



ShieldNet

Document Title	ShieldNet Cybersecurity Management System
Release Date	March 2026
Next Review	February 2027 (annual review cycle)
Distribution	Public – Creative Commons BY-NC-ND 4.0

1. Why this Management System Exists

This document defines how an SME governs and manages cybersecurity using the ShieldNet Core Standard as its foundation and OKRs as its operating model. It explains not only what to do, but how to plan, measure, evidence, and improve security in a simple and structured way.

Most SMEs do not have a dedicated security team, yet they face regulatory, contractual, and operational risks. Without structure, security becomes reactive and inconsistent. This system provides a lightweight but disciplined governance model that allows SMEs to demonstrate control, accountability, and readiness for certification without excessive bureaucracy.

This is a Cybersecurity Management System aligned to the ShieldNet Cybersecurity Core Standard and its annexes. It translates ShieldNet controls into measurable Objectives and Key Results, and connects them directly to evidence stored using Annex A artefacts. The system ensures that security is not a one-time checklist exercise, but a continuous cycle of planning, execution, review, and improvement supported by documented proof.

2. How we have built the Management System

This system mirrors the structure and naming logic of the ShieldNet Core Standard. It uses the same roles, Action Zones, and artefact references, and it does not rewrite controls but activates them through OKRs.

2.1. How OKRs translate ShieldNet into action

Objectives describe what the organization wants to improve within a given Action Zone. Key Results define how success will be measured using control tags such as [KP1] or [SB3] and evidence from Annex A.

Each Objective must:

- Belong to one Action Zone
- Reference relevant control tags in brackets
- Be supported by measurable Key Results
- Produce evidence aligned to Annex A

No more than 10 Objectives per year are allowed across all Action Zones. This limit forces prioritization and keeps the system manageable.

2.2. How cross referencing works, controls and evidence tags

The system uses three reference mechanisms:

- Control tags, for example [KP1], [SB3], [WP2]
- Evidence tags, for example Annex A A.1, Annex A A.2
- Action Zone tags, using official ShieldNet Action Zone names

Example format inside an Objective:

- Objective: Strengthen identity and access governance in SHIELD and BUILD
- Controls: [SB1], [SB3]
- Evidence: Annex A A.2 Asset Register, Annex A A.4 Access Review Log

This method ensures traceability from strategic intent to operational control and stored evidence

2.3. Risk driven prioritization

Cybersecurity improvements in this management system are driven by risk. The organization prioritizes its Objectives based on the most significant risks to its systems, services, and regulatory obligations. Risk information is maintained in the Risk Register using Annex A artefacts. High risk items normally translate into Objectives within the relevant Action Zone, ensuring that the OKR system focuses effort where it has the greatest impact.

This approach ensures that the Cybersecurity Management System remains proportionate for SMEs while still aligning with the risk based requirements found in EU cybersecurity and data protection laws.

3. Who This Management System Is For and How to Read It

This section clarifies scope and expectations so that SMEs can apply the system proportionately and correctly.

3.1. Scope and applicability for SMEs

This system is designed for SMEs, startups, NGOs, and small regulated entities that operate without a large IT department. It applies to the defined organizational scope, including people, systems, data, and third party providers.

3.2. What is included and excluded

Included are governance, risk management, operational security controls, monitoring, incident handling, and improvement. The system covers digital systems and supporting processes that affect confidentiality, integrity, and availability.

Excluded are unrelated business risks such as purely financial or marketing risks, unless they directly affect cybersecurity posture.

4. Who Does What in Cybersecurity

Clear ownership is the main success factor for a lightweight system. This section assigns accountabilities so OKRs do not become nobody's job. You must appoint owners who can act, not only observe. This aligns to the Core Standard expectation to assign security responsibility and define authority.

