



ShieldNet

Document Title	ShieldNet Cybersecurity Standard
Release Date	September 2025
Next Review	August 2026 (annual review cycle)
Distribution	Public – Creative Commons BY-NC-ND 4.0
Version	1.1

1. Why this Standard Exists

Small and medium businesses today face a growing maze of cybersecurity obligations under European Union law. In just the past few years, landmark regulations like the NIS2 Directive, GDPR, the Cyber Resilience Act, the Digital Services Act, and others have set new expectations for how companies protect their data, products, and users. But for startups, SMEs, and NGOs, keeping up with these evolving legal requirements can be overwhelming. Many struggle to untangle which rules apply, what “minimum compliance” means, or how to prepare for multi-agency breach reporting. Most don’t have a full-time security team or legal counsel on hand. Meanwhile, cyberattacks are rising in frequency and impact – from ransomware disrupting hospitals and local councils, to supply chain hacks exposing customer data across thousands of businesses. The damage is real: trust is lost, reputations are hurt, and the financial costs can be fatal for smaller organizations.

The ShieldNet Cybersecurity Standard is built to close this gap. It offers a practical, plain-language cybersecurity playbook for small organizations that want to protect themselves, comply with EU law, and build digital trust – without getting buried in complexity. This standard distills the shared baseline obligations across all major horizontal EU cybersecurity regulations into a clear structure of 48 mandatory controls. These are grouped into five “Action Zones” that mirror the natural flow of a security program: plan, protect, monitor, respond, and improve. The controls are designed for real-world use – each one is short, understandable, and matched to the kind of capabilities a lean team can manage. Whether you're a five person civic tech startup or a 100 person education NGO, this standard gives you a practical foundation to meet your legal obligations, demonstrate good security hygiene, and foster long-term resilience. By helping small innovators “do security right,” This standard supports a stronger, safer, and more trusted digital economy across the European Union.

2. How we have built the Standard

The ShieldNet Cybersecurity Standard was designed from the ground up to be lightweight but rigorous – providing meaningful security guidance without overwhelming small teams. To achieve this, the standard is built on a flexible schema that considers two key dimensions:

- Organization Size & Capacity
- Sector Exposure or Sensitivity

The core controls in this document represent the minimum baseline that every startup, SME, or NGO should meet – regardless of their industry. These controls were selected to be feasible for smaller organizations (≤ 250 staff) with modest IT and compliance resources. They rely on practical processes, open-source tools, and proportional effort. Most controls can be implemented by an internal InfoSec Coordinator, not requiring a full security team. Controls also scale: while a 5-person SaaS start-up might track risks in a spreadsheet, a 200 person manufacturer might use formal registers and dedicated tools – but the expectation is the same.

At the same time, the standard recognizes that some organizations face sector-specific risks or regulations. For this reason, ShieldNet Cybersecurity Standard includes a modular “Sector Add-Ons”. Organizations handling sensitive personal data, operating in regulated sectors like finance or healthcare, or providing high-risk digital services (e.g. AI, critical infrastructure platforms) can augment the core controls with additional sector-specific requirements. This matrix-based design – core for size, extended for sector – keeps the standard adaptable and risk-based. It avoids one-size-fits-all complexity, while still aligning with EU law’s principles of proportionality and accountability. Whether you’re a civic tech startup, a B2B software vendor, or a grassroots NGO, this schema ensures you can adopt and grow your security program in step with your actual exposure – and demonstrate it clearly to regulators, partners, and users.

	<i>Low Sensitivity Sector</i>	<i>Moderate Sensitivity Sector</i>	<i>High Sensitivity Sector</i>
Micro	CORE Only	CORE Only	CORE + Optional
Small	CORE Only	CORE + Optional	CORE + Mandatory
Medium	CORE + Optional	CORE + Mandatory	CORE + Mandatory + Audit

3. Who This Standard Is For – and How to Read It

ShieldNet Cybersecurity Standard is built for startups, small-to-medium-sized enterprises (SMEs with up to 250 staff), and non-profit NGOs that operate in or sell into the European Union. It focuses on horizontal cybersecurity rules – that means the general, cross-sector requirements found in core EU laws like the NIS 2 Directive, GDPR, the Cyber Resilience Act, the Cybersecurity Act, the Digital Services Act, and others. These laws apply to many organizations regardless of what industry they’re in.

This standard pulls out the common baseline security duties from those laws and turns them into a clear set of 48 practical, mandatory controls. Every control in this document uses the word “must” – because they reflect the minimum practices that small organizations are expected to follow. If your organization operates in a regulated sector like health, finance, or energy, you might need to extend this core with sector-specific controls defined in the “Sector Add-On”. But the base standard gives you a solid legal and security foundation, with a focus on proportionate, real-world measures that small teams can actually implement.

Here’s a quick glossary of key terms used throughout this standard:

Term	Definition (for purposes of this standard)
<i>SME / Startup</i>	Micro, Small or medium enterprise with ≤ 250 employees.
<i>NGO</i>	Non-governmental, non-profit organization.
<i>Board</i>	The top executive or governing body of the organization (e.g. directors).
<i>InfoSec Coordinator</i>	Person appointed to manage and coordinate cybersecurity efforts (part-time role or dedicated).
<i>System Owner</i>	Individual responsible for a specific IT system or data set and its security.
<i>Third-Party Provider</i>	External supplier of services or products (e.g. cloud, IT support) that the organization uses.
<i>Control</i>	A mandatory security requirement in this standard (all controls use “must” language).

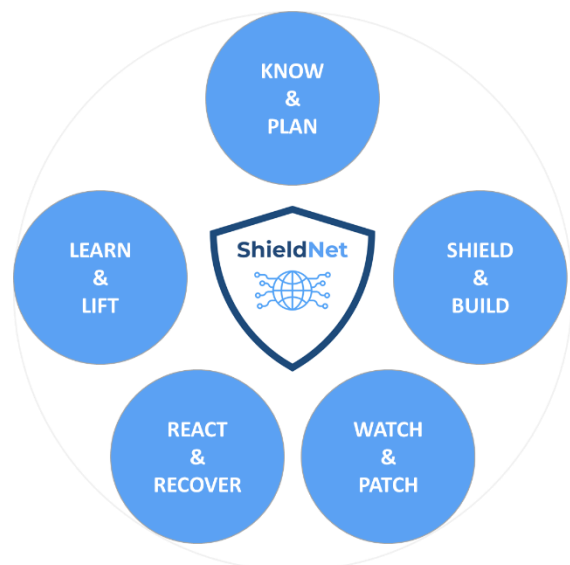
4. Who Does What in Security

All stakeholders in the organization have a part to play in cybersecurity. The table below summarizes key responsibilities:

