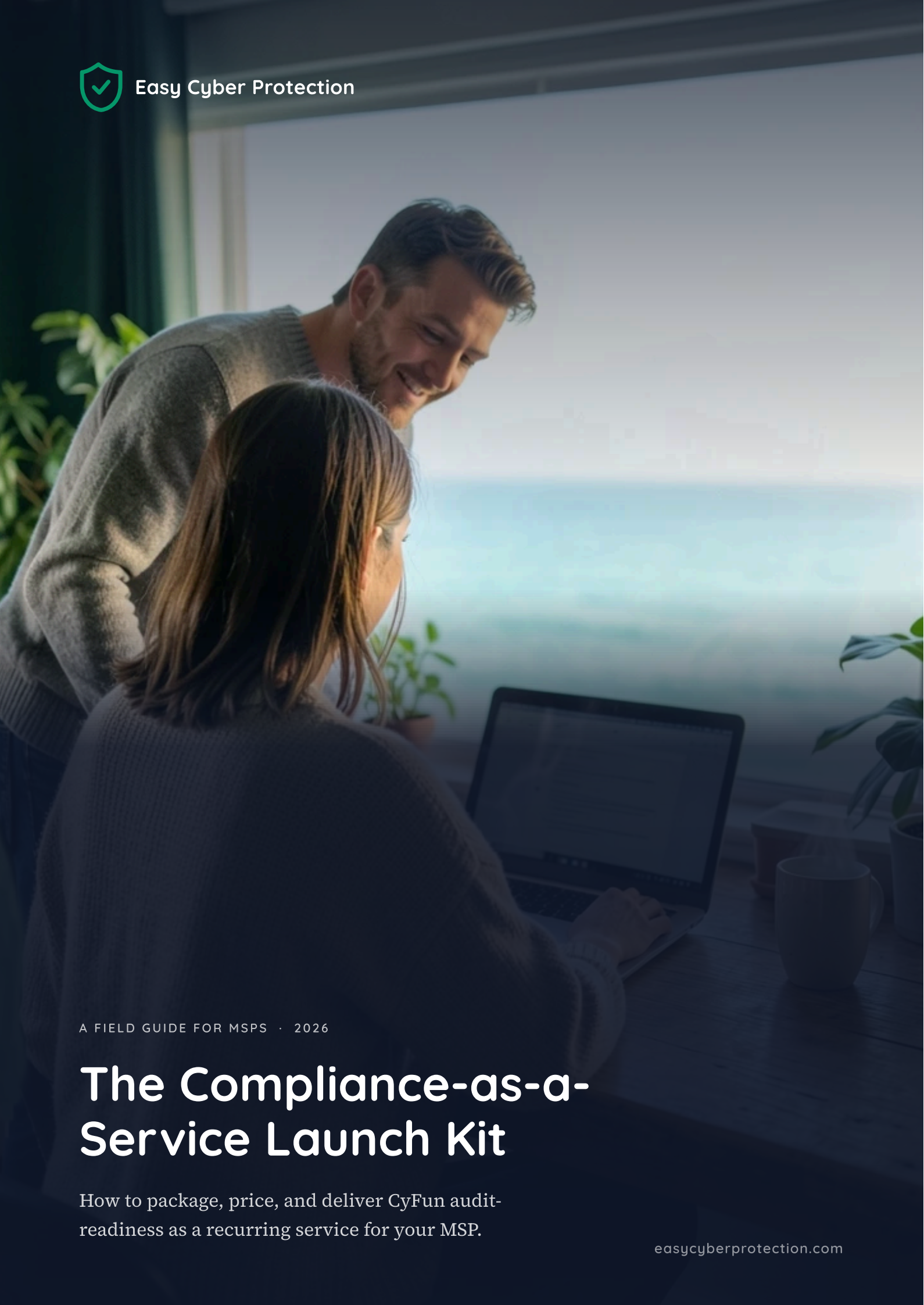
Easy Cyber Protection



A FIELD GUIDE FOR MSPS · 2026

The Compliance-as-a-Service Launch Kit

How to package, price, and deliver CyFun audit-readiness as a recurring service for your MSP.

easycyberprotection.com

FOREWORD

Tom Janssens

Founder, Easy Cyber Protection

I built Easy Cyber Protection because I kept seeing small and mid-sized businesses told they had to be "secure" and "compliant," with no one to make it practical. NIS2 raised the stakes. CyFun made it measurable. And all of it landed on the MSPs who already keep these businesses running.

This guide is the playbook I wish those MSPs had on day one. It is honest about the work: what CyFun actually asks for, what the evidence looks like, what it costs, and how to package it as a service your clients will gladly pay for, year after year. Most of it works whether or not you ever use our platform. That is on purpose. We do make a platform built for exactly this, and we introduce it honestly on the last page, after you have the full picture.

Compliance does not have to be stressful, for your clients or for you. Read it to the last page and you will know exactly how to turn the regulation everyone is worried about into the most dependable recurring revenue line you offer.

Tom Janssens

Founder, Easy Cyber Protection · 2026

Table of Contents

NEW TO THIS?

