRA and NIS2 are complementary rather than interchangeable. The CRA regulates the cybersecurity of products with digital elements made available on the EU market; NIS2 requires essential and important entities to manage organisational and supply-chain cyber risk. An OEM may be directly subject to one or both regimes, while its customers may rely on secure products and credible supplier evidence to meet their own NIS2 duties [1, 2].

For customers, the practical value is not another compliance label. It is faster, more precise and more trustworthy operational information: whether the deployed product is affected, which update is authentic, what configuration is supported, when support ends and whether remediation succeeded. OEMs that can answer those questions reduce customer uncertainty and downtime while demonstrating credible lifecycle ownership—an increasingly important procurement and renewal criterion in regulated and critical environments.

The ESPR DPP infrastructure is legally separate. The CRA does not mandate a DPP, and an ESPR passport is not evidence of CRA conformity by default. Yet the ESPR requirements for persistent identifiers, data carriers, access rights and interoperable product data—and the operational registry and harmonised DPP standards adopted in 2026—create a reusable substrate for cyber evidence [3–5].

1.1 Threat reality, without hype

Geopolitical instability and hybrid operations increase the strategic value of exploiting products that sit inside communications networks, OT/ICS, factories, buildings, supply chains and homes. Frontier AI compounds the pressure. Official UK assessments conclude that AI already improves reconnaissance, vulnerability research, exploit development and the exploitation of known weaknesses; advanced zero-day assistance is likely to improve first for skilled actors. They also judge fully automated, end-to-end advanced attacks unlikely to be the near-term norm [6, 7]. The management implication is urgent, but precise: reduce the interval between signal, affected-product resolution, authorised remediation and verified closure.

Table 1 translates the principal threat pressures into management implications.

Table 1: Threat pressures and management implications

Pressure	Where it lands	Management implication
Faster exploitation of disclosed flaws	Connected products, firmware, gateways and software dependencies	Resolve advisories to affected builds and instances before exposure becomes fleet-wide.

Table 1: Threat pressures and management implications

Pressure	Where it lands	Management implication
Supply-chain compromise	Components, build systems, update channels and supplier services	Preserve dependency lineage, provenance and supplier attestations across releases.
Remote-service and configuration drift	Cloud APIs, managed services, OT settings and customer deployments	Treat service version and deployed configuration as first-class evidence subjects.
Hybrid disruption and AI capability uplift	Critical infrastructure, communications and high-availability environments	Prepare high-volume triage, controlled update gates, fallback and verifiable recovery.

Sources: CRA [1]; NIS2 context [2]; NCSC and AISI assessments [6, 7].

1.2 Macro context: the risk is dynamic, the evidence is fragmented

The operational risk changes after release, but the evidence needed to understand that change is usually dispersed across product lifecycle management, source and build systems, supplier portals, vulnerability platforms, fleet inventories, cloud-service records, support tools and customer environments. These systems use different identifiers, owners, access rights and update cycles. The result is a management gap: the organisation may possess every required artefact yet still be unable to resolve a new vulnerability to the affected release and deployed customer instance quickly enough. A CRA-capable DPP addresses that fragmentation by linking authoritative evidence; it does not require every source system to be replaced.

> **OPERATING FRAME** Use continuous cyber assurance as the management model: maintain a current, verifiable relationship between the assessed product, the product actually deployed and its changing risk state. "Continuous conformity" is an analytical operating term—not an automated legal status.

2. The CRA-capable DPP architecture

A CRA-capable DPP is a distributed, versioned and access-controlled evidence architecture. The data carrier or QR code is only an entry point. The architecture resolves a persistent product subject to authoritative evidence, records changes and supersession, and gives each relying party a purpose-appropriate view. Sensitive SBOM, vulnerability and deployment data should not be made public merely because a passport exists.