Role	Key Accountabilities
<i>Board</i>	- Ultimately accountable for cybersecurity and compliance. - Approve the security program and allocate sufficient resources. - Embed cybersecurity into overall strategy and risk management. - Review cybersecurity status and major incidents at least annually, ensuring corrective actions.
<i>Info-Sec Coordinator</i>	- Day-to-day lead for implementing this standard's controls. - Develops and updates security policies and procedures. - Monitors threats, vulnerabilities, and compliance with regulations. - Reports regularly to the Board on cybersecurity risks, incidents, and improvements.
<i>System Owner</i>	- Ensures security of their assigned system or data set (e.g. maintaining updates, backups, access controls). - Implements applicable controls from this standard for their system. - Evaluates and accepts residual risk for the system in line with organizational risk appetite (in consultation with the Board/Coordinator).
<i>All Staff</i>	- Follow the organization's security policies and procedures in daily work. - Maintain basic cyber hygiene (e.g. use strong passwords, handle data safely). - Complete required security training and awareness activities. - Stay vigilant and immediately report suspected incidents or weaknesses.
<i>Third-Party Provider</i>	- Adhere to the organization's security requirements as per contracts/agreements. - Protect the organization's data and systems they have access to, at least to the same standard as the organization does. - Inform the organization of any security incident or breach affecting the provider's service. - Comply with applicable data protection clauses (e.g. GDPR data processing agreements) and assist in incident response and audits as needed.

5. Action Zones

The Action Zones are the heart of the ShieldNet Cybersecurity Standard – a five-part structure that breaks cybersecurity into manageable focus areas. These five zones – *KNOW & PLAN*, *SHIELD & BUILD*, *WATCH & PATCH*, *REACT & RECOVER*, and *LEARN & LIFT* – cover everything from preparation to continuous improvement. Together they provide a comprehensive roadmap for managing risks, ensuring no critical aspect of security is overlooked. The approach is deliberately kept clear and accessible: each zone is named in plain English and corresponds to a key stage in the security lifecycle. By organizing controls into these zones, even organizations with small teams can tackle cybersecurity step by step. The language is simple and the actions are practical, making it easier for startups, SMEs, and NGOs to engage with the guidance without needing specialist expertise.



In practice, the Action Zones guide how to sequence and assign cybersecurity activities in a small organization. First comes *KNOW & PLAN*, where the team identifies what needs protecting and charts out a sensible security plan (establishing a “security mindset” from the start). Next is *SHIELD & BUILD*, focused on putting up defenses and building secure systems according to the plan – for example, setting up firewalls, access controls, and safe development practices. The third zone, *WATCH & PATCH*, is all about vigilance: continuously monitoring systems, training staff to spot issues, and promptly patching or updating to fix weaknesses. If an incident does occur, the organization shifts into *REACT & RECOVER*, executing its incident response plan to contain damage and restore operations – a prepared team will always handle incidents far more efficiently than one caught off-guard, and today companies are judged by how well they respond rather than if they get hacked at all. Finally, the cycle concludes with *LEARN & LIFT*, encouraging a mindset of continuous improvement. In this zone the team reviews what happened, learns lessons, and “lifts” its security maturity to prevent similar issues in the future. By following these five zones in sequence and spirit, startups, SMEs, and NGOs can assign clear responsibilities for each stage and foster the right mindset at each step – from strategic planning through proactive defense, active monitoring, emergency response, and ongoing learning. This structured yet flexible approach turns cybersecurity from an overwhelming challenge into a series of actionable phases that fit naturally into an organization’s workflow, ensuring progress and resilience over time.



5.1. KNOW & PLAN

Know your assets, risks, and obligations – and plan ahead for security.

Good security starts with knowing what you have and what you need to protect. In this zone, the organization lays its cybersecurity foundation: identifying critical information and systems, understanding its legal duties, and planning how to manage risk. Leadership involvement is key – a clear plan and assigned responsibilities ensure everyone knows what to do. This section translates broad requirements (like NIS2’s call for risk analysis policies and asset management) into concrete actions. By mapping risks, resources, and regulations, a small organization can prioritize its efforts smartly. Plan now to avoid panic later: create policies, prepare for continuity, and bake security and privacy into new projects from the start. (If the organization provides online services or AI, special planning steps ensure compliance with the Digital Services Act and AI Act as well.)

[KP1] Assign Security Responsibility

Control text: Designate an internal InfoSec Coordinator (however small the organization) and define their authority to implement security controls.

Why: Every organization needs a point person for security otherwise, critical tasks will be missed.

Evidence examples: Appointment letter from CEO, org chart showing role, job description, meeting notes.

Legal anchors: GDPR Art 5(2), NIS2 Art. 21(2)(a), NIS2 Art. 20(6).

[KP2] Map Legal Requirements

Control text: Maintain a simple compliance matrix listing all EU cybersecurity / data security laws that apply to the business and mapping how each requirement is met. A list of horizontal laws and mapping to specific ShieldNet Cybersecurity controls can be found in Annex B. Use the ShieldNet sector Add-ons to map sector specific requirements.

Why: This ensures no obligation “falls through the cracks” even sector specific – avoiding fines or legal troubles

Evidence examples: Compliance matrix table (law vs. controls), regulatory tracker spreadsheet, meeting records reviewing legal changes.

Legal anchors: GDPR Art. 5(2), NIS2 Art. 21(1), Cybersecurity Act Art. 53, DSA Art. 10(2).

[KP3] Inventory Assets & Data

Control text: Create and update an asset register covering all IT systems, devices, software, and datasets and classify each by sensitivity (e.g. confidential, internal, public) and criticality (e.g. high, medium, low). Try to group assets by process it will help you to assess risks.

Why: You can't protect what you don't know about. An up-to-date inventory lets you focus on what's mission-critical or sensitive.

Evidence examples: Asset inventory spreadsheet, network diagram, data flow map, personal data processing registry.

Legal anchors: NIS2 Art. 21(2)(i), NIS2 Art. 21(2)(d), GDPR Art. 30, CRA Annex I(1).

[KP4] Assess Risks Regularly

Control text: Conduct a cyber risk assessment at least annually and for major changes – identify key threats, impacts, and likelihood, and decide how to reduce or accept each risk. Try to assess the risks and impact to processes rather than systems, it will help you understand which systems to prioritize.