Role	Key Accountabilities
<i>Board</i>	- The Board holds ultimate accountability for cybersecurity. It approves annual Objectives, reviews quarterly results, and ensures sufficient resources are allocated. - The Board does not manage technical details, but it makes risk acceptance decisions and signs off on major corrective actions.
<i>Info-Sec Coordinator</i>	- The Info Sec Coordinator is responsible for coordinating the Cybersecurity Management System. This role maintains the OKR register, tracks evidence, and prepares management review materials. - The Info Sec Coordinator ensures that controls referenced in Objectives are implemented and evidenced, but does not replace operational owners.
<i>System Owner</i>	- Each critical system has a System Owner responsible for implementing relevant controls such as [SB2] or [WP1]. System Owners provide evidence such as screenshots, logs, and configuration exports. - They participate in monthly check ins and report on Key Results affecting their systems.
<i>All Staff</i>	- All Staff must follow security policies and participate in training aligned to controls such as [LL1]. They are responsible for reporting incidents and suspicious activity. - Security is a shared responsibility and is reinforced through Objectives in LEARN and LIFT.
<i>Third-Party Provider</i>	- A Third Party Provider delivers outsourced services such as cloud hosting or IT support. The organization must ensure contractual security clauses aligned to [KP3] and [SB4]. - Evidence includes contracts, due diligence records, and review logs stored under Annex A A.3 Risk Register or equivalent.

You may combine roles in small teams, but you must still assign each accountability to a named person. If one person holds multiple roles, you should document how independence is maintained for approvals and exceptions.

5. Strategic Planning and Priorities

Strategic planning ensures that cybersecurity efforts support the organization's real business needs and risk exposure. Before defining Objectives and Key Results, leadership should briefly review the organization's systems, risks, and obligations to determine where security improvements will have the greatest impact.

For SMEs, strategic planning does not require complex frameworks or long reports. A short annual discussion between the Board and the Info Sec Coordinator is sufficient to confirm priorities, identify key risks, and decide which areas of the organization require the most attention during the coming year.

The output of this process becomes the set of Objectives implemented through the OKR system.

5.1. Scope and risk context

Strategic planning begins with confirming the scope of the cybersecurity program and understanding the current risk landscape. This ensures that planning decisions are based on real operational conditions rather than assumptions.

Inputs for this review typically include:

- Annex A A.1 Asset and Data Inventory
- Annex A A.2 Risk Assessment Matrix
- recent incidents recorded in Annex A.A 4 Incident Log
- supplier and Third Party Provider risks recorded in Annex A A.3
- major technology or organizational changes

The Board and Info Sec Coordinator should confirm that the scope still reflects the organization's most important systems, services, and data. If major changes occurred during the year, the inventory and risk records should be updated before planning continues.

5.2. Annual security priorities

After reviewing the scope and risks, leadership identifies the most important cybersecurity priorities for the coming year. These priorities represent the areas where improvement will most effectively reduce risk or strengthen operational resilience.

Typical priorities may include:

- strengthening identity and access control
- improving vulnerability management and patching
- increasing staff security awareness

- strengthening supplier security oversight
- improving backup and recovery readiness

These priorities do not yet define specific actions. Instead, they represent strategic focus areas that guide how Objectives will be selected across the Action Zones.

5.3. Translating priorities into Objectives

Once priorities are agreed, the Info Sec Coordinator converts them into measurable Objectives within the OKR system. Each Objective should address a priority identified during strategic planning and reference relevant ShieldNet controls.

When creating Objectives, the following rules apply:

- each Objective must belong to one Action Zone
- Objectives should address significant risks or operational weaknesses
- each Objective must have three to five measurable Key Results
- the total number of Objectives should not exceed ten per year

This approach ensures that the Cybersecurity Management System remains focused on the issues that matter most, while keeping the workload manageable for SMEs with limited security resources.

6. Action Zones as the Operating Cycle

The Action Zones structure the Cybersecurity Management System into five logical areas that reflect the full security lifecycle. They ensure that Objectives are not chosen randomly, but are distributed across understanding risk, implementing protection, monitoring operations, responding to incidents, and improving over time.

For SMEs, the Action Zones prevent overfocusing on technology while neglecting governance or recovery. A balanced annual OKR plan should include Objectives from multiple zones so that risk identification, control implementation, operational vigilance, resilience, and learning evolve together in a coordinated way.

Each Objective must clearly state which Action Zone it belongs to. This ensures traceability to ShieldNet controls and helps the Board understand whether the organization is strengthening strategy, protection, detection, response, or improvement in a structured and measurable way.

