



ShieldNet

Document Title	ShieldNet Cybersecurity Standard – Annex A – Quick-Start Artefact Kit
Release Date	September 2025
Next Review	August 2026 (annual review cycle)
Distribution	Public – Creative Commons BY-NC-ND 4.0

1. What is the Quick-Start Kit?

The Quick-Start Artefact Kit is the practical, “ready-to-use” toolkit that brings the ShieldNet Core Standard to life. It contains a set of structured templates you can use to record the essential information needed to meet the 48 mandatory controls — and to prove your compliance with EU cybersecurity laws such as NIS2, GDPR, the Cyber Resilience Act, and the AI Act. The kit is designed for SMEs, NGOs, and startups that often lack large security teams or formal compliance systems. Each template can be maintained using simple tools like spreadsheets, shared folders, or your existing workflow platforms.

The kit is organized into two tiers of templates:

- **Core Templates (A-1 to A-6)** – These form the baseline records every ShieldNet member should maintain from day one. They cover the essentials: your assets and data, identified risks, supplier checks, incident logging, business continuity priorities, and staff security training. Together, they ensure you meet the core operational and legal requirements in the standard.
- **Extended Templates (A-7 to A-13)** – These add a deeper layer of governance, monitoring, and strategic oversight. They help you map your compliance obligations to the ShieldNet controls, track access rights and vulnerability management, review policies and plans, measure KPIs, manage AI-related risks, and document BC/DR testing. Extended Templates are ideal for organizations that are growing, operating in higher-risk environments, or aiming for a more advanced maturity level.

By keeping both sets of templates up to date, you create a clear, verifiable record of your security posture — one that satisfies regulators, reassures customers, and strengthens internal decision-making. You don’t need to complete every field from day one; start with what you know, and improve over time. The important thing is to treat these artefacts as living documents, updating them whenever systems, risks, or responsibilities change. Over time, the Quick-Start Kit becomes your organization’s single source of truth for cybersecurity compliance and readiness.

2. How to use the Kit

The Quick-Start Artefact Kit is most effective when treated as a living set of documents that evolves with your organization. You don't need to complete every template perfectly on day one — the goal is to start with what you know and improve over time. Begin with the Core Templates (A-1 to A-6), as these cover the minimum baseline evidence you'll need to meet the ShieldNet Core Standard and your core EU legal obligations. For many SMEs, NGOs, and startups, these six templates can be fully managed using spreadsheets or shared documents, and updated as part of routine work (e.g., when onboarding new staff, renewing vendor contracts, or responding to incidents).

Once your Core Templates are in place and consistently maintained, you can introduce the Extended Templates (A-7 to A-13) to strengthen governance and resilience. These templates allow you to link your controls directly to legal obligations, track technical security actions like vulnerability scanning, measure performance with KPIs, and document advanced activities like BC/DR testing or AI system compliance. Extended Templates are not just for large organizations — even a small team can use them to proactively manage risk, especially when operating in higher-risk sectors or aiming for advanced certification levels.

Best practice for maintaining the kit:

- *Assign ownership* – Make sure each template has a named person responsible for updates.
- *Set review intervals* – Core Templates should be reviewed quarterly or when significant changes occur; Extended Templates can be reviewed annually unless risk level demands more frequent updates.
- *Link to controls* – When updating a template, note which ShieldNet Core Standard controls it supports.
- *Keep it centralized* – Store the templates in a secure, shared location so relevant team members can access and contribute.
- *Show your work* – Keep older versions to demonstrate improvement over time; this is valuable for audits and compliance reviews.

By following this approach, the Quick-Start Kit becomes your single source of truth for cybersecurity compliance and operational resilience — simple enough for a small team to manage, but robust enough to stand up to regulatory scrutiny.

3. Core Templates

The Core Templates (A-1 to A-6) are the foundation of the Quick-Start Artefact Kit. They give every ShieldNet member — whether an SME, NGO, or startup — the essential records needed to put the ShieldNet Core Standard into practice from day one. Each template captures key operational information that supports multiple controls in the standard and provides clear evidence of compliance with EU cybersecurity laws such as NIS2, GDPR, and the Cyber Resilience Act.