Why: A periodic “reality check” on risks prevents complacency. It helps prioritize limited resources to the most serious threats (e.g. ransomware, data leaks).

Evidence examples: Risk register (with risks, ratings, mitigations), risk assessment report, meeting minutes approving risk treatment.

Legal anchors: NIS2 Art. 21(2)(a), GDPR Art. 32(1), AI Act Art. 9.

[KP5] Establish Security Policies

Control text: Write down a cybersecurity policy (and supporting procedures) covering at least access control, data handling, device use, and incident reporting, and have top management approve it. The main document should be short and set the rules of cybersecurity in your organization. Support the document by adding standards and procedures if necessary.

Why: Policies set the rules of the road. Written, approved policies make expectations clear to everyone (“use strong passwords”, “report incidents immediately”, etc.).

Evidence examples: Approved security policy document, acceptable use policy, employee handbook section on IT security, revision history showing annual review.

Legal anchors: NIS2 Art. 21(2)(a), NIS2. Art 21(2)(g), GDPR Art. 24(2), DSA Art 14.

[KP6] Plan for Continuity

Control text: Develop a basic business continuity and disaster recovery plan addressing how to keep working through common crises (e.g. malware outbreak, IT outage) including data backups and restoration procedures. Ensure you define who does what in case of an incident.

Why: Outages or cyberattacks shouldn't put you out of business. Planning backup and recovery in advance reduces downtime and chaos when incidents hit.

Evidence examples: BCP / DR plan document, backup schedule and logs, list of critical systems with Recovery Time Objectives (RTOs), disaster recovery drill reports.

Legal anchors: NIS2 Art. 21(2)(c), GDPR Art. 32(1)(c)&(d), CRA Annex I(1)(c).

[KP7] Vet Suppliers & Partners

Control text: Screen third-party providers for security before and during engagement, ensure contracts include security / data protection requirements, and prefer certified or reputable suppliers. Use public registers like STAR Registry from Cloud Security Alliance for cloud service providers.

Why: Your security is only as strong as your weakest vendor. A bad breach at a supplier can cascade to you, so choose and manage partners with care.

Evidence examples: Vendor security checklist, due diligence reports, contract clauses for GDPR and security, copies of ISO 27001 or EU security certification from suppliers.

Legal anchors: NIS2 Art. 21(2)(d), GDPR Art. 28(1)&(3), Data Act Art. 27(1).

[KP8] Build Security into Projects

Control text: For every new IT system, product, or feature, embed security and privacy by design – set security requirements from the start and review designs for potential weaknesses (including protection of personal data). Expect the same from your vendors.

Why: It's cheaper and safer to build it right than to fix it later. Early attention to security (access control, encryption, minimal data use) prevents dangerous flaws and privacy breaches.

Evidence examples: Secure design checklist in project plans, architecture review meeting notes, threat modeling documents, privacy impact assessment (for new personal data uses).

Legal anchors: NIS2 Art. 21(2)(e), GDPR Art. 25(1), CRA Art. 10(2), AI Act Art. 15.

[KP9] Set Online Content Rules

Control text: If you host or transmit user content (as an online platform or service), publish clear terms of use banning illegal content/abuse and implement a notice-and-action process to remove or disable illegal content when notified.

Why: Even small platforms must keep users safe online and obey the Digital Services Act. Clear rules and quick removal of illegal material (e.g. hate speech, pirated data) protect users and avoid liability.

Evidence examples: Terms of Service on website (with content policies), procedure for handling takedown notices, log of content removal requests and actions, designated point-of-contact for authorities.

Legal anchors: DSA Art. 14(1) & Art. 16, DSA Art. 17, DSA Art. 10(1).

[KP10] Manage AI Risks

Control text: If you develop or deploy AI systems, identify any high-risk AI per the EU AI Act and implement required controls (risk assessment, data quality checks, human oversight, etc.) before use or market release.

Why: AI can introduce new risks (e.g. biased decisions, unsafe behavior). Making sure your AI is trustworthy and compliant prevents harm and legal issues.

Evidence examples: AI system inventory (with risk category noted), AI risk assessment reports, records of AI training data provenance and quality tests, documentation of human review/override in AI processes.

Legal anchors: AI Act Art. 9, AI Act Art. 10, AI Act Art. 13, AI Act Art. 15.

5.2. SHIELD & BUILD



Shield your technology and build it strong – keep attackers out from the start.

This zone is about putting protective measures in place. You’ve planned; now it’s time to build defenses around your systems and data. These controls correspond to classic “preventive” cybersecurity: controlling access, hardening systems, using encryption, and developing software securely. The focus is on practical steps a small IT team can take – for example, turning on multi-factor authentication, installing firewalls, and avoiding default passwords. EU laws expect even smaller entities to practice basic cyber hygiene like this. The Cyber Resilience Act also requires manufacturers to design products with fewer vulnerabilities, and GDPR demands protecting personal data through measures like pseudonymization and access control. In short, Shield & Build is where you fortify your castle: ensuring only the right people get in, building systems that resist common attacks, and reducing the harm if something does go wrong.

[SB1] Control User Access

Control text: Maintain unique user accounts for each person and service, and grant each account the minimum access rights it needs (principle of least privilege). Regularly remove or adjust access when roles change.

Why: Tight access control prevents both accidents and malicious use. Unique IDs and least privilege mean if one account is compromised, the damage stays limited.

Evidence examples: List of active user accounts with roles, access control policy, user access review records, account termination checklist for leavers.

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

[SB2] Secure Hiring and Exit

Control text: Screen employees and contractors (at least verify identity and basic references for trustworthiness) and have them sign confidentiality agreements. Upon terminations or role changes, promptly revoke all their access and retrieve company devices.

Why: Insider threats are real. Basic HR security steps such as hiring vetted people and cutting access when they leave, prevent misuse of systems and data.

Evidence examples: HR onboarding checklist (with security steps), NDA forms, background check policy or records, leaver offboarding log (account disablement timestamps).

Legal anchors: NIS2 Art. 21(2)(i), GDPR Art. 5(1)(f).

[SB3] Enable Multi-Factor Authentication

Control text: Turn on multi-factor authentication (MFA) for all remote logins and important accounts (at least administrators, email, VPN, cloud dashboards) – requiring a second factor (app code, key, etc.) beyond just password.

Why: Stolen or guessed passwords alone shouldn't grant access. MFA is a cheap and effective way to stop most account breaches cold.

Evidence examples: MFA enforcement setting screenshots, list of systems with MFA enabled, user MFA enrollment records, authentication policy.

