



Document Title	ShieldNet Cybersecurity Standard- E-commerce & Retail Add-on
Release Date	January 2026
Next Review	December 2026 (annual review cycle)
Distribution	Public – Creative Commons BY-NC-ND 4.0
Version	1.0

1. What is the E-commerce & Retail Add-on

The E-commerce and Retail Add on is a sector specific extension to the ShieldNet Core Standard for small and medium sized organizations that sell online, operate stores, or run mixed retail models. The Core Standard establishes the baseline cyber hygiene and resilience practices that every SME should have, regardless of industry. This Add on builds on that baseline by adding controls that address the most common abuse and harm patterns in this sector, such as account takeover, checkout and refund manipulation, promotion and gift card abuse, marketplace listing risks, and connected product exposure. It is designed to be practical for teams with limited time and budget, and to focus effort on the customer journeys and business processes where retail risk concentrates.

This Add on is grounded in the EU legal landscape that most often drives security expectations for E-commerce and Retail. It draws on NIS2 for risk management measures, incident handling, and supplier assurance expectations, and on GDPR for security of processing and breach response where personal data is involved. It also reflects the Digital Services Act for platform and marketplace duties around safe and trustworthy online environments, the Payment Services requirements through the RTS on strong customer authentication and secure communications for secure payment flows, and the General Product Safety framework for rapid action on unsafe products in digital commerce. Where retailers place connected products or digital elements on the market, the Cyber Resilience Act themes are used to support secure updates, vulnerability handling, and transparency toward users during the support period.

The result is a set of controls that is intentionally unique to the E-commerce and Retail sector and complements the Core Standard rather than repeating it. It helps you translate legal requirements into actions you can implement and evidence in a lightweight way, while keeping the focus on outcomes that matter to retail businesses, including customer trust, loss prevention, and continuity of sales operations.

2. How to use the E-commerce and Retail Add-on

Use this Add on the same way you use any ShieldNet sector module, as an extension after the Core Standard is in place. Start by implementing the Core Standard first, because it provides the essential governance, baseline protections, monitoring, and response foundations that every SME needs. Once the Core controls are operating, you then decide whether the E-commerce and Retail Add on should be applied as optional or required, based on your size, exposure, and criticality. For example, an organization with high transaction volume, heavy reliance on online revenue, broad supplier integrations, or marketplace features will typically treat the Add on as required rather than optional.

Begin with the Common Controls section, because those controls apply to all organizations in the sector, whether you are a pure online shop, a brand with stores, or a platform operator. The Common Controls are written to strengthen the highest risk retail journeys, such as customer account access, checkout, refunds, loyalty value, and product safety actions, and they are meant to be layered on top of the Core foundations. After the Common Controls are implemented, move to the detailed controls that match your organization type, such as online merchant with fulfillment, marketplace operator, omnichannel retailer, or retailer selling connected products or operating a retail app.

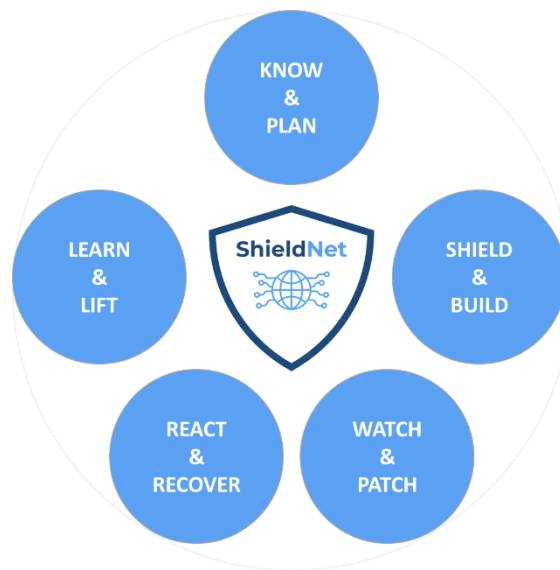
Follow the same adoption approach described in the Core guidance by keeping the implementation evidence light and reusable. Treat each control as a small operational commitment with clear ownership, a simple way to prove it is happening, and a routine review cadence that fits your business rhythm such as campaign cycles and peak seasons. If you are unsure where to start, prioritize the controls that reduce customer harm and financial loss fastest, then expand coverage until you meet the level of assurance your risk profile and legal obligations require.