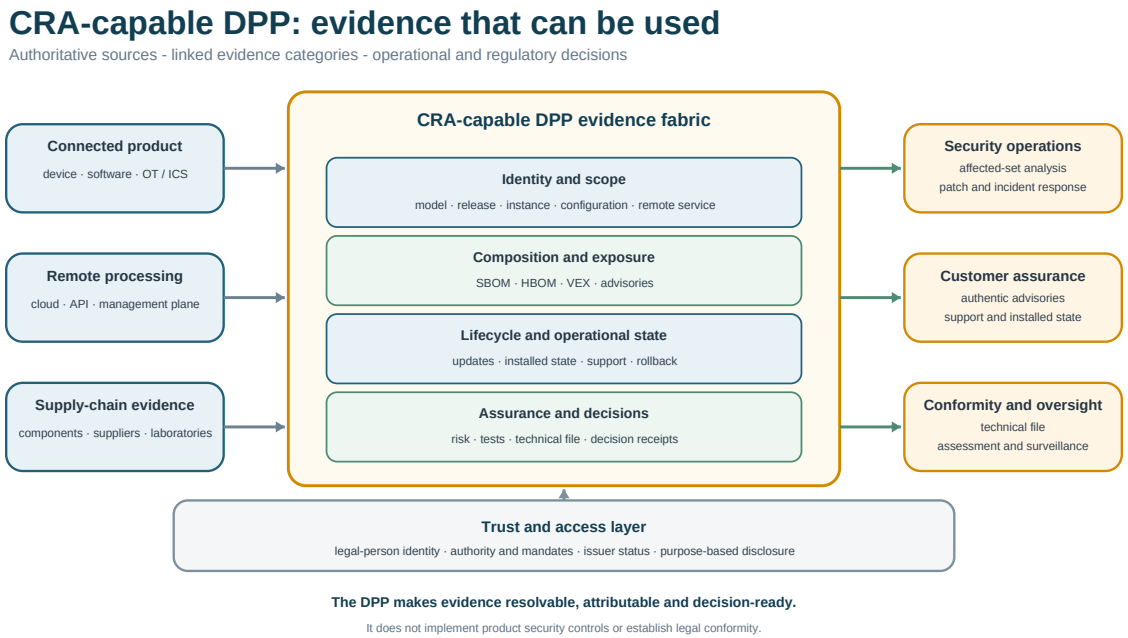

Figure 1: A CRA-capable DPP links product, remote-service and supply-chain sources to four categories of lifecycle evidence and three operational uses. A trust and access layer governs who may issue, view and rely on that evidence. Source: Authors' architecture.

Read Figure 1 from left to right. Product, remote-service and supply-chain sources feed a governed evidence fabric; authorised parties then receive the decision-ready view appropriate to security operations, customer assurance or conformity work. The trust layer spans the architecture because signed evidence is not automatically trustworthy: reliance also depends on issuer identity, authority, current status, purpose and permitted disclosure.

2.1 What the CRA-capable DPP contains

- **Identity and scope.** Persistent identifiers connect the product model, assessed release, deployed instance, configuration and manufacturer-responsible remote service. Without that binding, evidence can be valid but applied to the wrong object.
- **Composition and exposure.** A Software Bill of Materials (SBOM) and Hardware Bill of Materials (HBOM) describe the components in an exact release. Vulnerability Exploitability eXchange (VEX) records whether a product or component is affected, not affected, fixed or still under investigation—and the rationale for that status.
- **Lifecycle and operational state.** Advisories, updates, installed versions, approved configurations, support periods, deferrals, rollback and recovery evidence show what changed after market entry and what is actually deployed.
- **Assurance and accountable decisions.** Risk assessments, tests, technical-documentation references, conformity artefacts and decision receipts preserve the basis, scope, owner and time of a material decision.
- **Trust and access.** Legal-person identity, organisational roles, mandates, issuer status, signatures, credential status and purpose-based disclosure determine who may create, change, see or rely on each evidence object.

The categories are valuable only when linked. An SBOM is an inventory, not proof of security;

VEX is a product-context conclusion, not a vulnerability scan; and a QR code or valid signature does not establish that the evidence is current, authorised or sufficient for conformity.

2.2 Three capabilities leaders can use immediately

- **Automated evidence readiness.** Verify that required artefacts exist, are signed, current, attributable and applicable to the assessed release. Use interoperable formats such as SPDX or CycloneDX where appropriate [8, 9]. Do not label that result 'legal conformity'.
- **Contextual vulnerability resolution.** Trace a CVE or supplier advisory through component, build, instance and deployment configuration to distinguish affected from not-affected products, backed by VEX or equivalent rationale.
- **Dependency-graph operations.** Expose which products rely on a changed library, remote API, certificate, cloud service or update channel, then coordinate remediation and customer communication.

2.3 The five-subject model: resolve evidence to the right object

The most common architectural error is to attach all evidence to a product family. That is too coarse for vulnerability response and often too vague for conformity evidence. The five-subject model separates stable commercial identity from the changing technical and operational state.