Legal anchors: NIS2 Art. 21(2)(j), CRA Annex I(1)(d), GDPR Art. 32(1).

[SB4] Protect User Devices

Control text: Secure all endpoints (computers, phones, tablets) with baseline protections: install reputable anti-malware software, enable host firewalls, apply security patches, and enforce device login passwords/PINs and auto-lock.

Why: Laptops and mobiles are prime targets. A lost or infected device can become a backdoor. Basic hygiene on devices helps prevent malware and data loss (part of "cyber hygiene").

Evidence examples: Endpoint management tool reports, anti-virus deployment records, device encryption setting, mobile device policy (BYOD rules).

Legal anchors: NIS2 Art. 21(2)(g), GDPR Art. 32(1)(b)&(c), CRA Annex I(1)(e).

[SB5] Secure Your Network

Control text: Use a firewall or cloud security groups to block unwanted network traffic, and segment networks so that critical systems (e.g. servers, production environment) are isolated from user PCs or public internet access except for what's necessary.

Why: A well-configured network is like a moat – it keeps many attackers out and limits movement if they do get in. Segmentation contains breaches to prevent a single infected laptop from compromising an entire database.

Evidence examples: Network diagram highlighting firewall zones, firewall configuration file showing allowed ports/IPs, VLAN or subnet setup documentation, penetration test reports showing network isolation.

Legal anchors: NIS2 Art. 21(2)(e), CRA Annex I(1)(c)&(d).

[SB6] Harden Configuration

Control text: Configure systems securely: disable or uninstall default accounts, passwords, and services you don't need; use secure settings (e.g. turn on OS security features, restrict admin interfaces to internal network). Establish a baseline configuration and apply it consistently.

Why: Out-of-the-box settings are often easy targets. Taking an hour to turn off unused features and enforce good settings closes common holes (many attacks exploit default creds or open ports).

Evidence examples: Secure configuration checklist, screenshots of critical system settings (e.g. "password required: yes", services list), configuration management policy, results from a CIS Benchmark or similar hardening guide.

Legal anchors: NIS2 Art. 21(2)(e), CRA Annex I(1)(b)&(d).

[SB7] Encrypt Sensitive Data

Control text: Encrypt data wherever appropriate – especially personal data or confidential info. Use HTTPS/TLS for data in transit, and use strong encryption (or hashing/pseudonymization) for data at rest (files, databases, backups), with proper key management.

Why: Encryption is a safety net. Even if attackers grab your data, encryption can make it useless to them. It's often explicitly expected for personal data protection.

Evidence examples: Inventory of sensitive data with encryption status (e.g. "HR database – encrypted at rest"), TLS test results for website (showing strong cipher configuration), encryption policy, key storage procedure (e.g. keys in a secure vault).

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

[SB8] Develop & Acquire Securely

Control text: Build security into software development and procurement: follow secure coding practices (validate inputs, handle errors safely, etc.), use code analysis / testing tools, and avoid using components with known vulnerabilities or patch them before release. Apply similar scrutiny when buying/off-the-shelf solutions.

Why: Most security bugs are mistakes in code or known flaws in components. By adopting secure coding guidelines and checking for vulns (in your code or open-source libraries) early, you ship safer products and reduce patch fire drills.

Evidence examples: Secure coding standard document, code review checklist including security, results of dependency vulnerability scans (e.g. "no critical CVEs open"), penetration testing or QA security test reports before go-live, supplier security questionnaire for COTS software.

Legal anchors: NIS2 Art. 21(2)(e), CRA Art. 10(2), CRA Annex I(1)(d), AI Act Art. 17.

[SB9] Minimize Data Collection

Control text: Collect and retain only the data you need for business purposes, especially personal data. Don't store sensitive data (like customer personal info) longer than necessary; anonymize or delete it when no longer required. Configure systems to enforce data retention and deletion policies.

Why: Data you don't have can't be stolen. Unnecessary hoarding of data (especially personal data) increases breach impact and legal risk. Data minimization is a core privacy and security principle.

Evidence examples: Data inventory indicating purpose and retention period for each dataset, data retention/deletion policy, logs of automated data deletion, example of an anonymization technique applied to a dataset.

Legal anchors: GDPR Art. 5(1)(c) & (1)(e), GDPR Art 25(2), CRA Annex I(1)(b), AI Act Art. 10(3).

5.3. WATCH & PATCH



Watch for signs of trouble, and patch problems quickly to stay secure.

Even strong shields can be breached. This zone focuses on detecting issues early and fixing them fast. Small organizations often lack dedicated SOC's, but they can still implement basic monitoring – collecting logs, checking alerts, and keeping an eye on news about threats. EU directives like NIS2 emphasize timely detection and remediation of vulnerabilities. The Cyber Resilience Act likewise mandates that manufacturers have processes to handle and disclose vulnerabilities throughout a product's lifecycle. For an SME, "Watch & Patch" means setting up simple mechanisms to know when something's wrong (like an unauthorized login or an available security update) and then acting promptly. By watching systems (and what vendors are doing) and proactively patching software, the organization can prevent incidents or keep them small. Essentially: be your own cyber lookout – stay vigilant, and never ignore a known weakness.

[WP1] Log Security Events

Control text: Enable logging on systems, applications, and security devices to record important events (logins, admin actions, errors, etc.), and retain those logs in a safe place for at least 6 months for analysis.

Why: Logs are your security camera. When something goes wrong, logs provide clues – or even an early warning – about what happened and who did what. No logs = flying blind during an incident.

Evidence examples: System log configuration (e.g. syslog settings, cloud service audit logs enabled), sample log files showing timestamps and events, centralized log archive setup, log retention policy.

Legal anchors: NIS2 Art. 21(2)(a)&(b), CRA Annex I(2), AI Act Art. 12.

[WP2] Monitor for Anomalies

Control text: Regularly review logs and alerts for signs of incidents or suspicious behavior – such as repeated failed logins, unusual after-hours access, new devices on the network – and investigate promptly.

Why: Attackers often leave footprints. By watching for odd patterns, you can catch breaches early. Even a small team can spot red flags if they look (or set up basic alerting tools).

Evidence examples: List of defined security alerts (e.g. "email if >5 failed login attempts"), log review schedule or checklist, SIEM/monitoring tool screenshots with example alerts, incident tickets spawned from detected anomalies.

Legal anchors: NIS2 Art. 21(2)(b), GDPR Art. 32(1)(d), CSA Art. 5(1)(a).