3. Action Zones

The controls in each category are organized by the five ShieldNet Action Zones, mirroring the security lifecycle. Retail organizations should address all five zones for a comprehensive program:

- **KNOW & PLAN** - understanding your digital sales, store, and logistics assets, the threats and regulations that apply, and planning accordingly.
- **SHIELD & BUILD** - implementing protective measures and secure architecture for retail operations.
- **WATCH & PATCH** - monitoring for issues and keeping systems up-to-date.
- **REACT & RECOVER** - responding to incidents in a structured way to minimize financial loss and downtime and recovering critical services like payment processing and online storefronts quickly.
- **LEARN & LIFT** - learning from incidents and changes to continually improve.

Each control below is written in plain language and directly actionable. We reference EU regulations and industry standards (like GDPR, NIS2, DSA, Cyber Resilience Act, PSD2, PCI DSS) where relevant to show alignment - adhering to these controls will help meet those legal requirements. Use this add-on as a checklist or extension of your core ShieldNet implementation: integrate the controls into your risk assessments, update your security policy to cover these items, and assign responsibility (e.g. an IT Security Coordinator, store IT staff, DevOps team, or external service provider) for each. By following both the core and retail-specific controls, even small retail organizations can enhance their cybersecurity posture and compliance standing, protecting customers' data and payments while keeping the approach practical for a smaller team.



3.1. COMMON CONTROLS

The following controls are baseline cybersecurity requirements for all retail or e-commerce organizations in the ShieldNet program (online shops, physical retailers, marketplaces, logistics providers, etc.). They extend the Core Standard with retail-specific measures and are organized under the five Action Zones. Each control is proportionate for small teams, written in plain English, and mapped to EU laws or standards e.g., GDPR, NIS2, DSA, PCI DSS, to help you meet legal obligations. Implement these first across your organization and maintain simple evidence this will give you a defensible, audit-ready foundation that secures customer data, payment processes, and retail operations.

3.1.1. *KNOW & PLAN*

[KP-EC1] Map Customer Trust Journeys

Control text: Document the end to end customer journeys that create trust and loss exposure, including account access, checkout, refunds, loyalty value, and customer support. Identify where personal data, payment related data, and high value actions flow across teams and suppliers. Assign an owner per journey and list the top abuse scenarios to prevent.

Why: Ecommerce risk concentrates in a few high impact journeys, not across every system equally.

Evidence examples: Journey map, data flow diagram, list of high value actions, abuse scenario notes, named owners per journey.

Legal anchors: NIS2 Art. 21(2)(a), GDPR Art. 25(1), DSA Art. 25(1).

[KP-EC2] Set Fraud and Abuse Risk Rules

Control text: Define what fraud and abuse look like for your business, including account takeover, card testing, promotion abuse, refund abuse, and fake returns. Set clear thresholds for when to step up verification, block actions, or require manual review. Review the thresholds at least quarterly and after major campaigns.

Why: Clear thresholds prevent inconsistent decisions and reduce losses during traffic spikes.

Evidence examples: Fraud rulebook, threshold table, quarterly review notes, change log of rules.

Legal anchors: NIS2 Art. 21(2)(a), NIS2 Art. 21(2)(b), PSD2 RTS Art. 18(2)(c), PSD2 RTS 2018/389 Art. 21(1).