The Basics in 30 Seconds

Before anything else, here are the four terms you need. Everything in this playbook uses them.

- **NIS2** is the EU's new cybersecurity law. It forces thousands of organisations, and critically their whole supply chain, to prove they have basic security in place. Belgium was the first EU country to transpose it into national law (Law of 26 April 2024).
- **CyFun (CyberFundamentals Framework)** is the free framework published by Belgium's Centre for Cybersecurity (the CCB) that shows organisations exactly how to meet the requirement. It has four levels: Small (7 controls), Basic (34 controls), Important (132 controls), and Essential (217 controls). Most SME clients land on **Basic**.
- **A CAB** (Conformity Assessment Body) is the accredited auditor who officially checks a client against CyFun and issues a certificate. You get the client audit-ready. The CAB does the audit. Never blur that line.
- **Audit-ready** means every control is documented, evidenced, and above the passing threshold. It does not mean certified. The CAB makes that call.

That is the whole vocabulary. The rest of this playbook is what to do about it.

SECTION 1

1 Why This Is Suddenly Worth Money

1.1 The regulation is already in force

NIS2 has been Belgian law since April 2024. The deadline for essential-entity self-assessment passed on **18 April 2026**. CyFun certification or ISO 27001 must follow by **April 2027**. This is not a future thing. It is happening now.

Fines for non-compliance reach **€10 million or 2% of global annual turnover**, whichever is higher (NIS2 Article 83). Executives can be held personally liable.

4,000+
NIS2-obligated entities registered in Belgium by October 2025

160,000+
Organisations in scope across the EU

67%
Of Belgian SMEs with no compliance plan yet *(Agoria, 2025)*

1.2 The pressure flows downhill — and that is your market

THE SUPPLY-CHAIN COMPLIANCE CASCADE

NIS2 Article 21(2)(d): supply-chain security is a legal obligation for every regulated entity — and flows to their suppliers

1.3 The security case is real, not just regulatory

67%
Of ransomware victims are SMEs *(BlackFog, 2026)*

88%
Of SME data breaches involve ransomware *(Verizon DBIR, 2025)*

2
Accredited CAB auditors currently in Belgium for CyFun certification

The controls inside CyFun Basic (MFA, tested backups, endpoint protection, patching) are the exact controls that stop the most common attacks. You are helping clients stay secure and stay compliant at the same time.

Only **two CAB auditors are currently accredited** in Belgium to certify CyFun. Thousands of entities need audits by April 2027. The queue is already forming. Organisations that prepare early get scheduled first. Those who wait get pushed back and risk missing the deadline entirely. That urgency is a genuine selling point, not a scare tactic.

SECTION 2

2 What You Are Actually Selling

2.1 Readiness, not the certificate

This distinction matters legally and commercially. You deliver a state of audit-readiness: documented controls, evidenced practices, scores above the CCB threshold. A CAB auditor certifies the outcome. You are not selling a certificate you cannot issue. You are selling the readiness that makes certification possible.

Lead every client conversation with this framing: *"We get you ready. The auditor checks our work."* It sets the right expectation and positions you as the expert who prepares the file, not the body that stamps it.

2.2 A service, not a project

Security posture drifts continuously. A new laptop lands without the policy applied. An employee leaves and an account stays active. A backup schedule slips. A software version goes unpatched.

The gap-close is a one-time project. Keeping the client above the threshold month after month is the recurring service. **That is where the margin lives**, and that is what clients cannot do themselves.

SECTION 3

3 What It Takes to Get a Client Audit-Ready

Here is the honest, unvarnished scope of the work. Every step below applies whether you use a tool or do it by hand.

3.1 Step 1: Find the Right Level

Not every client needs Basic. Run the NIS2 risk assessment to determine which level applies. Most SMEs land on Basic, but a healthcare client or one supplying energy infrastructure may need Important or Essential.

CCB RESOURCES — LEVEL SELECTION

atwork.safeonweb.be/tools-resources/cyberfundamentals-framework

atwork.safeonweb.be/sites/default/files/2024-01/BE-NIS2-RA-v20240108.xlsx

NIS2 selection tool (.xlsx) — determines which level applies to a given client

3.2 Step 2: Download the Official CCB Booklet

Each level has its own booklet with the full list of controls, what they mean, and what evidence is expected.

CCB BOOKLETS (PDF)

safeonweb.be/sites/default/files/2026-06/CyFun2025_Booklet_BASIC_E.pdf — Basic

safeonweb.be/sites/default/files/2026-06/CyFun2025_Booklet_Important_E_0.pdf — Important

safeonweb.be/sites/default/files/2026-06/CyFun2025_Booklet_Essential_E_0.pdf — Essential

3.3 Step 3: Get the Self-Assessment Workbook

The CCB publishes an official Excel workbook for each level. This is the scoring tool that maps directly to what a CAB auditor will check.