These templates are intentionally lightweight and easy to maintain, even for organizations with limited or no dedicated cybersecurity staff. You can complete them using simple tools like spreadsheets or shared documents, and keep them updated as part of your normal business processes. By maintaining these six artefacts, you create a living picture of your assets, risks, suppliers, incidents, continuity plans, and staff awareness — the baseline elements every organization needs to stay secure, meet its legal duties, and build trust with customers and partners.

A-1: Asset & Data Inventory Template

This template is your master list of the systems, devices, and data your organization relies on. It should be kept current at all times — update it when you add, remove, or repurpose assets. The goal is to know what you have, who is responsible for it, and how sensitive the data it contains is. This record is essential for both risk management and compliance with EU laws that require awareness of your processing environment (e.g., GDPR Art. 30, NIS2 Art. 21).

Column-by-column guidance:

- **Asset / System** – Name or short description of the asset. Include servers, laptops, cloud services, applications, or critical physical systems.
- **Owner** – The person in your organization responsible for the asset’s security and upkeep. Avoid leaving this blank; every asset needs a clear owner.
- **Purpose / Function** – State why the asset exists or what it does (e.g., “process payroll,” “host customer portal”).
- **Data Stored (and Sensitivity)** – Describe the type of data handled (personal, financial, confidential business data) and assign a sensitivity level (High, Medium, Low) based on potential harm if compromised.
- **Criticality (High/Med/Low)** – Based on how essential the asset is to operations, not just the sensitivity of data. A public website may hold low-sensitivity data but still be Medium criticality for reputation.

ShieldNet Cybersecurity Standard – Annex A

- Location – Physical or cloud location where the asset resides. For cloud, include region (e.g., “Cloud host – EU West”).

Asset / System	Owner	Purpose / Function	Data Stored (and Sensitivity)	Criticality (High/Med/Low)	Location
HR Payroll Server	IT Manager	Employee payroll processing	Personal data (salaries, SSNs) – High sensitivity	High – critical for paying staff	On-prem datacenter
Company Website	Webmaster	Public web presence	Public content only – Low sensitivity	Medium (brand/reputation)	Cloud host (EU region)
Laptop #23 (John Doe)	John Doe (Staff)	Workstation (remote work)	Client project files – Med sensitivity	Low (individual device)	Employee home (UK)
... (add all assets)					

Best practices:

- Review and update this list at least quarterly or when major changes occur.
- Use your Criticality column in combination with the Data Sensitivity to prioritize protection measures.
- Keep older versions archived to show historical changes — this is useful for audits and incident investigations.
- Link this inventory to other templates (e.g., Access Matrix, Patch Ledger) so you have a connected picture of security controls for each asset.

A-2: Risk Assessment Matrix (Abridged Example)

This template helps you record and prioritize the cybersecurity risks your organization faces. It combines a clear description of each risk with a likelihood × impact score to rank which risks need the most attention. EU laws like NIS2 (Art. 21) and the Cyber Resilience Act require proportionate risk management, and this artefact is your evidence that risks are being identified, assessed, and addressed.

Column-by-column guidance:

- Risk ID – Assign a unique code for easy tracking (e.g., R-1, R-2). Keep it short but consistent across related documents.
- Risk Description – Clearly describe the risk scenario, including cause and consequence (e.g., “Ransomware attack paralyzes file server – data unavailable”).
- Likelihood (1–5) – Rate the probability of the risk occurring: 1 = Rare, 5 = Almost Certain.
- Impact (1–5) – Rate the potential severity if the risk occurs: 1 = Negligible, 5 = Severe
- Risk Level (L × I) – Multiply Likelihood by Impact to produce a score (max 25). This makes it easy to sort risks by criticality.
- Mitigations (Controls in place) – List what you already do to reduce the risk, referencing specific ShieldNet control IDs where possible (e.g., “[KP6] Backups nightly”).
- Owner – Person responsible for monitoring and addressing the risk.
- Status – Current progress or next steps (e.g., “Further action: test restores by Q4”).