[KP-EC3] Prepare Product Safety and Illegal Product Actions

Control text: Maintain a simple playbook for handling dangerous or illegal products in digital sales, including who can delist, how to stop sales fast, and how to contact customers. If you run an online marketplace, define how you will meet product safety contact and internal process duties. Align this playbook with your incident response so cyber events and safety events do not collide.

Why: Product safety events move fast and can become reputational crises if you cannot act immediately.

Evidence examples: Product delisting procedure, contact list, customer notification templates, test record for a delisting drill.

Legal anchors: DSA Art. 9(1), DSA Art. 16(6), GPSR Art. 22(1), GPSR Art. 22(3).

3.1.2. SHIELD & BUILD

[SB-EC1] Protect Customer Accounts Against Takeover

Control text: Implement customer account defenses proportional to your risk, including rate limits, bot protection, and step up checks for high value actions like payout changes and address changes. Require recent authentication for sensitive actions and block reused compromised credentials where feasible. Ensure the login and reset flow is not manipulable by interface tricks.

Why: Account takeover is a top driver of fraud, refunds, and data exposure in retail.

Evidence examples: Login protection settings, step up policy, bot mitigation dashboard, test results for reset flow.

Legal anchors: GDPR Art. 32(1), NIS2 Art. 21(2)(e), DSA Art. 25(1).

[SB-EC2] Keep Payment Credentials Out of Your Systems

Control text: Use a payment flow that prevents your systems from storing or exposing customer authentication data and sensitive payment credentials. Ensure logs, support tools, and analytics never capture full credentials or authentication codes. If you must handle tokens, restrict their use to the minimum needed for the transaction.

Why: Reducing exposure of payment credentials limits breach impact and supports secure payment processing.

Evidence examples: Payment architecture diagram, log redaction rules, evidence of hosted payment or tokenization, support tool masking proof.

Legal anchors: PSD2 RTS Art. 22(1), PSD2 RTS Art. 22(2), GDPR Art. 32(1).

[SB-EC3] Secure Promotions Gift Cards and Store Value

Control text: Treat promotions, gift cards, store credit, and loyalty points as financial value and protect them with anti-abuse controls. Apply limits, anomaly checks, and step up verification for creation, redemption, and transfer. Keep rules consistent across web, app, and in store channels.

Why: Attackers often shift from payments to promotional value because controls are weaker and losses are harder to recover.

Evidence examples: Promotion abuse controls, gift card issuance limits, loyalty transfer policy, anomaly rule list.

Legal anchors: NIS2 Art. 21(2)(a), NIS2 Art. 21(2)(b), GDPR Art. 32(1).

3.1.3. WATCH & PATCH

[WP-EC1] Detect Account and Checkout Abuse Early

Control text: Monitor customer facing abuse signals, including spikes in failed logins, password resets, cart creation, checkout failures, and address changes. Alert when thresholds are crossed and require investigation within a defined time window. Maintain a short list of the most important signals to avoid alert fatigue.

Why: Early detection prevents losses and reduces customer harm during fast moving attacks.

Evidence examples: Abuse signal dashboard, alert rules, investigation tickets, weekly review notes.

Legal anchors: NIS2 Art. 21(2)(b), NIS2 Art. 21(2)(f), PSD2 RTS Art. 18(2)(c).

[WP-EC2] Track Fraud Rates and Chargeback Drivers

Control text: Track fraud and chargeback trends by payment method, channel, geography, and campaign. Identify the top drivers and adjust controls before thresholds become unacceptable. Share a short monthly summary with management.

Why: Fraud changes quickly, and trending data is your earliest indicator that controls are no longer effective.

Evidence examples: Monthly fraud report, chargeback analysis, rule change log, management summary email.

Legal anchors: PSD2 RTS Art. 19(1), PSD2 RTS Art. 21(1), NIS2 Art. 21(2)(f).

[WP-EC3] Watch Product Safety and Vulnerability Alerts for Sold Products

Control text: Subscribe to relevant product safety and vulnerability sources for products you sell, especially connected products. If you operate an online marketplace, integrate Safety Gate signals into internal review. Trigger delisting or warnings when credible risk is identified.