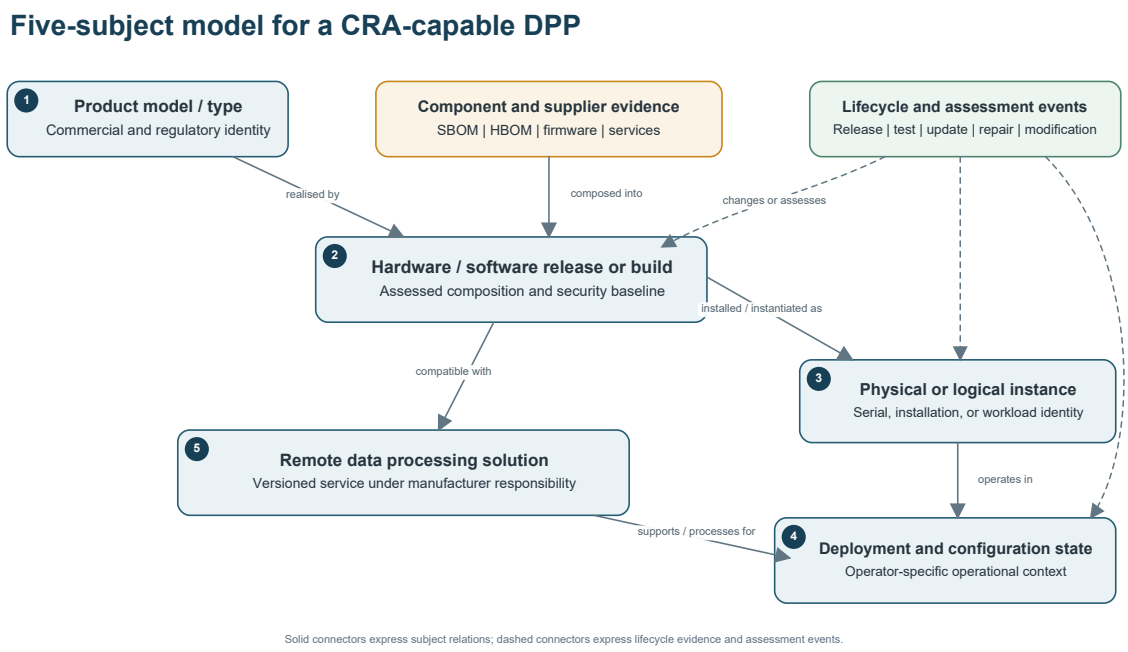

Figure 2: Five-subject model for a CRA-capable DPP. Product type, assessed release or build, deployed instance, configuration state and remote processing solution are linked to supplier evidence and lifecycle events. Source: Authors' model; adapted from the long-version Figure 1.

Each subject answers a different incident and conformity question. The product type establishes the commercial and regulatory scope; the release fixes the assessed composition; the instance identifies the affected unit; the deployment state supplies operational context; and the remote solution captures services whose changing version can alter product risk.

Table 2 summarises the management question and evidence associated with each subject.

Table 2: Five-subject model: management questions and example evidence

Subject	Management question	Example evidence
1. Product model / type	What is the regulated commercial product?	Manufacturer, model identifier, intended purpose, classification
2. Release / build	Which assessed composition and baseline apply?	SBOM/HBOM, tests, risk assessment, release signature
3. Instance	Which physical or logical unit is affected?	Serial, installation or workload identity; installed version
4. Deployment state	Does the operating context change exposure?	Configuration, network zone, compensating controls, attestation
5. Remote processing solution	Which versioned service is part of product function?	Service release, API dependency, availability and change record

2.4 Where a CRA-capable DPP helps—and where it does not

Start with the boundary. A CRA-capable DPP is an evidence and operational-assurance layer. It can connect, validate, disclose and preserve evidence about product security. It does not replace the product controls and governance processes that create conformity. A signed record of a test is not the test; a current SBOM is not vulnerability handling; and an evidence-completeness check is not a legal conformity decision.

Official implementation guidance points manufacturers towards secure-by-design and secure-by-default engineering, product cybersecurity risk assessment, SBOM creation, vulnerability handling, security updates, support-period management, technical documentation, the applicable conformity-assessment procedure and Article 14 reporting. BSI TR-03183 gives practical technical guidance on manufacturers' cybersecurity requirements and SBOMs. The DPP can connect the resulting evidence and make it operationally usable; it cannot perform those controls or allocate legal responsibility [10, 11].

Table 3 separates DPP contributions from the controls and decisions that remain outside the passport.

Table 3: Where a CRA-capable DPP contributes—and which measures remain outside it

CRA / OEM outcome	DPP contribution	Measures still required outside the DPP
Scope and traceability	Links product type, assessed build, deployed instance, configuration and remote service through persistent identifiers.	Legal scope and classification analysis; intended-purpose definition; accountable product ownership.
Evidence readiness and automation	Checks signatures, provenance, freshness, completeness, versioning and role-based access; assembles an auditable evidence view.	Secure development, threat modelling, risk assessment, testing, technical-documentation judgement and evidence-quality review.
Vulnerability and update operations	Connects SBOM/VEX and advisories to affected builds and instances; records update publication, installation, deferral and recovery evidence.	PSIRT operations, disclosure handling, update engineering and delivery, Article 14 reporting, incident response and customer support.

Table 3: Where a CRA-capable DPP contributes—and which measures remain outside it

CRA / OEM outcome	DPP contribution	Measures still required outside the DPP
Customer cyber assurance	Provides authenticated advisories, precise affectedness, trusted update provenance, support-end information and deployment-state visibility.	Customer-side asset management, monitoring, backups, network controls, safe change management and local risk acceptance.
Conformity decision	Supplies a versioned evidence package and an attributable decision record for the applicable product and release.	Applicable conformity procedure, notified-body involvement where required, EU declaration of conformity, CE marking and market-surveillance cooperation.

For customers, this translates into faster and more precise answers: whether their deployed unit is affected, which remediation is authentic, when support ends, what changed and whether installation succeeded. That reduces unnecessary intervention, narrows outage risk and supports safer operations—particularly in OT, critical infrastructure and long-lived connected products.