Risk ID	Risk Description	Likelihood (1-5)	Impact (1-5)	Risk Level (LxI)	Mitigations (Controls in place)	Owner	Status
R-1	Ransomware attack paralyzes file server – data unavailable, potential loss if backups fail.	3 (Possible)	5 (Severe)	15 (High)	- [KP6] Backups nightly (offsite) - [SB4] AV on server & [WP3] prompt patching - [RR9] Manual process defined for critical ops	IT Coord.	<i>Further action:</i> test restores ([WP9]) by Q4
R-2	Phishing email tricks employee, leads to account takeover and data breach of client info.	4 (Likely)	4 (Major)	16 (High)	- [SB3] MFA on email accounts - [LL1] Security awareness & phishing tests - [SB1] Least privilege limits data access	IT Coord.	<i>Further action:</i> deploy anti-phishing email filter by Q3

ShieldNet Cybersecurity Standard – Annex A

R-3	Third-party cloud outage (hosting provider down) causes website downtime.	2 (Unlikely)	3 (Moderate)	6 (Medium)	- [KP7] SLA with provider (99.9% uptime) - [RR9] Backup static page on alternate host if down -	Webmaster	Acceptable (monitor SLA)
-----	---	--------------	-----------------	---------------	---	-----------	-----------------------------

Best practices:

- Review the matrix at least twice a year, or after major changes in systems, processes, or threat landscape.
- Update likelihood/impact scores if new controls reduce the risk or if threat trends change.
- Use the Risk Level to focus resources where they matter most – high scores should be addressed first.
- Reference mitigations using the control IDs from the ShieldNet Core Standard so you can show exactly how each risk is managed.
- Keep a copy of older versions to demonstrate how your risk posture evolves over time.

A-3: Vendor & Service Security Checklist (Third-Party Assessment)

This template helps you track and verify the security posture of the third-party providers and services your organization relies on. Under NIS2 (Art. 21), GDPR (Art. 28), and other EU regulations, you’re responsible for ensuring that suppliers handling your data or systems meet security and compliance requirements. The checklist gives you a structured way to record those checks and set review intervals.

Column-by-column guidance:

- **Third-Party Service (Provider)** – The name of the vendor or service, plus any brand or platform names (e.g., “Cloud Hosting – ExampleCorp Cloud”).
- **Data/Systems Accessed** – Briefly state what the vendor has access to (e.g., “Hosts public website; access to non-personal app data”).
- **Criticality** – Rate as High, Medium, or Low depending on the importance of the service to operations or the sensitivity of data handled.
- **Security Measures Verified** – List the security controls or measures you’ve confirmed are in place. Be specific and include contractual protections, certifications, and technical safeguards (e.g., “GDPR terms in contract, ISO 27001 certified datacenter, MFA for admin console”).
- **Compliance/Certifications** – Summarize relevant standards or legal compliance proof the vendor holds (e.g., ISO 27001, SOC 2, CSA STAR).
- **Review Date** – When you last reviewed or validated the vendor’s security posture.
- **Next Review** – When you plan to check again (typically yearly for high-criticality vendors, every 2 years for low-criticality).

Third-Party Service (Provider)	Data / Systems Accessed	Criticality	Security Measures Verified	Compliance / Certifications	Review Date	Next Review
Cloud Hosting (ExampleCorp Cloud)	Hosts public website; access to web app data (non-personal).	High	☒ Contract includes GDPR terms ☒ ISO 27001 certified datacenter ☒ MFA enabled for admin console	ISO 27001, SOC 2	Jan 2025	Jan 2026
Payroll Processor (PayrollCo)	Receives personal & salary data for payroll.	High	☒ DPA signed (GDPR Art 28) ☐ No recent pen test report provided (requested) ☒ Uses encryption for data transfer	GDPR-compliant (DPA), claims ISO 27001	Mar 2025	Sep 2025 (mid-year audit)

ShieldNet Cybersecurity Standard – Annex A

VPN Service (SecureVPN Ltd)	Provides employee VPN – access to internal network.	Medium	✔ No-logging policy verified ✔ MFA supported for VPN login ✔ Servers based in EU only	None (self-attested security)	Jul 2025	Jul 2026
-----------------------------	---	--------	---	-------------------------------	----------	----------

Best practices:

- Always keep proof of verification (e.g., certification documents, signed contract clauses, vendor security questionnaire responses).
- Prioritize annual reviews for High-criticality vendors, especially those storing or processing personal data.
- Flag and follow up on any gaps in the vendor’s security controls; set clear deadlines for remediation.
- Use this checklist as part of onboarding new suppliers and when renewing contracts.
- Keep historic records to show consistent supplier due diligence over time.