Why: Retailers and marketplaces are often the fastest way to stop harm once a dangerous or vulnerable product is in circulation.

Evidence examples: Safety Gate monitoring record, vulnerability alert inbox, delisting decisions, customer warning posting log.

Legal anchors: GPSR Art. 22(6), GPSR Art. 26(1), CRA Annex I Part II(2), CRA Annex II(7).

3.1.4. REACT & RECOVER

[RR-EC1] Run a Checkout Containment Playbook

Control text: Define how you will contain incidents that affect checkout, orders, or customer accounts, including when to disable features and when to switch to safer flows. Coordinate actions with your payment provider and key suppliers. Record every containment decision and its rationale.

Why: Speed matters during ecommerce incidents, and improvised actions often increase customer impact.

Evidence examples: Containment playbook, supplier contact tree, incident timeline, feature toggle audit log.

Legal anchors: NIS2 Art. 21(2)(b), NIS2 Art. 23(4)(a), GDPR Art. 33(1).

[RR-EC2] Notify Customers for Security and Safety Events

Control text: Prepare customer communications that explain what happened, what customers should do, and what you are doing next. Use clear language and provide a single trusted channel for updates. Ensure communications cover both data impact and product safety impact when applicable.

Why: Clear communication reduces harm, supports trust, and limits secondary fraud using confusion and phishing.

Evidence examples: Customer notice templates, update page, call center script, proof of dispatch to affected users.

Legal anchors: GDPR Art. 34(1), NIS2 Art. 23(1), DSA Art. 32(1).

[RR-EC3] Remove Dangerous Products and Support Recalls

Control text: If you run an online marketplace, ensure you can receive and execute authority orders for dangerous products quickly, and process product safety notices within required timeframes. Support effective recalls by notifying affected buyers and publishing recall information. Maintain an audit trail of all actions taken.

Why: Product safety actions have strict expectations and delays can directly harm consumers.

Evidence examples: Order handling log, notice processing log, buyer notification proof, delisting audit trail.

Legal anchors: GPSR Art. 22(4), GPSR Art. 22(8), GPSR Art. 22(12)(a), DSA Art. 9(1).

3.1.5. LEARN & LIFT

[LL-EC1] Review Security Outcomes After Peak Campaigns

Control text: After major sales events, review fraud, abuse, outages, and customer support escalations and identify what controls failed. Update thresholds and playbooks before the next campaign. Keep the review short and focused on actions.

Why: Peak periods reveal real weaknesses and provide the best data for improvement.

Evidence examples: Post campaign review notes, updated rule thresholds, updated playbooks, action tracker.

Legal anchors: NIS2 Art. 21(2)(f), PSD2 RTS Art. 21(1).

[LL-EC2] Improve Fraud Controls Using Evidence

Control text: Maintain a backlog of fraud and abuse improvements prioritized by loss and customer harm. Validate that each change reduced abuse without creating unfair friction. Retire controls that do not work.

Why: Continuous tuning is essential because attackers adapt faster than annual planning cycles.

Evidence examples: Fraud improvement backlog, before and after metrics, A B test results, retired rule list.

Legal anchors: NIS2 Art. 21(2)(f), PSD2 RTS Art. 19(1), PSD2 RTS Art. 21(1).

3.2. CONTROLS BY ORGANIZATION TYPE

In this section, the Ecommerce and Retail Add on provides control guidance tailored to different organization types found in the sector. While the common controls apply to all ecommerce and retail environments, the controls below focus on the specific risk drivers and operational realities of each model, such as account takeover and payment fraud for online stores, returns and refund abuse for customer operations, marketplace seller governance and product safety enforcement, and point of sale and store network resilience for physical retail. Use the controls that match your business model and delivery channels, and keep the scope aligned with the customer journeys and systems that are most critical to revenue, customer trust, and regulatory compliance.