[WP3] Apply Patches Quickly

Control text: Install security updates and patches for operating systems, software, and firmware as soon as possible, preferably within 14 days of release or sooner if a critical vulnerability is being actively exploited. Enable automatic updates where feasible.

Why: Patches fix known holes. Cybercriminals often exploit bugs that already have fixes available, beating them to the punch by updating promptly is one of the simplest and most effective defenses.

Evidence examples: Patch management log or ticket system showing update timelines, automatic update settings enabled on devices, list of current software versions vs. latest available, policy requiring prompt patching of critical vulns (e.g. within 48 hours).

Legal anchors: NIS2 Art. 21(2)(e), CRA Annex I(2), GDPR Art. 32(1)(b), CSA Recital 100.

[WP4] Scan for Vulnerabilities

Control text: Regularly scan systems for known vulnerabilities and misconfigurations – using free or commercial vulnerability scanners, and address any high-risk findings. Perform these scans at least quarterly and after significant changes.

Why: A vulnerability scanner is like a health check for your IT, it can find “holes” you didn’t realize were there (e.g. an outdated server or open port). Routine scans help catch missed patches or insecure settings before attackers do.

Evidence examples: Recent vulnerability scan reports (with date and number of findings), list of open issues from scans and their remediation status, documented process for monthly or quarterly scanning, screenshots from tools (e.g. OpenVAS, Nessus) showing scans.

Legal anchors: NIS2 Art. 21(2)(e), CRA Annex I(2), GDPR Art. 32(1)(d).

[WP5] Get Threat Alerts

Control text: Subscribe to threat intelligence feeds or alerts relevant to your technology (e.g. CERT-EU, national CSIRT bulletins, vendor security advisories) so you are aware of emerging cyber threats and patches. Act on alerts that impact your systems.

Why: Staying in the know helps you react faster. If an exploit or ransomware is targeting businesses like yours, you want to hear about it early, preferably from a trusted alert, not from the attackers themselves.

Evidence examples: Subscription confirmations to CERT or ISAC bulletins, vendor security mailing list emails, internal process for reviewing and actioning alerts (e.g. “Log4j vulnerability, assessed and patched within 2 days” documented), threat intel platform screenshot.

Legal anchors: CSA Art. 7(1), NIS2 Recital 57, NIS2 Art. 29(4).

[WP6] Test Security Regularly

Control text: Conduct periodic security tests of your environment, such as an annual penetration test or at least a basic vulnerability assessment, as well as drills like phishing tests or simulated incidents, to evaluate and improve your defenses.

Why: You don’t want the attacker to be the first to find a weakness. Regular testing by friendly testers (or internal drills) finds the cracks so you can fix them. Drills also keep your team sharp and reveal gaps in procedures.

Evidence examples: Penetration test report (with date and summary of findings), records of a phishing simulation campaign and results (click rates, etc.), tabletop incident drill agenda and notes, plan for remediation of issues found in tests.

Legal anchors: NIS2 Art. 21(2)(f), GDPR Art. 32(1)(d), CRA Annex I(1)(c).

[WP7] Prepare for Vulnerability Reports

Control text: Set up a public contact (e.g. security@ email or web form) for external researchers or users to report security vulnerabilities. Acknowledge reports and fix verified issues without undue delay, and inform the reporter (and public, if appropriate) when fixed.

Why: You want friendly heads-up about flaws, not silent exploitation. Providing a channel for responsible disclosure can lead to valuable findings at little cost, and it shows good faith to regulators and customers that you handle vulnerabilities seriously.

Evidence examples: Web page or security.txt file with disclosure instructions, sample vulnerability report and your response, internal procedure for triaging and fixing reported vulns, record of an announced fix (e.g. release notes or advisory to users).

Legal anchors: CRA Annex I(2), NIS2 Art. 21(2)(e), CSA Art. 26(1)(c).

[WP8] Review Access and Privileges

Control text: Periodically audit user accounts and privileges (at least twice a year) to ensure that active accounts are still needed and that each user’s access rights are appropriate for their current role. Disable or adjust any that aren’t.

Why: Over time, people switch roles or leave, and access tends to accumulate (“permission creep”). Regular housekeeping finds dormant accounts (which hackers love to exploit) and over-privileged users, tightening your overall security.

Evidence examples: User access review report (listing accounts checked and changes made), meeting notes from an access review session, before-and-after examples where a user’s unnecessary admin rights were removed, access recertification policy.

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

[WP9] Verify Backups & Recovery

Control text: Test your backups and recovery procedures regularly (e.g. quarterly file restore tests and an annual full restore drill for a critical system) to ensure data can be restored and systems recovered within acceptable timeframes.

Why: Simply having backups isn’t enough, you need confidence they actually work. Regular restore tests catch backup failures or corrupted files, so you’re not unpleasantly surprised during a real crisis. Practice also hones your team’s recovery skills.

Evidence examples: Backup restoration test log (dates, data restored, success/fail), screenshots of a successful test restore, disaster recovery drill report (time to recover vs. target RTO), backup system dashboard showing backup job status.

Legal anchors: NIS2 Art. 21(2)(c), GDPR Art. 32(1)(c), NIS2 Art. 23(4)(b).

[WP10] Monitor Third-Party Security

Control text: Keep an eye on key third-party providers’ security status, e.g. by reading their security advisories or reports, and ensure they promptly patch issues that could affect you. If a provider has a known breach or vulnerability, take appropriate action (apply mitigations, change credentials, etc.).

Why: Your vendors’ problems can quickly become your problems. Monitoring their security news (like a cloud provider announcing a serious bug) means you can react to supply-chain issues and protect your own system and data.

Evidence examples: Subscription to vendor security bulletins, record of checking cloud provider’s SOC 2 or ISO 27001 report annually, example incident where a supplier breach was addressed (ticket describing how you responded), vendor management policy section on security monitoring.

Legal anchors: NIS2 Art. 21(2)(d), CRA Art. 10(10), DGA Art. 12(5).

5.4. REACT & RECOVER



React fast when incidents strike, and recover to business-as-usual quickly.

No defense is perfect. This zone prepares the organization to respond to cybersecurity incidents effectively and fulfill its reporting obligations. EU laws like NIS2 and GDPR put strict timelines on breach notification (e.g. 24 hours for critical incidents under NIS2, 72 hours to notify data authorities under GDPR). Being caught flat-footed can lead to chaos and penalties. React & Recover controls ensure you have a plan, act quickly to contain damage, and keep stakeholders informed. Even a small team should know *who does what* if systems get hacked or data is leaked. This includes technical steps (isolate infected machines, restore backups) and communication steps (notify customers or authorities as required). Crucially, once the immediate crisis is handled, you need to get operations back on track, whether by restoring from backups or switching to manual workarounds. By planning and practicing incident response, an SME can turn a potentially devastating cyber incident into a manageable IT issue. Remember: speed, clarity, and communication are your allies in a crisis.