A-4: Incident Response Log and Report Template

This template provides a structured way to record every security incident, from detection to resolution. Keeping accurate, timely records is critical for EU regulatory compliance — for example, GDPR (Art. 33) requires breach notification within 72 hours if personal data is involved, and NIS2 (Art. 23) requires prompt incident reporting to competent authorities. Even incidents that don't meet reporting thresholds should be logged for trend analysis and lessons learned.

Column-by-column guidance:

- Incident ID – Assign a unique identifier for tracking (e.g., INC-2025-001). Use a consistent numbering format for easy reference.
- Date/Time Detected – The exact date and time the incident was first observed or reported.
- Reporter – Name and role of the person who first raised the alert, whether staff, contractor, or external contact.
- Description of Incident – A concise summary of what happened, including any visible impact or suspicious behavior (e.g., “Ransomware detected on laptop; ‘files encrypted’ note found”).
- Impacted Systems/Data – List the systems, devices, or datasets potentially affected. Include whether personal, financial, or sensitive business data was involved.
- Severity Level (Low/Med/High) – Rate based on the potential business, legal, and reputational impact. A ransomware attack on a key device would generally be High; a blocked phishing email might be Low.

Incident ID	Date/Time Detected	Reporter	Description of Incident	Impacted Systems/Data	Severity Level (Low / Med / High)
INC-2025-001	2025-03-10 09:14	Jane Smith (Sales)	Ransomware detected on laptop; “files encrypted” note found.	Laptop #45 (JS); potential access to shared drive (X).	High
INC-2025-002	2025-07-22 16:30	System Alert (IDS)	Unusual outbound traffic from DB server (possible data exfiltration).	Database Server 3; customer data potentially.	High

Actions Taken:

- INC-2025-001:
 - Containment: Laptop removed from network within 15 min, user account disabled.
 - Eradication: IT re-imaged laptop, ran AV scan on shared drive (no infection spread).
 - Recovery: Restored latest files from backup to laptop, user back working by 2025-03-12.
 - Notifications: No external notification required (no data breach); internal team informed.

- INC-2025-002:
 - Containment: Blocked server's outbound traffic at firewall; isolated DB server from network.
 - Investigation: Found malicious process dumping data – killed process.
 - Eradication: Applied security patch to DB server OS (was missing update); changed DB admin credentials.
 - Recovery: Server back online 2025-07-24.
 - Notifications: Reported to DPA within 72h (potential personal data involved); customers notified due to possible data access.

Lessons Learned / Follow-Up:

- INC-2025-001: Need better email filtering – phishing email was root cause. Action: implement advanced spam filter by Q2 ([WP5]). Users praised for quick report.
- INC-2025-002: Patch management gap identified. Action: enforce critical patch deployment within 7 days ([WP3]); also implement database activity monitoring.

Best practices:

- Record incidents as soon as possible — don't wait until resolution.
- Keep the description factual; save root cause analysis and recommendations for the post-incident review phase.
- Assign severity using your organization's agreed criteria (ideally linked to your criticality levels in the standard).
- Cross-reference this log with the A-5 BCP/DR Test Log if the incident triggered contingency plans.
- Store incident records securely, with access restricted to those handling the response and compliance reporting.

A-5: Business Continuity Plan (BCP) Summary – “Recovery Priority & RTOs”

This template summarizes your organization’s recovery priorities and time targets if a major disruption occurs. It focuses on Recovery Priority (what gets restored first) and Recovery Time Objectives (RTOs) — the maximum time you can tolerate a service or process being down before serious harm. This document is central to NIS2 (Art. 21), the Cyber Resilience Act, and general EU resilience principles, showing that you have planned for business continuity in a proportionate way.

Column-by-column guidance:

- **Process or System** – Identify the business process or IT system being tested (e.g., “Payroll processing system,” “Customer order database”).
- **Priority Level** – Rate as High, Medium, or Low based on operational and compliance impact. High-priority items are those that must be restored first to avoid serious damage.
- **Acceptable Downtime (RTO)** – The Recovery Time Objective — the maximum acceptable outage before significant impact occurs (e.g., “4 hours,” “2 days”).
- **Backup Exists?** – Indicate Yes/No and whether backups are local, cloud, or offsite.
- **Restoration Procedure Summary** – Short description of how the system or process would be restored, including any manual workarounds if systems are unavailable.
- **Owner (for recovery)** – The person responsible for leading the restoration of the process/system during an actual incident.