For the OEM, customer assurance is not an optional communications benefit. It demonstrates lifecycle ownership, can reduce blanket notifications and support effort, improves incident co-ordination and strengthens confidence in the brand. The executive implication is to fund the underlying product-security, PSIRT, update, quality and customer-success capabilities together with the evidence backbone; funding the DPP alone would digitise gaps rather than close them.

> **EXECUTIVE TEST** Ask two separate questions: 'Are the product and its lifecycle processes sufficient for CRA conformity?' and 'Can the organisation produce trustworthy, current evidence of that sufficiency for the right product, customer and decision?' The DPP materially strengthens the second question and selected operational parts of the first.

3. Zero Trust and the dual-plane trust model

NIST SP 800-207 removes implicit trust based on network location or ownership. Each access request is evaluated through policy decision and enforcement functions using identity, context and current resource state [12]. A CRA-capable DPP applies the same principle to evidence: possession of a link, credential or supplier relationship is not sufficient reason to trust a claim.

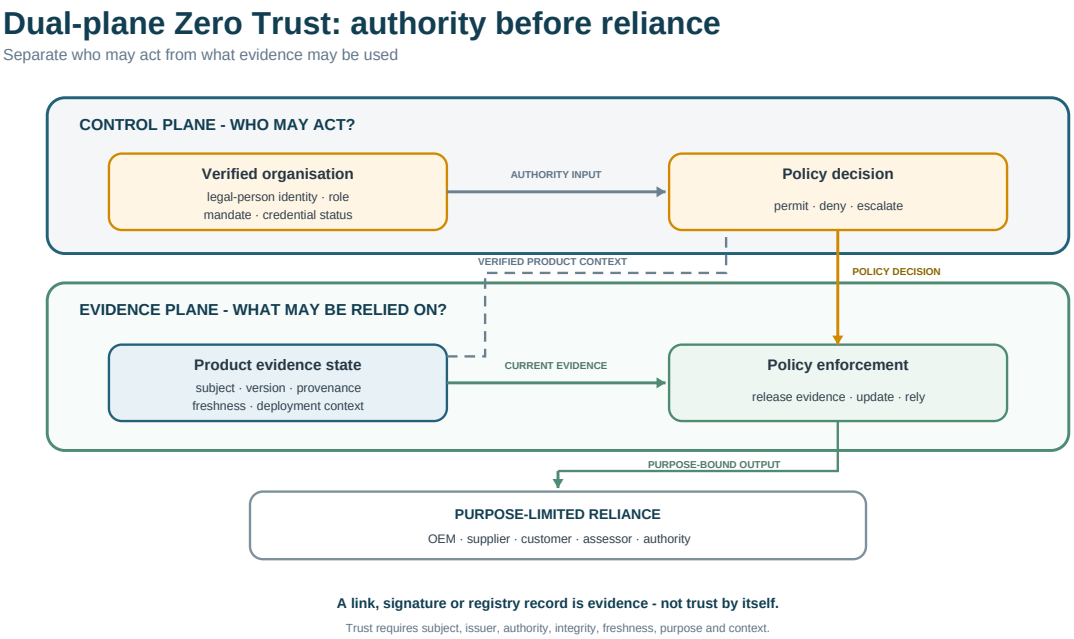

Figure 3: Simplified dual-plane Zero Trust model. The control plane verifies organisational authority and decides whether an action is permitted; the evidence plane verifies the applicable product state and enforces purpose-limited access or action. Source: Authors' architecture aligned with NIST SP 800-207 [12].

Figure 3 separates authority from evidence processing. The control plane answers who may act and under which mandate; the evidence plane answers what may be relied on for the relevant product subject and state. Policy enforcement joins both answers before evidence is disclosed, an update is authorised or a decision is accepted.

Control plane. Establishes legal-person identity, organisational authority, roles, mandates, credential status and purpose. Its policy decision point determines permit, deny or escalate; its policy enforcement point controls access, issuance and reliance. eIDAS 2.0 provides a binding trust-services framework [13]. European Business Wallets could become an important organisational implementation, but COM(2025) 838 remains a legislative proposal and must not be presented as applicable law [14].

Evidence plane. Manages SBOMs/HBOMs, VEX, advisories, tests, risk assessments, update receipts, installed-state observations and lifecycle lineage. NIST uses a control plane and data plane; the 'evidence plane' here is the authors' domain-specific adaptation for governed evidence resources, not a term defined by NIST.

> **ZERO-TRUST RULE** Verify the subject, issuer, authority, evidence integrity, freshness, purpose and deployment context for each reliance decision. Minimise implicit trust zones and record the decision receipt.

3.1 Closing the OEM–customer information loop

For many OEMs, the direct customer relationship is lost when products move through wholesalers, distributors, systems integrators or retailers. The OEM may know what it manufactured but not who currently owns or operates an instance; the customer may struggle to distinguish current OEM information from copied manuals, outdated distributor material, fraudulent support sites illicit actors acting as man-in-the-middle with manipulated documents.