6.1. KNOW AND PLAN

This zone focuses on understanding assets, risks, legal duties, and defining strategy. Good Objectives here improve visibility and governance clarity.

Typical Objectives:

- Improve risk assessment maturity [KP1], [KP2]
- Complete asset inventory accuracy

Typical evidence:

- Annex A A.1 Asset Register
- Annex A A.3 Risk Register
- Board approval minutes

6.2. SHIELD AND BUILD

This zone implements protective measures and secure configurations. Objectives here reduce exposure and strengthen architecture.

Typical Objectives:

- Enforce multi factor authentication [SB1]
- Implement network segmentation [SB3]

Typical evidence:

- Configuration screenshots
- Access control matrix Annex A A.4

- Firewall rule exports

6.3. WATCH AND PATCH

This zone ensures monitoring and vulnerability management are working effectively. Objectives focus on detection and maintenance.

Typical Objectives:

- Reduce critical vulnerabilities older than 30 days [WP2]
- Establish daily log review [WP1]

Typical evidence:

- Vulnerability scan reports Annex A A.5
- Patch logs
- Alert review checklist

6.4. REACT AND RECOVER

This zone ensures resilience and incident readiness. Objectives aim to reduce impact and recovery time.

Typical Objectives:

- Test backup restoration quarterly [RR2]
- Update incident response plan [RR1]

Typical evidence:

- Backup restore screenshots
- Incident drill minutes
- Business continuity documentation Annex A A.6

6.5. LEARN AND LIFT

This zone focuses on improvement, training, and internal audit. Objectives here strengthen culture and governance maturity.

Typical Objectives:

- Achieve 100 percent staff training completion [LL1]
- Close audit findings within 60 days

Typical evidence:

- Training attendance logs
- Audit reports
- Corrective action tracker

7. Risk Management

Risk management is the foundation that ensures cybersecurity activities remain proportionate, targeted, and aligned with business priorities. In this management system, risks determine which security improvements become Objectives and which controls receive the most attention.

For SMEs with limited resources, a structured but simple risk process helps avoid reacting only after incidents occur. By identifying and assessing risks regularly, the organization can focus its efforts on the threats that matter most while demonstrating compliance with the risk based expectations of EU cybersecurity and data protection regulations.

Risk management in this system is documented through the Risk Register and related artefacts defined in Annex A. These records form the basis for prioritizing Objectives in the Action Zones and for demonstrating governance oversight during management reviews.

7.1. Risk identification

Risk identification ensures the organization understands what could negatively affect the confidentiality, integrity, or availability of its systems and data. The goal is to recognize potential threats and weaknesses before they lead to operational disruption or regulatory exposure.

Risks should be identified using information from several sources:

- the Asset and Data Inventory maintained in Annex A A.1
- system knowledge provided by each System Owner
- incident history recorded in Annex A A.4 Incident Log
- vulnerability scanning results and patch records
- supplier and Third Party Provider assessments

Common cybersecurity risks for SMEs include:

- ransomware or malware affecting critical systems
- phishing attacks leading to account compromise
- misconfigured systems or missing security patches
- service outages at cloud or infrastructure providers
- accidental disclosure of sensitive or personal data

Risk identification should occur at least annually and whenever significant changes occur, such as introducing new systems, expanding services, or onboarding new suppliers.

7.2. Risk assessment

Risk assessment evaluates how serious each identified risk is and determines which issues require the most urgent attention. The process should remain simple and understandable so that SMEs can perform it without specialized tools.

Each risk is evaluated using two basic factors:

- likelihood, the probability that the risk event could occur
- impact, the severity of consequences if the event occurs

These factors are combined to determine a risk level that allows the organization to prioritize mitigation actions. The results are documented in the Risk Register using the Annex A A.2 Risk Assessment Matrix.

A simplified scoring approach may be used, for example:

- likelihood rated from rare to very likely
- impact rated from negligible to severe

Higher combined scores represent risks that should normally be addressed through Objectives in the OKR system.

7.3. Risk ownership and accountability

Every identified risk must have a clearly assigned owner responsible for monitoring the risk and coordinating mitigation actions. Assigning ownership ensures that risks are actively managed rather than remaining unresolved observations.