Process or System	Priority Level	Acceptable Downtime (RTO)	Backup Exists?	Restoration Procedure Summary	Owner (for recovery)
Online E-commerce Platform	1 (Critical)	4 hours	Yes (hourly DB backup, redundant server)	See DR Plan Section 3: failover to backup server in EU region; DNS redirect within 1 hr.	CTO / DevOps Lead
Internal Email	2 (High)	24 hours	Yes (cloud service with geo-redundancy)	Cloud provider auto-failover; IT to verify switch.	IT Coordinator

Best practices:

- Update after significant changes in systems, processes, or staffing.
- Ensure High-priority processes have the shortest RTOs and tested restoration methods.

ShieldNet Cybersecurity Standard – Annex A

- Keep this summary short, clear, and accessible — it's a quick reference during a crisis, not a full plan.
- Link to detailed recovery procedures stored in your BCP or DR documentation.
- Review at least annually, and whenever your business or IT environment changes significantly.

A-6: Security Training & Awareness Tracker

This template is your record of staff cybersecurity awareness and skills development — essential for compliance with NIS2 (Art. 20), GDPR (Art. 39), and best practices under the Cyber Resilience Act. It helps you monitor who has been trained, what topics were covered, and when refresher sessions are due. Keeping this tracker up to date demonstrates that your organization actively invests in security awareness, a key factor in reducing human error–related incidents.

Column-by-column guidance:

- **Employee Name** – Full name of the staff member or contractor who received the training.
- **Role** – Their primary job function (e.g., “Developer,” “Finance Officer”). This helps tailor training to relevant risks.
- **Last Training Date** – The most recent date the employee completed a cybersecurity-related training session.
- **Training Topics Covered** – A brief list of the topics included (e.g., “Secure coding, Data protection, Phishing awareness”).
- **Phishing Test Click Rate** – The percentage of simulated phishing emails clicked during recent tests (lower is better). Include date of the last test for context.
- **Next Training Due** – When the employee should receive their next training (commonly annual for all staff; more frequent for high-risk roles).

Employee Name	Role	Last Training Date	Training Topics Covered	Phishing Test Click Rate	Next Training Due
John Doe	Developer	2025-01-15	Secure coding, Data protection, Phishing awareness	0% (did not click bait in Mar 2025 test)	Jan 2026
Jane Smith	Sales Manager	2024-12-10	Password hygiene, Mobile device security, Phishing	20% (1 out of 5 test emails clicked)	Sep 2025 (refresh early due to click)

Best practices:

- Run phishing simulations at least twice a year and record results here.
- Adjust training topics based on emerging threats, regulatory changes, or incident trends in your organization.
- Prioritize refresher training for staff with higher click rates or in sensitive roles.
- Store related training materials, attendance records, and test reports with this tracker for full audit readiness.

- Use this tracker as evidence in supplier or customer security reviews to demonstrate a proactive culture of security.

4. Extended Templates

The Extended Templates (A-7 to A-13) build on the Core Templates by adding more advanced records that strengthen governance, legal compliance, and operational resilience. While the Core Templates focus on the essential day-to-day artefacts every ShieldNet member should maintain, the Extended Templates help you go deeper — linking your security program directly to EU law requirements, tracking higher-level performance metrics, and preparing for complex scenarios like AI compliance or disaster recovery testing.

These templates are especially valuable for organizations that are growing in size, expanding their digital footprint, or operating in higher-risk sectors. They provide structured evidence for regulators, auditors, and business partners, demonstrating that your organization is not only meeting baseline obligations but is also proactively managing security maturity. Each Extended Template is still designed to be practical for SMEs, NGOs, and startups — no unnecessary complexity, just the extra governance and visibility you need when scaling.

A-7: Legal & Compliance Mapping Table

This template links each relevant EU law or regulation to the specific ShieldNet Core Standard controls and your internal policies or procedures. It helps you meet [KP2] “Map Legal Requirements” and supports Annex B cross-referencing. This table is your quick reference for understanding why a control exists and which legal obligation it fulfills. It also helps you stay prepared for audits or regulatory inquiries by showing the connection between external requirements and internal action.

