Easy Cyber Protection

A FIELD GUIDE FOR MSPS · 2026

NIS2 Compliance for MSPs

How to offer your clients CyFun audit-readiness as a recurring service, without hiring a compliance expert.

easycyberprotection.com

FOREWORD

Tom Janssens

Founder, Easy Cyber Protection

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

This guide shows you how to offer that audit-readiness to your clients as a recurring service, without hiring or training a compliance person. It is honest about the work: what CyFun actually asks for, what the evidence looks like, what it costs, and how to package it so clients gladly pay year after year.

What makes that possible is the platform. You run all of it on Easy Cyber Protection, so the work that would normally need a compliance specialist is handled for you. And if you would rather not touch the compliance side at all, our own CyFun expert can run it with you, under your brand, while you keep the client relationship. Either way, you turn the regulation everyone is worried about into your most dependable recurring revenue line. That is what the rest of this book is for.

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.

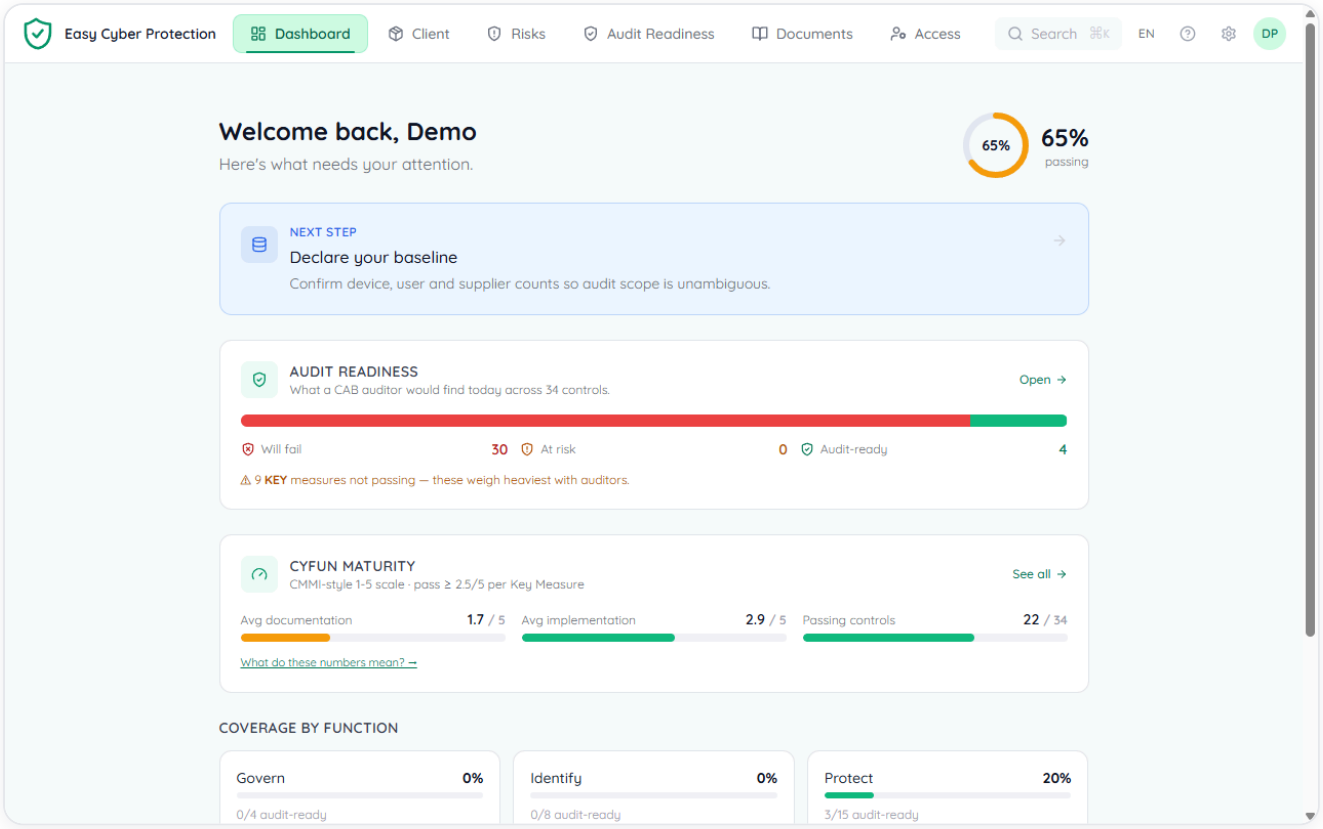
2.2 A service, not a project

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.

2.3 How you deliver it without staffing a compliance team

Here is the part most MSPs get wrong: they assume "compliance service" means "hire a compliance person." It does not. You run this on Easy Cyber Protection, the platform built for exactly this work. It automates the CyFun scoring, the evidence collection, and the policy documentation, so your existing team delivers the service with no compliance hire. The moment you connect a client's existing tools, a large share of the controls are already satisfied, before anyone writes a policy. This is what one client looks like on it:



One client in Easy Cyber Protection: audit-readiness, CyFun maturity, and where the gaps are, at a glance.