Typical ownership responsibilities include:

- monitoring the risk and any related indicators
- coordinating implementation of mitigation measures
- reporting progress during governance reviews

In most cases:

- the System Owner manages risks related to their system or service
- the Info Sec Coordinator oversees the overall Risk Register

The Board retains ultimate accountability for cybersecurity risk decisions. This includes approving risk treatment strategies and formally accepting residual risks when mitigation is not practical.

7.4. Risk treatment and prioritization

Risk treatment determines how the organization responds to identified risks. Decisions made during this step directly influence which improvements become Objectives within the OKR system.

Common treatment options include:

- reduce the risk by implementing additional security controls
- transfer the risk through contractual safeguards or insurance
- avoid the risk by changing the affected activity or process
- accept the risk when mitigation would be disproportionate to the potential impact

When a risk requires mitigation, the improvement actions should be translated into Objectives within the relevant Action Zone. For example:

- governance related risks may generate Objectives in KNOW and PLAN
- technical protection gaps may generate Objectives in SHIELD and BUILD
- monitoring weaknesses may generate Objectives in WATCH and PATCH

This linkage ensures that the Cybersecurity Management System continuously addresses the most significant risks facing the organization.

7.5. Risk monitoring and review

Risk monitoring ensures that previously identified risks remain under control and that new risks are detected as the organization evolves. Risks and mitigation actions must be reviewed regularly to confirm that assessments remain accurate.

Risk review activities include:

- updating the Risk Register when systems or services change
- verifying that mitigation actions are implemented effectively
- reviewing incident records for emerging threats
- reassessing risk levels when new vulnerabilities or regulations appear

Risk monitoring is integrated with the governance cadence described in Section 7. Annual planning uses the Risk Register to determine security priorities, while quarterly reviews verify that mitigation actions and Objectives are reducing risk exposure.

Maintaining an active risk management process ensures that the Cybersecurity Management System remains aligned with real operational threats and supports continuous improvement of the organization's cybersecurity posture.

8. Governance cadence and management review

A Cybersecurity Management System only works if it runs on a predictable rhythm. Governance cadence defines when decisions are made, who makes them, what evidence is reviewed, and how underperformance is corrected. Without a structured cadence, Objectives drift, evidence becomes outdated, and risks accumulate silently.

For SMEs, the cadence must be lightweight but disciplined. Meetings must be short, role driven, and evidence based. The purpose of this section is to define a minimal operating model that ensures cybersecurity is reviewed at strategic, tactical, and operational levels without creating unnecessary overhead.

The cadence connects OKRs to real management oversight. It ensures that the Board exercises accountability, the Info Sec Coordinator maintains visibility, and System Owners actively manage controls aligned to ShieldNet requirements.

8.1. Annual planning

Annual planning defines strategic direction and sets the security priorities for the year. This is where the organization translates risk exposure and business objectives into no more than 10 measurable Objectives across the Action Zones.

Participants: Board, Info Sec Coordinator

Decisions made:

- Approve annual Objectives and assign Action Zones
- Confirm scope and risk posture
- Approve budget or resource needs

Evidence updated:

- Annual OKR register
- Updated Annex A A.1 Asset Register if scope changed
- Updated Annex A A.3 Risk Register

If a Key Result from the prior year was not achieved, the Board decides whether to carry it forward, redefine it, or formally accept the risk.

8.2. Quarterly review and reset

Quarterly reviews provide structured oversight of progress and allow controlled adjustment. This cadence ensures Objectives remain relevant and measurable rather than symbolic.

Participants: Board, Info Sec Coordinator, relevant System Owners

Decisions made:

- Confirm percentage completion of each Key Result
- Validate that evidence is current and complete
- Adjust timelines or scope if justified

Evidence updated:

- *OKR progress report*
- *Annex A artefacts referenced by each Key Result*
- *Corrective action tracker*

If a Key Result is off track, a corrective action is defined with a named owner and deadline. If the delay creates significant risk exposure, the issue is escalated formally to the Board for decision.