3.2.1. ONLINE MERCHANT WITH OWN STORE AND FULFILMENT

[KP-EC4] Map Order Data Sharing and Shipping Dependencies

Control text: Document what order and customer data is shared with fulfilment, delivery, returns, and customer support vendors, and why. Confirm which partner is responsible for each security task in the order lifecycle. Review this map when adding a new carrier, warehouse, or customer service provider.

Why: Order operations often leak data through many small integrations that are easy to overlook.

Evidence examples: Order data flow map, vendor responsibility matrix, integration inventory, change review record.

Legal anchors: NIS2 Art. 21(2)(d), GDPR Art. 28(3), GDPR Art. 30(1).

[SB-EC4] Verify Identity in Customer Support Workflows

Control text: Implement a consistent identity check before support agents change account email, phone, address, payment details, or refund destination. Use a verification method that is resistant to social engineering and does not rely on easily guessed information. Log high risk support actions for review.

Why: Customer support is a common bypass route when logins are well protected.

Evidence examples: Support verification script, agent tooling rules, audit log of sensitive support changes, QA call reviews.

Legal anchors: GDPR Art. 32(1), NIS2 Art. 21(2)(i).

[WP-EC4] Monitor Order Manipulation and Integration Failures

Control text: Monitor for suspicious order edits, repeated address changes, unusual refund requests, and fulfilment API failures. Alert when patterns indicate account compromise or integration abuse. Investigate quickly during peak shipping windows.

Why: Many fraud cases show up first as order anomalies, not as classic security alerts.

Evidence examples: Order anomaly dashboard, investigation tickets, integration error logs, weekly anomaly review.

Legal anchors: NIS2 Art. 21(2)(b), NIS2 Art. 21(2)(e).

[RR-EC4] Contain Refund and Return Abuse During Incidents

Control text: Define how to pause or slow high risk refunds and returns during suspected fraud waves, while keeping legitimate customer remedies available. Use short time bound holds and manual review for high risk cases. Document criteria for returning to normal operations.

Why: Attackers monetize quickly through refunds and returns once they gain access.

Evidence examples: Refund hold criteria, manual review queue, incident decision log, post incident restoration record.

Legal anchors: NIS2 Art. 21(2)(b), GDPR Art. 32(1).

[LL-EC3] Improve Support and Customer Messaging Against Scams

Control text: Update customer support scripts and help pages to reduce phishing and impersonation risk, especially after incidents and campaigns. Include how customers can verify official messages and where to report suspicious contacts. Review effectiveness using customer reports and fraud cases.

Why: Clear guidance cuts down successful scams that exploit brand trust after high visibility events.

Evidence examples: Updated help content, support training notes, customer scam reports, reduction in impersonation tickets.

Legal anchors: NIS2 Art. 21(2)(g), GDPR Art. 32(1).

3.2.2. ONLINE MARKETPLACE OPERATOR WITH THIRD PARTY TRADERS

[KP-EC5] Maintain Trader Traceability File

Control text: Collect and securely store the required trader information before allowing sales, and keep it accurate and up to date. Define how you validate completeness and reliability using official sources or reliable documents. Delete the data after the required retention period ends.

Why: Traceability is the foundation for stopping illegal and unsafe trade while enabling enforcement when needed.

Evidence examples: Trader onboarding checklist, verification evidence, secure storage record, retention and deletion log.

Legal anchors: DSA Art. 30(1), DSA Art. 30(2), DSA Art. 30(5).

[SB-EC5] Enforce Product Safety Information on Listings

Control text: Ensure the listing workflow requires product safety and traceability information and displays it clearly to consumers. Block listings that miss required manufacturer and warning information until corrected. Keep a record of listing blocks and corrections.

Why: Missing safety information is one of the simplest signals of higher risk sellers and unsafe products.