Column-by-column guidance:

- Regulation / Article – State the full name of the regulation and specific article or recital number (e.g., “GDPR – Art. 32(1)(b)”).
- Obligation Summary – Describe the requirement in plain language (e.g., “Implement measures to ensure ongoing confidentiality, integrity, availability of processing systems”).
- Relevant Controls – List the ShieldNet Core Standard control IDs that address this requirement.
- Internal Policy/Procedure Reference – Point to the internal document or SOP that implements the control.
- Last Review Date – When you last checked this mapping for accuracy (review annually or after legal updates).

ShieldNet Cybersecurity Standard – Annex A

Regulation / Article	Obligation Summary	Relevant Controls	Internal Policy / Procedure Reference	Last Review Date
GDPR – Art. 32(1)(b)	Protect data processing systems' availability, confidentiality, and integrity	KP-4, SB-2, WP-3	Information Security Policy v2.1, Backup SOP v3	2025-06-15
NIS2 – Art. 21(2)(c)	Identify and manage network and information system security risks	KP-1, KP-2, KP-5	Risk Management Procedure v1.4	2025-06-15
CRA – Art. 10	Ensure security of products with digital elements through secure development	SB-4, SB-5	Secure Development Guidelines v1.0	2025-06-15
AI Act – Art. 9	Perform risk management for high-risk AI systems	KP-10, LL-7	AI Risk Assessment Procedure v1.0	2025-06-15

Best Practices

- Keep it updated whenever EU laws are amended or new regulations enter into force.
- Use official references for articles and recitals to avoid confusion in audits.
- Cross-link this table with Annex B so both sections reinforce each other.
- Assign ownership — usually the Info-Sec Coordinator or Compliance Officer — for maintaining this mapping.
- Review annually or sooner if new products, services, or markets bring in additional regulatory scope.

A-8: Access Rights Review Log

This template records periodic reviews of user accounts and system access rights. It helps ensure that only authorized people have access to systems and data, and that privileges match current job roles. It supports controls [WP8] “Review User Access” and [SB1] “Limit Access by Role” in the ShieldNet Core Standard, as well as EU requirements for access control under NIS2 and GDPR. Maintaining this log provides clear evidence for regulators, auditors, and customers that you regularly check and correct access permissions.

Column-by-column guidance:

- **Review Date** – The date the access review took place.
- **System/Asset** – Name of the system, application, or data repository reviewed (e.g., “HR Payroll Server”).
- **Reviewer** – Person who performed the review, ideally the system owner or Info-Sec Coordinator.
- **Accounts Reviewed (#)** – Number of accounts or users reviewed during the session.
- **Changes Made** – Summary of any actions taken (e.g., “Removed 2 inactive accounts; downgraded 1 admin to user role”).
- **Next Review Date** – Planned date for the next review based on risk or criticality (e.g., quarterly for high-risk systems).

Review Date	System/Asset	Reviewer	Accounts Reviewed (#)	Changes Made	Next Review Date
2025-06-30	HR Payroll Server	IT Manager	12	Removed 1 inactive account, enforced MFA for admins	2025-09-30
2025-06-30	CRM Cloud Platform	Sales Director	25	Revoked contractor account, corrected 2 role levels	2025-12-31

Best Practices

- Review high-criticality systems at least quarterly; low-criticality ones annually.
- Always document changes, even if they are “no changes” — this still counts as evidence of review.
- Coordinate with HR and onboarding/offboarding processes to ensure leavers’ access is revoked promptly.
- Cross-reference with your Asset & Data Inventory (A-1) to ensure all systems are covered.
- Store logs in a secure location and restrict access to authorized staff only.

A-9 – Vulnerability Scan & Remediation Log

This template tracks the results of vulnerability scans and the follow-up remediation actions. It supports [WP4] “Run Vulnerability Scans” and [WP3] “Apply Patches Promptly” in the ShieldNet Core Standard, and helps demonstrate compliance with NIS2 and the Cyber Resilience Act requirements for identifying and mitigating security flaws. Keeping this log up to date shows that your organization is actively finding and fixing weaknesses before attackers can exploit them.