A CRA-capable DPP can create a persistent, bidirectional trust channel anchored in the product identifier. 'Direct' describes the end-to-end trust relationship even where a DPP provider or channel partner technically mediates the exchange.

The CRA requires manufacturers to provide product identification, a directly accessible vulnerability-reporting contact, secure-use information, vulnerability handling and security updates with appropriate user information. A CRA-capable DPP can make those obligations product-, release- and deployment-specific, although the CRA does not prescribe a DPP. The ESPR DPP framework contributes persistent identifiers, controlled access and requirements for authenticity, reliability, integrity, security and privacy [1, 3].

OEM to customer. The channel can carry authenticated vulnerability warnings, VEX affectedness statements, signed update manifests, authorised download locations, release and rollback instructions, current operating manuals, secure-configuration and safety procedures, support status, recalls and retirement information. Customers can verify that the information comes from the accountable OEM, applies to their product and release, remains current, and has not been superseded or revoked.

Customer to OEM. Customers can return vulnerability reports, installed-version or configuration attestations, update or recovery receipts, ownership or operator changes and—where lawfully authorised—selected fleet observations. This closes the operational evidence loop: the OEM can determine whether remediation reached affected products, while the customer receives authoritative information without depending on an unverified intermediary.

Zero Trust applies to the information, not merely the connection. Each material reliance should verify the issuing OEM and mandate, product applicability, object signature or seal, integrity, timestamp, validity, supersession or revocation status, recipient authority and purpose [12]. Transport encryption protects the session; object-level signatures protect information as it passes through intermediaries. For firmware, the product should independently verify the signed manifest, payload digest, compatibility and anti-rollback state. A valid QR code or web session is not enough [15].

For enterprise customers and fleet operators, a European Business Wallet could provide verifiable legal-person identity, representative authority, mandates and trusted document exchange. It remains a legislative proposal, so the architecture should be wallet-compatible rather than wallet-dependent [13,14]. Verified identity can support authorised-user, service-partner, trading-partner and export-control workflows, but cannot automate their legal outcome: dual-use compliance still requires product classification, destination, end-user and end-use screening, sanctions checks, licence determination and accountable controls [16].

With customer authorisation, product instances can be assembled into a private fleet view of versions, configurations, support horizons, vulnerability exposure and remediation status. Selected, minimised observations, such as failed updates, recurring configuration weaknesses or attack indicators, can improve threat intelligence, testing and product hardening. The EU Data Act gives users rights over connected-product data; it does not give the OEM an unrestricted collection right. OEM use of readily available data requires the applicable contractual basis, and personal-data processing remains subject to data-protection law [17]. The DPP should record purpose, permission and provenance, while high-volume telemetry remains in governed operational systems.

This trusted lifecycle relationship can reduce support and incident-scoping costs, improve update adoption and customer retention, and enable compatible services such as fleet assurance, managed security and lifecycle support. Mandatory safety information, vulnerability notices and CRA-required security updates must remain separate from marketing consent and premium-service conditions [1].

EXECUTIVE IMPLICATION Treat the channel as product infrastructure, not a marketing database. Fund trusted product and organisational identity, version and revocation services, ownership transfer, fleet resolution, permission management and evidence receipts.

4. Guardrails senior leaders should make non-negotiable

Bounded automation. Software may verify signatures, hashes, schema validity, freshness, completeness, policy conditions and consistency. It may recommend or route a decision and integrate with a secure software development lifecycle [18]. It cannot assume the legal responsibility assigned to a manufacturer, authorised representative, conformity assessment body or authority. Every material decision needs an identifiable decision owner, basis, time and scope.

Cryptographic agility and long-lived evidence. Products and records may outlive algorithms, keys, certificate chains, trust services and vendors. Preserve validation material, time evidence, revocation status and migration paths; design re-signing and re-attestation without destroying provenance.

Provider-neutral continuity. Contract for exportable identifiers, evidence objects, schemas, access-policy definitions, audit logs and verification metadata. Test an escrow or migration path before a critical provider fails or exits.

Cyber-safety change gates. In OT, medical, automotive and other safety- or availability-constrained settings, urgency does not eliminate change control. Security, functional safety and essential service continuity must be assessed together, with time-bounded exceptions and compensating controls where immediate deployment is unsafe [19].