Evidence examples: Listing form requirements, block rules, sample compliant listing, block and fix log.

Legal anchors: DSA Art. 31(1), GPSR Art. 22(9), GPSR Art. 22(10)(a).

[WP-EC5] Detect Frequent Non-Compliant Traders and Illegal Listings

Control text: Identify traders that repeatedly offer non-compliant or illegal products and apply escalation steps that include warnings and suspension. Use random checks and credible signals to detect illegal offers without imposing a general monitoring approach. Track repeat patterns and outcomes.

Why: Repeat offenders create systemic risk and must be handled consistently to protect consumers.

Evidence examples: Repeat offender report, suspension decisions, random check logs, warning notices to traders.

Legal anchors: GPSR Art. 22(11), DSA Art. 31(3), DSA Art. 23(1).

[RR-EC5] Execute Authority Orders and Trader Suspensions

Control text: Ensure you can receive authority orders, act on them quickly, and confirm execution through the designated channels. Suspend traders when required by traceability failures or repeated illegal activity, and preserve evidence of the decision. Provide clear redress information where applicable.

Why: Fast execution and good records are essential for enforcement, safety, and legal defensibility.

Evidence examples: Order receipt log, execution confirmation, trader suspension record, statement of reasons to trader.

Legal anchors: DSA Art. 9(1), DSA Art. 30(3), GPSR Art. 22(4).

[LL-EC4] Review Platform Interface Practices That Increase Risk

Control text: Review whether your interface design increases unsafe buying, scam risk, or dark pattern behavior, and fix the highest risk patterns first. Include buyer complaint themes and safety events in the review. Re test after changes.

Why: Small interface changes can sharply reduce unsafe decisions and reduce abuse at scale.

Evidence examples: Interface review notes, change tickets, buyer complaint analysis, before and after conversion and fraud indicators.

Legal anchors: DSA Art. 25(1), DSA Art. 31(1).

3.2.3. OMNICHANNEL RETAILER WITH STORES POS AND LOYALTY PROGRAM

[KP-EC6] Define Cross Channel Payment and Loyalty Threat Scenarios

Control text: Document how online and in store systems connect, including POS, loyalty, refunds, and customer identities. Define specific scenarios such as loyalty point theft, return fraud across channels, and credential reuse. Assign owners across retail operations and IT.

Why: Omnichannel attacks exploit the gaps between teams and channels.

Evidence examples: Omnichannel system map, threat scenario list, owner assignments, review notes with retail leadership.

Legal anchors: NIS2 Art. 21(2)(a), GDPR Art. 25(1).

[SB-EC6] Secure Loyalty Accounts and High Value Transfers

Control text: Apply stronger checks for loyalty redemption, point transfers, and high value discounts, especially when combined with returns. Align controls across store and online experiences so attackers cannot pivot to the weaker channel. Monitor staff assisted overrides as high risk actions.

Why: Loyalty value is easy to steal and often bypasses payment protections.

Evidence examples: Loyalty control rules, override logs, policy for manual approvals, test cases across channels.

Legal anchors: GDPR Art. 32(1), NIS2 Art. 21(2)(b).

[WP-EC6] Monitor POS and Store Payment Anomalies

Control text: Monitor for unusual POS patterns, refund spikes, and repeated failed payment attempts across stores. Correlate these signals with online fraud indicators during campaigns. Escalate quickly when anomalies suggest compromise or organized fraud.

Why: Store anomalies often indicate fraud operations that also target online accounts and promotions.

Evidence examples: POS anomaly report, store escalation tickets, correlation notes, monthly fraud meeting minutes.

Legal anchors: NIS2 Art. 21(2)(b), RTS 2018/389 Art. 18(2)(c).

[RR-EC6] Isolate Store Operations During Suspected Compromise

Control text: Define when and how to isolate store systems, limit refund capabilities, and switch to a safer operating mode. Communicate clear steps to store managers and helpdesk. Restore full functionality only after validation checks are complete.