Column-by-column guidance:

- Scan Date – When the scan was run.
- System/Scope – The system(s), applications, or network segment included in the scan.
- Tool Used – Name of the vulnerability scanning tool or service (e.g., “OpenVAS,” “Qualys”).
- High/Medium/Low Findings – Number of vulnerabilities found in each severity category.
- Actions Taken – Summary of remediation steps (e.g., “Patched Apache to v2.4.57, disabled unused ports”).
- Completion Date – Date all remediation actions for that scan were completed.

Scan Date	System/Scope	Tool Used	High Findings	Medium Findings	Low Findings	Actions Taken	Completion Date
2025-06-10	Web application & DB host	OpenVAS	2	5	3	Patched DB to latest version; fixed XSS vulnerability	2025-06-15
2025-06-10	Internal file server	Nessus	0	2	4	Disabled SMBv1; applied security update KB5028168	2025-06-12

Best Practices

- Run vulnerability scans at least quarterly and after major system changes.
- Remediate high-severity issues immediately, ideally within days, and medium-severity within weeks.
- Keep evidence of remediation, such as patch reports, change tickets, or admin console screenshots.
- Use the same severity scoring system consistently (e.g., CVSS) for better tracking over time.
- Cross-reference with the Patch Ledger (if you maintain one) to align vulnerabilities with patching actions.

A-10 – Policy & Plan Review Register

This template helps you track the scheduled review of your organization’s key cybersecurity policies and plans. It supports [LL4] “Review Security Policies & Plans” in the ShieldNet Core Standard, and ensures compliance with EU requirements for maintaining up-to-date security documentation under NIS2 and GDPR. Having this register means you can easily prove that your policies are not just written once but are regularly reviewed, updated, and approved by the right people.

Column-by-column guidance:

- Document Name – Title of the policy or plan (e.g., “Information Security Policy,” “Incident Response Plan”).
- Owner – The person responsible for maintaining and updating the document.
- Last Review Date – The most recent date the document was reviewed.
- Changes Made – Short summary of updates since the last version (e.g., “Added AI system section, updated contact list”).
- Approved By – Name/role of the person or authority that approved the updated version.
- Next Review – Planned date for the next review based on organizational policy (commonly annual).

Document Name	Owner	Last Review Date	Changes Made	Approved By	Next Review
Information Security Policy	Info-Sec Coordinator	2025-05-15	Updated password policy, added MFA section	Board Chair	2026-05-15
Incident Response Plan	IT Manager	2025-06-01	Added ransomware playbook, updated contacts	COO	2026-06-01

Best Practices

- Review core security policies at least annually, or sooner after major incidents, regulation changes, or system overhauls.
- Keep all historic versions for legal and audit purposes.
- Link policy updates to lessons learned from incidents (from A-4 Incident Response Log).
- Store policies in a secure, version-controlled location.
- Assign clear approval authority — unapproved updates can create compliance gaps.

A-11 – Security Metrics Dashboard

This template captures key performance indicators (KPIs) and metrics that measure the effectiveness of your security program. It supports [LL8] “Track Security KPIs” in the ShieldNet Core Standard and provides tangible proof for management, regulators, and partners that you are actively monitoring and improving your cybersecurity posture. Metrics can cover technical measures (e.g., patching speed), human factors (e.g., phishing test results), and operational resilience (e.g., incident response times).

Column-by-column guidance:

- **Metric Name** – The specific measurement being tracked (e.g., “Critical patch compliance rate”).
- **Target** – The desired goal or benchmark for that metric (e.g., “95% patched within 14 days”).
- **Current Value** – The latest measured performance.
- **Trend** – Indicator of whether performance is improving, stable, or declining (e.g., “↑ Improving,” “↓ Declining”).
- **Notes/Actions** – Any relevant context or next steps (e.g., “Increase training to improve phishing test scores”).

Metric Name	Target	Current Value	Trend	Notes/Actions
Critical patch compliance rate	95% within 14 days	88%	↑ Improving	Patch backlog reduced after resource allocation
Phishing test click rate	< 5%	7%	↓ Declining	Schedule refresher phishing awareness training
Mean time to detect incidents	< 4 hours	3 hours	→ Stable	Maintain current monitoring practices

Best Practices

- Select metrics that align with your business goals and regulatory requirements.
- Track a mix of leading and lagging indicators — not just past performance, but also predictive measures.
- Review metrics with management quarterly to support decision-making.
- Use visualization tools for clarity, but keep raw data for audit purposes.
- Adjust targets annually based on maturity and evolving threats.