[RR1] Document Incident Response Plan

Control text: Write down a basic incident response plan that defines incident types/severity, roles (who leads response, technical vs. communication tasks), and step-by-step procedures for detection, containment, recovery, and required notifications. Make sure the team can access this plan even if systems are down.

Why: In a crisis, you don't want to figure everything out from scratch. An IR plan is a playbook that guides your team when adrenaline is high, it improves speed and coordination, which can greatly reduce damage.

Evidence examples: Incident response plan document (approved by management), incident flowchart or checklist, wallet card or printed copy distribution for critical staff, post-incident reports referencing use of the plan.

Legal anchors: NIS2 Art. 21(2)(b), GDPR Art. 33(5), NIS2 Art. 20(4).

[RR2] Detect and Escalate Incidents

Control text: Establish clear criteria for what constitutes an "incident" (e.g. system outage, malware detection, data leak) and ensure all staff know how to report signs of a potential incident immediately to the InfoSec Coordinator or response team. Set up an internal emergency contact method (e.g. a 24/7 number or chat) for rapid escalation.

Why: Quick reporting = quick response. If employees notice something weird (like a ransom note on screen or abnormal system behavior), they must alert IT security without delay. Clear definitions and communication channels speed up this critical first step in reacting.

Evidence examples: Incident classification matrix (with criteria for low/medium/high severity), internal communications or training snippet on “how to report an incident”, incident hotline or on-call rotation, an example of an incident ticket created by an employee report.

Legal anchors: NIS2 Art. 21(2)(b), NIS2 Art. 23(4)(a), GDPR Recital 87.

[RR3] Contain the Threat

Control text: When an incident is confirmed, act swiftly to contain it, for example, disconnect infected machines from the network, revoke compromised user credentials, block malicious IPs at the firewall, or switch off affected services to stop further damage. Document all containment actions taken.

Why: Limiting the blast radius is priority one. If attackers are in your system or malware is spreading, every minute counts. Quick containment can make the difference between a minor spill and a flood. It also demonstrates due diligence in case regulators review your response.

Evidence examples: Incident handling guide with containment steps, network access control rules or firewall changes made during an incident (timestamped), incident report log showing time from detection to containment, screenshots of admin consoles disabling accounts or systems during the event.

Legal anchors: NIS2 Art. 21(2)(b), NIS2 Art. 23(5), GDPR Art. 33(1).

[RR4] Eradicate and Recover

Control text: Eliminate the cause of the incident (e.g. remove malware, apply needed patches, close exposed ports) and restore systems and data to normal operation. Use clean backups or rebuild systems as necessary, and verify that systems are back to a safe state (test functionality and ensure no backdoors remain) before resuming business as usual.

Why: After stopping the immediate bleeding, you need to fix the wound and heal. If you don’t remove the threat (like cleaning out malware or plugging the security hole), you might get hit again. And if you can’t restore data or services properly, the incident’s impact drags on. Efficient recovery gets you back on your feet and making money.

Evidence examples: Incident post-mortem report detailing root cause removal (e.g. “applied patch X to vulnerable server”), cleanup scripts or AV logs confirming malware removal, system restore

logs from backups, testing sign-off document that systems passed checks post-recovery, user acceptance that services are back.

Legal anchors: NIS2 Art. 21(2)(b)&(c), GDPR Art. 32(1)(c), CRA Annex I(2).

[RR5] Notify Regulators

Control text: Report significant incidents to the relevant authorities within the required timeframes. For personal data breaches, notify your national data protection authority (DPA) within 72 hours (unless unlikely to pose risk). For NIS2 critical incidents (if you are in scope), notify the national CSIRT / competent authority within 24 hours for an early warning and a fuller report within 72 hours. Include in the report: what happened, what data or services are affected, and what you're doing about it.

Why: It's the law, GDPR and NIS2 have strict breach reporting rules, even for SMEs. Prompt notification can also get you help (like guidance from authorities) and shows transparency, which can reduce penalties. Not reporting, or reporting late, can result in heavy fines on top of the incident itself.

Evidence examples: Internal incident report timeline with notification timestamps, copy of breach notification sent to DPA and / or CSIRT with date, email receipts or web portal confirmation of submission, template form for breach notification, correspondence with regulators about the incident.

Legal anchors: GDPR Art. 33(1)&(3), NIS2 Art. 23(1), NIS2 Art. 23(4), CRA Art. 11(1).

[RR6] Inform Affected Users

Control text: Communicate with affected customers or users if their data or the service they use is impacted. Provide timely, plain-language notice of what happened, what risks or impact it may have on them, and what measures or precautions they should take. Do this without undue delay when required by law (for example, notify individuals of a personal data breach if it poses high risk to them).

Why: Your customers and users deserve to know if their information or the service they rely on has been compromised. Fast and honest communication helps them protect themselves (e.g. change passwords, be alert to scams) and helps rebuild trust. It's also legally mandated in serious data breaches.

Evidence examples: Draft or actual copies of customer breach notification letters / emails, public breach notification on website or press release, incident communication plan, list of affected individuals and confirmation of notification sent, customer support scripts related to the incident.

Legal anchors: GDPR Art. 34(1)&(2), NIS2 Art. 23(2), DSA Art 17.

[RR7] Coordinate with Authorities and Experts

Control text: Work with law enforcement or cyber incident response authorities as needed – for instance, if a crime is involved (like theft of data, ransomware), consider reporting to the police or engaging a CERT. Preserve any evidence (logs, malware samples, affected devices) that could aid investigation, without disrupting your recovery. If specialized help is needed, don't hesitate to call external incident response experts under a confidentiality agreement.

Why: Serious cyber incidents may be part of larger criminal campaigns; involving authorities can help catch the perpetrators and possibly assist your recovery (e.g. getting decryption keys). They can also provide guidance or resources in major cases. External experts can bring experience and tools you might lack. Preserving evidence is important for legal reasons and for learning what happened.

Evidence examples: Record of law enforcement notification (e.g. police report number) or correspondence, engagement contract or report from an incident response firm, forensic disk images or log archives set aside post-incident, chain-of-custody documentation for evidence, internal policy on when to involve outside authorities.