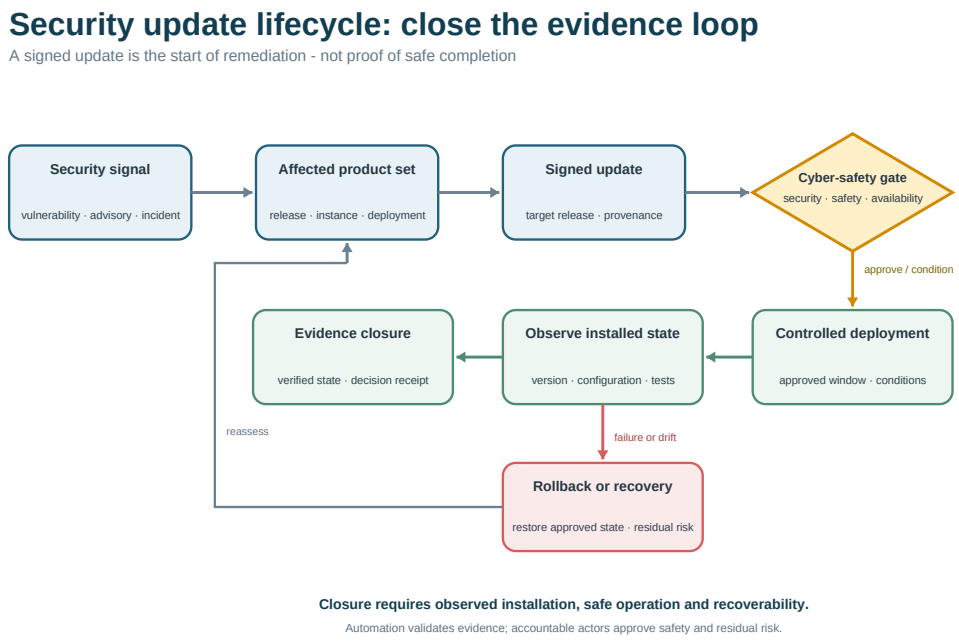

Figure 4: Simplified security-update evidence lifecycle. A security signal is resolved to the affected product set; a signed update passes a cyber-safety gate; controlled deployment, observation and recovery evidence close the lifecycle loop. Source: Authors' executive workflow; adapted from the long-version Figure 5.

Figure 4 makes the closure obligation visible. Publication of a signed update begins the operational process; it does not prove that the correct instances received it, that installation was safe,

or that recovery worked. OEM leadership therefore needs joined-up product-security, safety, service and customer-observation data. It shall not separate release and compliance dashboards.

> **CLOSURE TEST** An update is not complete when it is published. It is complete when the authorised target set is resolved, installation or deferral is observed, safety and service checks pass, failures can recover, and the new state is evidenced.

5. Strategic synthesis: turn compliance evidence into operational leverage

A well-governed DPP can reduce repeated evidence collection, shorten incident scoping, support supplier accountability and give operators a trustworthy view of deployed state. The same graph used for conformity preparation can answer operational questions: Which customers are exposed? Which release is safe? Which evidence is stale? Which supplier changed a dependency? Which authority may see what?

The value is asymmetric. DPP capabilities are strongest where CRA duties depend on identity, composition, vulnerability context, update status, conformity documentation and lifecycle traceability. They are weaker where the decisive control is implemented inside the product—such as runtime confidentiality or resilience. The heat map therefore shows support intensity, not a conformity score.

CRA requirements × CRA-capable DPP capabilities

Support intensity indicates evidence and governance value; it does not indicate legal conformity by itself.

CRA requirement cluster	Identity and scope	SBOM / HBOM	Configuration and deployed state	VEX and vulnerability evidence	Update and support state	Conformity evidence	Lifecycle lineage	Authority and access control
Product and manufacturer identification	H	—	L	—	—	M	M	H
Cybersecurity risk assessment	M	M	M	L	L	H	L	M
Secure design and default configuration	L	L	H	L	M	M	L	L
No known exploitable vulnerabilities	L	H	M	H	M	M	L	L
Access control, confidentiality and integrity	L	L	M	L	L	M	L	M
Logging, monitoring and traceability	L	—	M	L	L	M	M	L
Security updates, rollback and recovery	L	L	M	M	H	M	M	L
Vulnerability handling, CVD and reporting	L	M	L	H	M	M	L	M
Technical documentation and conformity evidence	M	M	L	M	M	H	M	M
Support period and user information	L	—	L	L	H	M	L	L
Secure removal, transfer and decommissioning	L	—	L	—	L	M	H	L
Substantial modification and post-market lifecycle	M	L	M	L	M	M	H	M

H Strong support: direct, high-value evidence linkage

M Material support: meaningful evidence and traceability contribution

L Limited support: indirect documentation or contextual contribution

— No material direct DPP contribution

Interpretation: the DPP is strongest where CRA duties depend on identity, evidence continuity, version-aware traceability, and lifecycle state.

Figure 5: CRA requirements × CRA-capable DPP capabilities. H/M/L indicate the strength of evidence and governance support, not legal conformity or a conformity score. Source: Authors' mapping based on the CRA [1]; reused from the long-version Figure 13.

The heat map must be read through the conformity boundary. A high-support cell means

that the DPP can materially improve evidence, traceability and governed access; it does not mean that the underlying product control is effective or that conformity is automatic. Secure design, runtime confidentiality, resilience, testing and corrective action remain engineering and governance responsibilities outside the passport.