CCB SELF-ASSESSMENT WORKBOOKS (EXCEL)

cyfun.eu — Self-Assessment_tool_BASIC_v2026_02_20.xlsx

cyfun.eu — Self-Assessment_tool_IMPORTANT_v2026_02_20.xlsx

cyfun.eu — Self-Assessment_tool_ESSENTIAL_v3.1.xlsx

3.4 Step 4: Score Every Control on Two Axes

Each of the 34 Basic controls gets two scores from 1 to 5: one for how well it is **documented**, and one for how well it is **set up and running**. Both scores matter.

THE 1–5 MATURITY SCALE

1	2	3	4	5
Nothing written / not set up	Informal notes / inconsistent	Proper policy / consistently applied	Reviewed & shared / monitored	Continuous improvement documented

SCORE	DOCUMENTATION	IMPLEMENTATION
1	Nothing written down	Not set up at all
2	Basic or informal notes	You do it, but not consistently
3	A proper policy or procedure is written	Standard practice, consistently applied
4	Regularly reviewed and shared with staff	Actively monitored, measured
5	Continuous improvement is documented	Continuously improved from real measurements

SCORING GUIDANCE (OFFICIAL PDF)

atwork.safeonweb.be/sites/default/files/2024-03/CyberFundamentals%20Maturity%20Level%20description.pdf

3.5 Step 5: Clear the Threshold

You do not need a perfect 5 across the board. The CCB weights certain controls more heavily, so a few weak spots can drag you below the line even if most controls score well.

LEVEL	CONTROLS	THRESHOLD
Basic	34	2.5 average (weighted key controls)
Important	132	3.0 for key controls
Essential	217	3.0 key controls + 3.5 overall

3.6 Step 6: Build the Evidence Dossier

A CAB auditor does not take your word for it. Every control needs proof: a signed policy, a screenshot of the MFA settings, a backup test report, a log excerpt, an asset inventory export. You assemble all of it into a single dossier. The cleaner and more complete it is, the faster and cheaper the audit goes for your client.

3.7 What each maturity level looks like in practice

The 1-5 scale can feel abstract until you see it applied to a real control. Here is what each level looks like for **PR-2 (Multi-factor authentication)**, broken across both axes:

LEVEL	DOCUMENTATION	IMPLEMENTATION
1	Nothing written. No policy mentions MFA at all.	MFA is off everywhere. Staff log in with password only.

2	Someone typed a note in a shared document: "We use MFA on email." No sign-off, no date.	MFA is on for some accounts — usually those who set it up themselves. No enforced baseline.
3	A written Access Management Policy exists, signed by management, covering which systems require MFA, what method is accepted (authenticator app vs SMS), and what exceptions require approval.	MFA enforced via Conditional Access Policy in Microsoft 365 or equivalent. Covers all staff on email, file storage, remote access. Tested and confirmed.
4	Policy is reviewed every six months. Changes are logged with a revision date. New joiners are briefed on it as part of induction, which is documented.	Compliance is actively monitored — a monthly report shows which accounts are MFA-enrolled, which have exceptions, and why. Exceptions need a named approval.
5	The organisation measures MFA adoption rate quarterly and feeds results into its security improvement plan. Previous findings from failed enrolments drove a change in process (documented).	Phishing-resistant MFA (FIDO2 or hardware token) is in use for privileged accounts. Regular tests confirm it blocks simulated credential attacks. Results update the security roadmap.

Most SME clients arrive at level 1-2. Getting them to level 3 across all controls is the gap-close project. Keeping them at 3 and above is the recurring service.

3.8 What the evidence dossier looks like

Think of the dossier as a folder — physical or digital — organised by control ID. Each control folder contains:

- **The policy or procedure document** (a PDF, dated and signed by management)
- **Proof the policy is implemented** (a screenshot from the admin console, a configuration export, a log excerpt)
- **Proof it is maintained** (a test report, a review record, an access log showing active use)

For some controls the evidence is a single screenshot. For others — like a tested backup — it is a restore test report with a date, the system tested, the files recovered, and the person who signed off. The CCB provides evidence checklists in the official booklets; use them as your packing list.

EVIDENCE CHECKLIST SOURCE

safeonweb.be — CyFun2025_Booklet_BASIC_E.pdf

Appendix B of the Basic booklet lists exactly what evidence each control requires

SECTION 4

4 Package It and Price It

4.1 The two-stream model

Everything you deliver for a client falls into one of two streams. Price them separately. That is the whole commercial structure.

Stream 1 — Implementation

- Multi-factor authentication (MFA)
- Tested, documented backups
- Endpoint protection (EDR)
- Log retention
- Retiring hardware that cannot be patched

One-time setup: €750–€2,500
+ Monthly managed service fee

Stream 2 — Documentation

- Written policies and procedures
- Access-review records
- Evidence for every control
- Quarterly policy refresh
- Full evidence dossier for CAB

One-time gap-close fee (from assessment)
+ Quarterly / annual iteration

4.2 What this is worth to you

THE MARGIN MATH — EXAMPLE: 25 CLIENTS

Clients × average monthly fee	25 × €250
Monthly recurring revenue	€6,250 / month
Margin (70%)	€4,375 / month
Annual operating profit	**€52,500 / year**