Legal anchors: NIS2 Recital 96, GDPR Recital 88, CSA Art. 9(4), Convention on Cybercrime Art. 12.

[RR8] Document Incident and Lessons

Control text: Keep an incident log / documentation throughout the response, noting timelines, decisions, actions taken, and their outcomes. After resolving the incident, perform a post-incident review to analyze root causes and lessons learned, and update your security measures and plans accordingly.

Why: Documentation creates a factual record (helpful if regulators or insurance ask) and ensures nothing critical is forgotten in the heat of response. The post-mortem analysis turns a painful incident into concrete improvements – so you don't get hit the same way twice. Learning from each incident is how your security posture gets stronger over time.

Evidence examples: Incident log book or digital timeline (timestamps of detection / containment / recovery, who did what), post-incident report or slide deck identifying root cause and areas for improvement, list of follow-up actions (with owners and deadlines) derived from incident review, updated policies or configurations that address the weaknesses revealed.

Legal anchors: GDPR Art. 33(5), NIS2 Art. 21(2)(f).

[RR9] Utilize Backup Workarounds

Control text: Implement manual or alternate procedures to continue critical operations during IT outages. For example, if your main system is down, you might switch to a read-only backup server, or use spreadsheets/paper for interim processing. Train staff on these contingency workflows as part of your recovery planning, and invoke them when needed to keep the business running.

Why: When systems fail, business shouldn't grind to a halt. Having *pre-thought* workarounds buys you time to properly fix issues without massive losses or customer harm. This is especially vital for small businesses that may not have redundant infrastructure – sometimes a bit of creativity and a Plan B (even if it's analog) can save the day.

Evidence examples: Business continuity plan section detailing alternative processes (e.g. "If ordering system offline, take orders via phone and record in template XYZ"), print-outs of critical forms or data needed for manual ops, evidence of a drill where staff performed tasks manually, communications to customers about use of a backup system (if applicable).

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

[RR10] Restore Confidence & Update Stakeholders

Control text: After recovery, update all relevant stakeholders, internally (management, employees) and externally (customers, partners), about the incident resolution and any pertinent follow-up. If services were degraded or taken offline, announce their restoration. Provide reassurance on what has been fixed and any new safeguards in place. Internally, also consider if the incident triggers any need to update contracts or service level agreements.

Why: Transparent communication shouldn't stop once the fire is out. Colleagues need to know things are back to normal, and customers will appreciate hearing that you've fully resolved the issue and strengthened security. This helps rebuild trust and sets the record straight (reducing rumors or misinformation). It also closes the loop, turning a negative event into a demonstration of your reliability and improvement.

Evidence examples: All-staff email or meeting notes summarizing incident and next steps, customer notification of service restoration or follow-up FAQs, press release or social media post about the incident being resolved, updated SLA or contract clauses if needed (with clients or providers) post-incident, feedback from clients or users after the resolution announcement.

Legal anchors: NIS2 Art. 23(2), DSA Art 11(3), GDPR Art 34(2).

5.5. LEARN & LIFT

Learn from every experience and lift your cybersecurity maturity continuously.



Cybersecurity is not a one-and-done effort – it’s an ongoing learning process. The final zone focuses on sustaining and improving security over time. For small organizations, this often means training people, reviewing what works and what doesn’t, and adjusting accordingly. Regulations like NIS2 explicitly require cybersecurity awareness and hygiene training, and a culture of continuous improvement underpins the “state of the art” principle in GDPR (Recital 83). Concretely, Learn & Lift includes regular staff training (keep security fresh in everyone’s mind), practice drills, management reviews, and perhaps seeking external certifications or audits to validate progress. The goal is to make security a habit and to steadily raise the bar – or “lift” your capabilities – as threats evolve and the company grows. Each incident or test should end with lessons learned; each year should end with security a bit stronger than before. By building this learning culture, even resource-strapped teams can achieve a high level of cyber resilience and compliance in the long run.

[LL1] Train and Test Staff

Control text: Provide all employees with cybersecurity awareness training at least annually (and during onboarding), covering phishing, safe password practices, data protection, and incident reporting. Periodically test their alertness, for example, run simulated phishing email exercises, to reinforce good habits and identify where more guidance is needed.

Why: Your people are your first line of defense, or weakness. Regular training turns them from potential targets into additional sensors and defenders. Testing (like phishing simulations) makes training real and engaging, and helps measure if the message is getting through. Users who are aware can prevent a breach (by not clicking that malicious link) or catch it early (by reporting odd activity).

Evidence examples: Training attendance records or certificates, training content slides or videos, results of last phishing simulation (e.g. % clicked, who needs follow-up training), staff quiz scores, policy acknowledgment signatures (affirming they understand security policies).

Legal anchors: NIS2 Art. 21(2)(g), GDPR Art. 39(1)(a).

[LL2] Conduct Incident Drills

Control text: Practice your incident response with drills at least once a year. This could be a tabletop exercise (simulated scenario run-through) with the incident team and management, or even a full live drill where a fake “incident” is injected to test detection and response. Use these exercises to verify everyone knows their role and to uncover gaps or confusion in the IR plan.

Why: Practice makes prepared. It's far better to stumble during a drill than during a real attack. Drills build muscle memory, so when a real incident happens, the team isn't doing everything for the first time. They also validate whether your documented plans actually work in practice. Regular exercises are expected as part of serious cyber programs and show regulators you take resilience seriously.

Evidence examples: Tabletop exercise agenda and scenario (e.g. "ransomware outbreak" playbook), list of participants and their roles in the drill, post-exercise report noting what went well/poorly and action items, revised incident response plan or procedures updated after the drill.

Legal anchors: NIS2 Art. 21(2)(b)&(f), GDPR Art. 32(1)(d), CSA Recital 13.

[LL3] Learn from Incidents

Control text: After any security incident or major near-miss, hold a retrospective to identify root causes and needed improvements. Update your security controls, policies, and procedures based on those lessons. Ensure that any weaknesses discovered (technical or human) are addressed – whether that means more training, a new tool, or a process change.

Why: Incidents are painful, but wasting them is worse. Each one is a free class in where your defenses or processes failed. By doing a structured post-mortem (the "lessons learned" meeting), you turn an incident into actionable next steps. This continuous improvement cycle is what regulators want to see under the principle of accountability. Over time, it significantly elevates your cyber maturity.