Why: Containment in stores is time sensitive and needs operational clarity to avoid chaos.

Evidence examples: Store isolation procedure, manager quick guide, incident log, restoration checklist.

Legal anchors: NIS2 Art. 21(2)(b), NIS2 Art. 23(4)(a).

[LL-EC5] Reconcile Fraud Across Channels and Reduce Weak Links

Control text: Review fraud cases that crossed channels and identify the weakest control in the chain. Prioritize fixes that remove the pivot path rather than adding friction everywhere. Confirm improvement with the next quarter of fraud data.

Why: Closing pivot paths reduces repeat attacks and improves customer experience.

Evidence examples: Cross channel case review, prioritized fixes list, updated controls, quarterly outcome summary.

Legal anchors: NIS2 Art. 21(2)(f), RTS 2018/389 Art. 21(1).

3.2.4. RETAILER OR BRAND SELLING CONNECTED PRODUCTS OR A RETAIL APP

[KP-EC7] Publish Security Support and Vulnerability Contact for Digital Products

Control text: For each connected product or app you place on the market, publish how long security updates will be provided and where vulnerabilities can be reported. Maintain a simple

coordinated vulnerability disclosure policy and keep it accessible. Ensure customer support can route vulnerability reports to the right team quickly.

Why: Transparency and a clear intake path are required to handle vulnerabilities at scale and protect users.

Evidence examples: Public support period statement, vulnerability contact page, disclosure policy, support routing guide.

Legal anchors: CRA Annex II(2), CRA Annex II(7), CRA Annex I Part II(5).

[SB-EC7] Secure Update Delivery for Apps and Connected Products

Control text: Ensure updates are delivered through a secure channel with integrity checks, and provide security updates without unnecessary delay. Separate security updates from feature updates where feasible. Provide advisory messages that explain what users should do.

Why: Update channels are a prime target and a failed update process can create widespread user harm.

Evidence examples: Update security design, integrity verification evidence, release notes, advisory message templates.

Legal anchors: CRA Annex I Part II(7), CRA Annex I Part II(8), CRA Annex I Part II(2).

[WP-EC7] Maintain a Vulnerability Intake and Triage Process

Control text: Track reported vulnerabilities, confirm affected versions, and prioritize fixes based on severity and exploitability. Share fixes and relevant information with component maintainers when appropriate. Keep the record updated for the full support period.

Why: A repeatable process prevents missed reports and supports timely remediation obligations.

Evidence examples: Vulnerability tracker, triage notes, vendor notifications, support period tracking record.

Legal anchors: CRA Art. 13(7), CRA Art. 13(8), CRA Annex I Part II(1).

[RR-EC7] Report Actively Exploited Vulnerabilities and Inform Users

Control text: If you become aware of an actively exploited vulnerability or a severe incident impacting product security, follow the required reporting timeline and inform affected users with clear mitigation steps. Maintain a ready template for rapid notifications and user advisories. Coordinate public messaging to reduce exploitation and confusion.

Why: Rapid reporting and user guidance reduce real world harm and limit cascading incidents.

Evidence examples: Early warning template, reporting submission record, user advisory message, incident timeline.

Legal anchors: CRA Art. 14(1), CRA Art. 14(2)(a), CRA Art. 14(2)(b), CRA Art. 14(8).

[LL-EC6] Improve Vulnerability Handling Performance Over Time

Control text: Track how long it takes to acknowledge, fix, and communicate vulnerabilities and use the data to improve. Focus improvements on the slowest steps, such as triage, release, and customer reach. Review results every quarter.

Why: Continuous improvement is essential because vulnerability volume grows with product adoption.

Evidence examples: Vulnerability handling metrics, quarterly review notes, process change log, improved timelines evidence.

Legal anchors: CRA Annex I Part II(2), NIS2 Art. 21(2)(f).