8.3. Monthly check in

Monthly check ins ensure operational visibility and prevent surprises at the quarterly level. This meeting is short and focused strictly on metrics and evidence status.

Participants: Info Sec Coordinator and relevant System Owners

Duration: Less than 30 minutes

Decisions made:

- Confirm current metric values
- Validate that logs and artefacts are stored correctly
- Identify early warning signs

Evidence updated:

- Access review logs
- Vulnerability and patch logs
- Incident log entries if applicable

If metrics show deterioration, immediate containment or remediation tasks are assigned without waiting for quarterly review.

8.4. Weekly habits

Weekly habits are operational micro controls that sustain discipline. They ensure that critical controls such as monitoring, patching, and backup checks remain active.

Participants: Info Sec Coordinator or delegated IT support

Activities under 30 minutes:

- Review critical alerts or security dashboard
- Confirm backup completion status

- Check patch deployment summary
- Confirm no unresolved high severity vulnerabilities

Evidence may include dashboard screenshots, log exports, or brief checklist confirmations saved under the relevant Annex A folders.

If a control fails during weekly checks, immediate corrective action is triggered and logged in the corrective action tracker

8.5. Corrective actions and continual improvement

Corrective action management ensures that missed Key Results or control failures lead to structured improvement rather than informal fixes. This mechanism closes the loop between measurement and governance.

When a Key Result is not achieved or a control is ineffective:

1. The Info Sec Coordinator performs a brief root cause analysis.
2. A corrective action is defined with a measurable outcome.
3. A System Owner is assigned with a deadline.
4. Progress is tracked in the improvement log.

Major corrective actions that involve cost, risk acceptance, or structural change are escalated to the Board for approval.

Continual improvement is achieved by feeding lessons from incidents, audits, and missed targets back into the next annual planning cycle, ensuring that the Cybersecurity Management System matures in a structured and measurable way.

9. Evidence management and Annex A alignment

A Cybersecurity Management System is only credible if it produces clear, structured, and retrievable evidence. Evidence management ensures that every Objective, every Key Result, and every referenced control tag such as [KP1] or [SB3] can be demonstrated through documented proof aligned to Annex A artefacts.

For SMEs, evidence must be simple, proportionate, and organized. The goal is not to create paperwork for its own sake, but to maintain a minimal, reliable evidence pack that shows controls are implemented and working in practice. Well managed evidence reduces audit stress, supports certification readiness, and strengthens internal accountability.

Annex A provides standardized Core Templates and Extended Templates. This section defines how those artefacts are used as the backbone of the system, how they are stored, and how document control is applied so that evidence remains current, versioned, and owned..

9.1. Minimal evidence pack

At minimum, maintain Core Templates aligned to Annex A A.1 to A.6. These typically include:

- Asset Register
- Risk Register
- Incident Log
- Access Review Log
- Vulnerability and Patch Log
- Business Continuity or Backup Record

Extended Templates may be adopted later as maturity increases.

9.2. Folder structure

Recommended catalog structure:

- Governance
 - A.1 Asset Register
 - A.2 System Inventory
- Risk
 - A.3 Risk Register
- Operations
 - A.4 Access Reviews
 - A.5 Vulnerabilities
- Resilience

- A.6 Backup and Recovery
- Improvement
- Audit and Training

The numbering mirrors Annex A to ensure certification readiness.

9.3. Document control rules

Each document must include:

- Owner, usually the Info Sec Coordinator or System Owner
- Version number
- Last review date
- Next review date

Review frequency is at least annual for governance documents and quarterly for operational logs. Retention must follow legal and contractual obligations, typically minimum 12 months for operational evidence.

10. Certification readiness alignment

Running this system prepares the organization for ShieldNet certification levels without extra restructuring.

10.1. Starter readiness

Starter requires implementation of all core controls and current Core Templates. By maintaining OKRs and Annex A evidence, the organization can provide a clean evidence pack for desk review.

This aligns with the Starter level described in Annex C Certification Schema

10.2. Verified readiness

Verified requires evidence of effectiveness and selected Extended Templates. Quarterly reviews, vulnerability logs, and access reviews provide proof of operational effectiveness.

Maintaining measurable Key Results and documented reviews supports independent validation as described in Annex C