Evidence examples: Post-incident review report with root cause analysis, list of follow-up actions (patch applied, config changed, additional monitoring added, etc.) with deadlines and sign-offs, revised policies or checklists updated after an incident, meeting minutes of lessons-learned discussion.

Legal anchors: GDPR Art. 33(5), NIS2 Art. 21(2)(f)

[LL4] Update Policies and Plans

Control text: Review and update all security policies, procedures, and plans at least annually (and after major incidents or changes). This includes the information security policy, incident response plan, business continuity plan, etc. Ensure they remain aligned with current business reality, emerging threats, and any changes in EU law. Obtain management re-approval for any significant updates and communicate changes to staff.

Why: Stale policies gather dust. The threat landscape and your business environment can change a lot in a year, your documentation should not lag behind. Regular review keeps plans effective

and compliant with the latest requirements. It's also an opportunity to re-engage leadership and employees with the security program each year.

Evidence examples: Document control page showing last review date of each policy/plan, change log highlighting what was updated, meeting minutes from annual policy review with management, email to staff summarizing policy updates, compliance checklist verifying policies against new regulations.

Legal anchors: NIS2 Art. 20(4), GDPR Art 24(1), Cybersecurity Act Art. 56(8).

[LL5] Seek Independent Assurance

Control text: Periodically obtain independent review of your security – this could be through a security audit, certification, or expert assessment. Alternatively, hire an external auditor or participate in industry security programs to benchmark your practices. Address any findings from these assessments.

Why: An external eye can catch issues you overlook and provides credibility. Achieving a certification or passing an audit gives assurance to customers and regulators that you meet a recognized security standard. It's also a learning opportunity, auditors often suggest improvements. Over time, aiming for higher assurance levels (from basic to advanced) will drive your security maturity upward.

Evidence examples: Audit report from an external security assessment (and your remediation action plan), gap analysis report from a consultant, correspondence with a certification body, budget or management approval for pursuing certification.

Legal anchors: Cybersecurity Act Art. 54, NIS2 Recital 88, GDPR Art/. 42(1).

[LL6] Management Review & Improvement

Control text: At least once a year, top management (the Board or executives) shall review the overall cybersecurity program – including recent incidents, audit results, compliance status, and resource needs. They should evaluate the effectiveness of current controls and decide on any strategic changes or investments for improvement. This review should be documented, and resulting actions (e.g. approving budget for new tools, policy changes, extra training) should be tracked to completion.

Why: Leadership engagement is crucial for sustained security. An annual management review ensures cybersecurity gets high-level attention and remains aligned with business priorities. It reinforces accountability at the top per NIS2, and helps secure necessary support (funding, staffing) to lift the security posture. Simply put, what gets reviewed by leadership gets done.

Evidence examples: Annual security review presentation slides, meeting minutes with CEO / Board discussing cybersecurity, list of decisions or approvals (e.g. “approved hiring of IT security consultant” or “mandate multi-factor for all accounts by Q2”), security metrics dashboard presented (incidents count, training completion, audit scores), follow-up report on implementation of management directives.

Legal anchors: NIS2 Art. 20(1) & (6), GDPR Art. 5(2).

[LL7] Engage in Information Sharing

Control text: Participate in cybersecurity knowledge-sharing with peers and industry groups. For instance simply network with similar organizations to exchange anonymized lessons learned and threat information. Share incidents or near-misses in a trusted forum so others can learn, and take in others’ experiences to improve your own defenses.

Why: Cybersecurity is a team sport. Attackers often repeat tactics across many victims – by sharing information, SMEs can collectively strengthen and avoid being easy targets. Contributing to community knowledge (even informally) also keeps your team updated on threats and best practices. The EU encourages such voluntary information-sharing as a way to raise the overall level of cyber resilience.

Evidence examples: Membership in a cybersecurity association (welcome letter, meeting attendance), examples of threat intel received from peers (sanitized indicators or warnings that led you to act), contribution you made (presentation or post about a lesson learned from your incident at a forum), emails or portal screenshots from a sharing community (with actionable info you applied).

Legal anchors: NIS2 Art. 29(4), CSA Art. 7.

[LL8] Track Security Metrics

Control text: Define and track a set of cybersecurity performance metrics to gauge your progress over time. These could include patching times (e.g. % of critical patches applied within deadline), number of reported incidents, training completion rates, audit findings count, etc. Review these metrics periodically and use them to identify trends or areas needing attention. Adjust your security efforts based on what the data shows (e.g. if phishing click rates remain high, intensify training; if patch times slip, refine the process).

Why: “If you can’t measure it, you can’t improve it.” Simple metrics help translate fuzzy security efforts into tangible numbers that management can understand and that teams can strive to improve. Metrics focus your improvement initiatives and provide evidence of effectiveness (or

early warning of issues). They also support the accountability and continuous improvement cycle mandated by regulations.

Evidence examples: Security metrics dashboard or spreadsheet (with historical data and targets), periodic security report to management showing KPIs (Key Performance Indicators) like “Mean Time to Detect/Respond” or “# of high vulnerabilities open”, meeting minutes where metrics were discussed and actions decided (e.g. to bring a metric to target), improvement in a metric after an initiative (graph of training completion over 3 years).

Legal anchors: NIS2 Art. 21(2)(f), GDPR Art. 24(1).

[LL9] Plan for Growth and Changes

Control text: Anticipate and plan for changes that could impact security – such as rapid team growth, entering a new market, adopting new technology (cloud services, IoT, AI), or regulatory changes. Update your risk assessment and controls to scale with the business. For example, if expanding to the EU market triggers new obligations (like appointing an EU representative under DSA or increasing data volume under GDPR), integrate those into your security program. Ensure continuity of security during mergers, acquisitions, or major pivots by conducting due diligence and integrating systems carefully.

Why: Security that worked for 10 people might fail at 100. Early planning for growth or change prevents security from being an afterthought. It’s easier and safer to bake in requirements for new contexts than to bolt them on later. Being proactive about regulatory changes (like new laws or updates) keeps you ahead of compliance rather than scrambling. Ultimately, this forward-looking stance ensures your “security baseline” remains effective and compliant no matter how the company evolves.

Evidence examples: Security implications section in business expansion plans or project proposals, records of consultation with legal/IT on compliance when launching a new service in EU, updated threat model or risk register reflecting a new technology adoption, M&A security due diligence checklist and findings, roadmap of security initiatives aligned to company growth (e.g. plan to hire a dedicated security officer once 100 employees reached).

Legal anchors: NIS2 Recital 20, GDPR Art. 24(1), AI Act Art. 4, DGA Art. 11(8).