For customers, however, a CRA-capable DPP can translate those responsibilities into timely, product-specific operational assurance: whether a deployed instance is affected by a vulnerability, which advisory or update is authentic, whether the installed version and configuration remain supported, what remediation or compensating controls are recommended, and whether an update, rollback or recovery action succeeded. This improves vulnerability management, asset and configuration management, incident response, secure change control, procurement assurance and end-of-support planning to reduce uncertainty and avoidable downtime while enabling customers to operate connected products more securely.

5.1 How executives should read the map

- Invest first in identity and scope, update state, vulnerability evidence, conformity evidence and lifecycle lineage; these create the broadest cross-functional return.
- Do not confuse evidence of a control with the control itself. A passport can prove the tested configuration; it cannot make an insecure configuration secure.
- Use the matrix to prioritise evidence services and assurance workflows—not to automate a legal conclusion.
- Prioritise customer-facing evidence paths alongside regulator-facing ones. Precise affectedness, authentic advisories, update status and support-end information convert conformity investment into safer customer operations and durable OEM trust.

6. The 12-month management agenda

The objective is not enterprise-wide deployment in year one. It is a controlled proof that the organisation can resolve a security signal to affected product subjects, make an authorised decision and close the lifecycle evidence loop. Reporting readiness cannot wait for the pilot: Article 14 applies on 11 September 2026. The pilot and scale decision should finish by August 2027 so that proven controls can be industrialised before 11 December 2027.

Table 4 assigns accountable owners, horizons and decision outcomes to the implementation workstreams.

Table 4: Twelve-month management agenda

Workstream	Accountable owner	Horizon	Decision outcome
1. Governance and scope	Board sponsor; General Counsel; CISO	0–90 days	Named authority, product scope, decision rights, legal-status taxonomy and risk appetite.
2. Subject and evidence model	CTO; CPO; Product Security	0–120 days	Five-subject identifiers, evidence ownership, retention and minimum metadata.
3. Evidence services	Engineering; Supply Chain; IAM	3–6 months	Signed SBOM/VEX/update flows, resolver, access policy, logs and freshness rules.

Table 4: Twelve-month management agenda

Workstream	Accountable owner	Horizon	Decision outcome
4. Operational pilot	Business unit; OT/Safety; SOC	4–9 months	One product-service chain proves advisory-to-instance resolution and cyber-safety change gates.
5. Assurance and scale	Compliance; Internal Audit; Procurement	9–12 months	Independent control test, vendor exit test, metrics and approved scale roadmap.

The workstreams move from accountability to proof. Governance fixes decision rights; the subject model creates resolvable scope; evidence services establish trusted data flows; the pilot tests the operating model under real constraints; and independent assurance determines whether the result is ready to scale.

6.1 Board scorecard

Table 5 proposes indicators that measure operational assurance rather than paperwork volume.

Table 5: Board scorecard for operational assurance

Indicator	Target direction	Why it matters
Time from advisory to verified affected set	Down	Measures dependency and instance resolution.
Evidence objects with valid issuer, signature and freshness	Up	Measures assurance readiness, not conformity.
Deployed instances with observed version/configuration	Up	Closes the build-to-operation gap.
Security changes passing joint cyber-safety gate	Up	Prevents unsafe urgency and undocumented deferral.
Critical evidence exportable from primary provider	100%	Reduces lock-in and continuity risk.

These indicators measure operational assurance rather than paperwork volume. They should be segmented by product line and risk tier, with exceptions carrying an owner, expiry date and remediation plan. A rising document count is not success if affected instances still cannot be resolved or safe closure cannot be observed.

6.2 Regulatory and standards status at the evidence cut-off

Table 6 records the status and appropriate management treatment of each instrument.

Table 6: Regulatory and standards status at the evidence cut-off

Instrument	Status on 23 August 2026	Management treatment
CRA — Regulation (EU) 2024/2847	Binding law. Article 14 reporting applies 11 September 2026; general application 11 December 2027 [1].	Operationalise lifecycle evidence and reporting now.

Table 6: Regulatory and standards status at the evidence cut-off

Instrument	Status on 23 August 2026	Management treatment
ESPR and DPP registry	Regulation (EU) 2024/1781 is binding; Implementing Regulation (EU) 2026/1778 has applied since 6 August 2026. Six harmonised DPP standards were OJEU-cited in July 2026 [3–5].	Reuse DPP infrastructure where product-group rules and access rights permit.
M/606 / ETSI EN 304 617–627 and 631–636	17 vertical Final Draft European Standards were under Public Enquiry; not yet OJEU-cited CRA harmonised standards [20, 21].	Use as design input; monitor final adoption and OJEU citation before claiming presumption of conformity.
eIDAS 2.0	Regulation (EU) 2024/1183 is binding [13].	Use trust services where they fit control-plane assurance.
European Business Wallets	COM(2025) 838 is a legislative proposal, not applicable law [14].	Design for compatibility; do not make delivery dependent on the proposal.