A-12 – AI System Risk & Compliance Register

This template is for organizations that develop, deploy, or operate AI systems falling under the EU Artificial Intelligence Act (AI Act). It supports [KP10] “Assess AI Risks” in the ShieldNet Core Standard and helps ensure that high-risk or regulated AI systems meet the Act’s requirements for risk management, transparency, and compliance. Even if your AI systems are not currently classified as high-risk, maintaining this register demonstrates proactive governance and readiness.

Column-by-column guidance:

- **AI System Name** – The name or identifier of the AI system (e.g., “Fraud Detection Model v3”).
- **Risk Category (per AI Act)** – Classification such as “High-Risk,” “Limited Risk,” “Minimal Risk,” based on the AI Act definitions.
- **Purpose** – Brief description of the system’s intended use.
- **Data Source** – Summary of the main datasets used for training or operation (e.g., “Customer transaction data,” “Open-source image datasets”).
- **Risk Assessment Date** – Date the AI risk assessment was last performed.
- **Controls Implemented** – Key technical, organizational, or procedural measures in place to comply with the AI Act (e.g., “Bias testing quarterly, human oversight in decision-making”).
- **Next Review** – Scheduled date for the next AI risk and compliance review.

AI System Name	Risk Category	Purpose	Data Source	Risk Assessment Date	Controls Implemented	Next Review
Fraud Detection Model v3	High-Risk	Identify fraudulent payments	Customer transaction data	2025-05-10	Bias testing quarterly; human verification step	2025-11-10
Chatbot Support Assistant	Limited Risk	Automate FAQs and support	Public FAQ database, chat logs	2025-04-20	Regular content review; opt-out option for users	2026-04-20

Best Practices

- Classify AI systems accurately according to the AI Act’s categories.
- Document data provenance and any preprocessing steps for transparency.
- Conduct bias, robustness, and security testing regularly for high-risk AI.
- Link this register to your Risk Assessment Matrix (A-2) for integrated risk management.

- Review classifications at least annually or after major system updates.

A-13 – BC/DR Test Log

This template records the execution and results of Business Continuity (BC) and Disaster Recovery (DR) tests. It demonstrates that your organization not only has plans in place but actively validates them — a requirement under NIS2, the Cyber Resilience Act, and best practices for operational resilience. It complements the A-5 – BCP Summary by showing how well your recovery priorities and RTOs perform in real-life or simulated scenarios.

Column-by-column guidance:

- Test Date – When the BC/DR test was carried out.
- Process/System Tested – The specific process or system under test (e.g., “Payroll system failover,” “Cloud database restore”).
- Scenario Used – Type of disruption simulated (e.g., “Ransomware attack,” “Data center outage”).
- Actual Recovery Time – Time taken to restore operations during the test.
- Target RTO – The maximum acceptable downtime from your A-5 – BCP Summary.
- Issues Found – Problems encountered during the test (e.g., “Backup not syncing,” “VPN access failed for remote team”).
- Actions Taken – Corrective actions implemented to resolve the issues and improve recovery capability.
- Next Scheduled Test – Planned date for the next test, ideally based on system criticality.

Test Date	Process/System Tested	Scenario Used	Actual Recovery Time	Target RTO	Issues Found	Actions Taken	Next Scheduled Test
2025-05-15	Payroll System	Ransomware attack	6 hours	4 hours	Backup sync lag	Implement hourly backup sync	2025-11-15
2025-05-20	CRM Cloud Database	Data center outage	3 hours	6 hours	VPN connection delays for remote	Added secondary VPN endpoint	2026-05-20

Best Practices

- Test high-priority systems at least annually; consider semi-annual tests for mission-critical processes.
- Use a mix of tabletop exercises and full operational tests to validate both planning and execution.
- Document all issues and assign follow-up actions with deadlines.
- Cross-reference test outcomes with Policy & Plan Review Register (A-10) to trigger plan updates.
- Involve multiple teams to test cross-departmental coordination during disruptions.