This status table is a decision-control device. Teams should record whether a source is binding law, official guidance, a cited harmonised standard, a draft standard or a legislative proposal, and should update that status register before using a source to justify presumption of conformity or a product-release decision.

7. Fact-check, interpretive boundaries and references

7.1 Fact-check and quality note

CRA identity and dates. Regulation number, title and staggered application dates were checked against the Official Journal. The brief does not imply that a DPP is mandated by the CRA.

CRA–NIS2 relationship. The CRA is described as product and market-access law; NIS2 is described as organisational cyber-risk law. Their complementary effects are stated without treating one as evidence of compliance with the other.

DPP legal status. ESPR and the 2026 DPP registry implementing act are treated as binding. CRA support is presented as an architectural use, not a statutory equivalence between ESPR and CRA.

Standards status. The 17 ETSI documents are described as Final Draft European Standards under Public Enquiry. No CRA presumption of conformity is claimed before final adoption and OJEU citation.

Identity frameworks. eIDAS 2.0 is distinguished from the proposed European Business Wallet Regulation. The wallet is presented as a possible organisational trust layer, not current law or a prerequisite.

AI threat. The prompt's 'general-public automated zero-day discovery' claim was narrowed. Current official evidence supports rapid capability uplift and lower barriers, while retaining skilled actors in the loop for advanced operations.

Zero Trust. NIST's PDP/PEP, control-plane and data-plane concepts are cited accurately. The evidence plane and five-subject model are labelled as the authors' architectural extensions.

Automation and conformity. The brief consistently separates machine-verifiable evidence from the legally attributable conformity decision.

Customer assurance. Bidirectional communication and fleet feedback are framed as governed operational capabilities, not as substitutes for OEM or customer controls or as an unrestricted right to collect product data.

Editorial and production. British English, section numbering, figure/table numbering, numeric citations, bibliography matching, CC BY notice, figure alt text and page-by-page rendering were checked in the production workflow.

> **LEGAL BOUNDARY** This brief is strategic and architectural guidance, not legal advice or a conformity determination. Product classification, applicable procedures and evidence sufficiency remain fact-specific.

References

[1] European Union (2024), Regulation (EU) 2024/2847 on horizontal cybersecurity requirements for products with digital elements (Cyber Resilience Act), OJ L 2024/2847. Source

[2] European Union (2022), Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union (NIS2), OJ L 333. Source

[3] European Union (2024), Regulation (EU) 2024/1781 establishing a framework for the setting of ecodesign requirements for sustainable products (ESPR), OJ L 2024/1781. Source

[4] European Commission (2026), Implementing Regulation (EU) 2026/1778 on the digital product passport registry, OJ L 2026/1778. Source

[5] European Commission (2026), Implementing Decision (EU) 2026/1736 on harmonised standards for digital product passports, OJ L 2026/1736. Source

[6] UK National Cyber Security Centre (2026), Impact of AI on cyber threat from now to 2027. Source

[7] UK AI Security Institute (2025), Frontier AI Trends Report. Source

[8] SPDX (2024), System Package Data Exchange Specification, version 3.0.1. Source

[9] OWASP Foundation and Ecma International (2025), CycloneDX Bill of Materials Standard, version 1.7. Source

[10] European Commission (2026), Cyber Resilience Act implementation: frequently asked questions and implementation guidance. Source

[11] Federal Office for Information Security (BSI) (2026), Technical Guideline TR-03183, Cyber Resilience Requirements for Manufacturers and Products. Source

[12] Rose, S., Borchert, O., Mitchell, S. and Connelly, S. (2020), Zero Trust Architecture, NIST SP 800-207. Source

[13] European Union (2024), Regulation (EU) 2024/1183 amending eIDAS as regards the European Digital Identity Framework, OJ L 2024/1183. Source

[14] European Commission (2025), Proposal for a Regulation on the establishment of European Business Wallets, COM(2025) 838 final. Source

[15] Moran, B., Tschofenig, H. and Birkholz, H. (2022), A Manifest Information Model for Firmware Updates in Internet of Things (IoT) Devices, IETF RFC 9124. Source

[16] European Union (2021), Regulation (EU) 2021/821 setting up a Union regime for the control of exports, brokering, technical assistance, transit and transfer of dual-use items, OJ L 206. Source

[17] European Union (2023), Regulation (EU) 2023/2854 on harmonised rules on fair access to and use of data (Data Act), OJ L 2023/2854. Source

[18] Souppaya, M., Scarfone, K. and Dodson, D. (2022), Secure Software Development Framework (SSDF) Version 1.1, NIST SP 800-218. Source

[19] IEC (2018–2019), IEC 62443-4-1, Secure product development lifecycle requirements, and IEC 62443-4-2, Technical security requirements for IACS components. Source

[20] European Commission (2025), Implementing Decision C(2025) 618 final, standardisation request M/606 in support of Regulation (EU) 2024/2847. Source

[21] ETSI (2026), 'ETSI launches approval process for 17 European Standards supporting the Cyber Resilience Act', 13 August 2026. Source