The rest of this book assumes you are running on the platform, because that is how MSPs deliver this at scale. If you would rather not build the compliance muscle yet, our CyFun expert can run it with you on the same platform, under your brand. The closing section covers the platform and the expert option, with pricing and how to start.

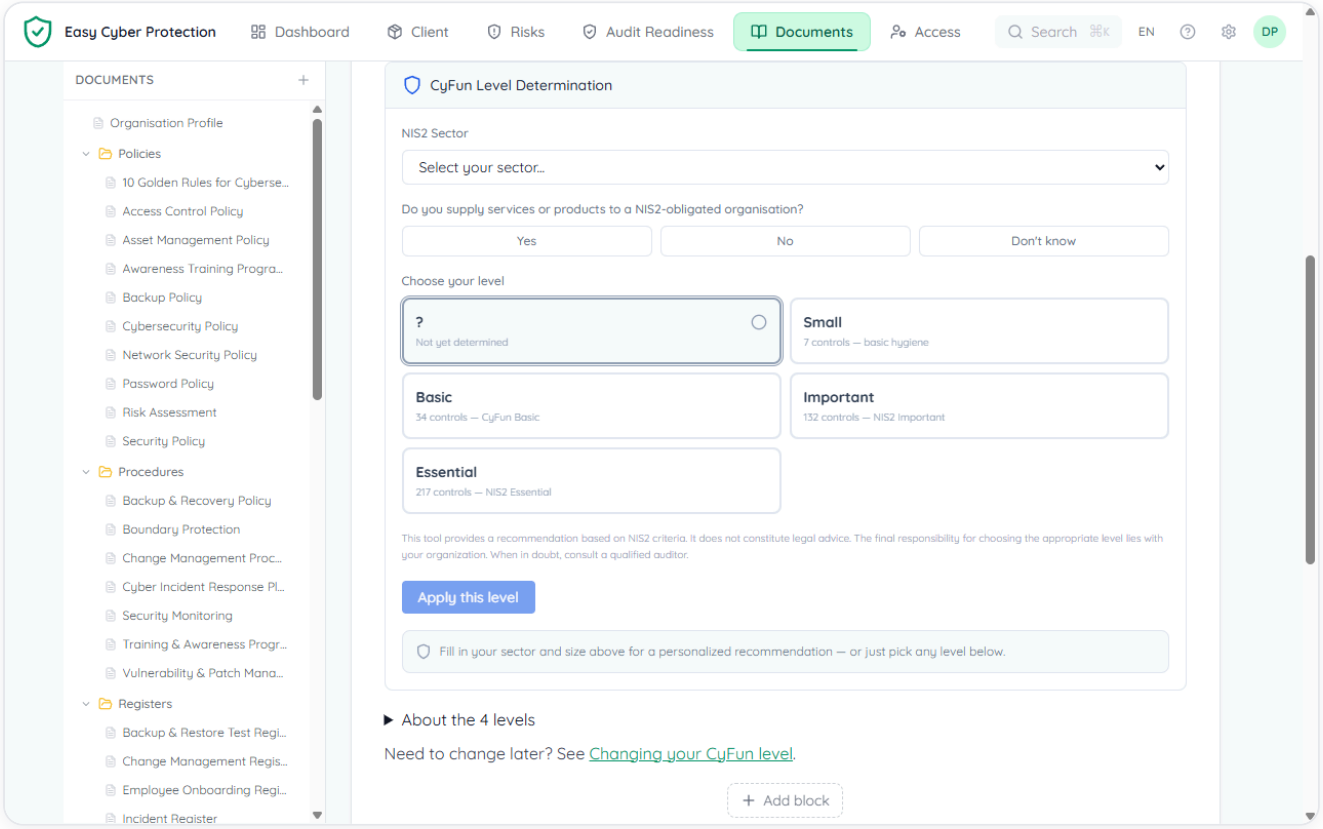
SECTION 3

3 Getting a Client Audit-Ready, the ECP Way

This is the real workflow, in the order you run it on the platform: pick the level, connect the client's tools, define what is in scope, work the assessment, then fill the documentation gaps until the client is ready. The platform does the heavy lifting at every step. You bring the judgment.

First, pick the level

Not every client needs Basic. Easy Cyber Protection has a built-in level selector: pick the client's NIS2 sector, answer whether they supply a regulated organisation, and the platform recommends the right CyFun level. Most SMEs land on Basic (34 controls), but a healthcare client or one supplying energy infrastructure may need Important (132) or Essential (217). You can change the level later without losing any work.



The built-in level selector: two questions, and the platform recommends Small, Basic, Important, or Essential.

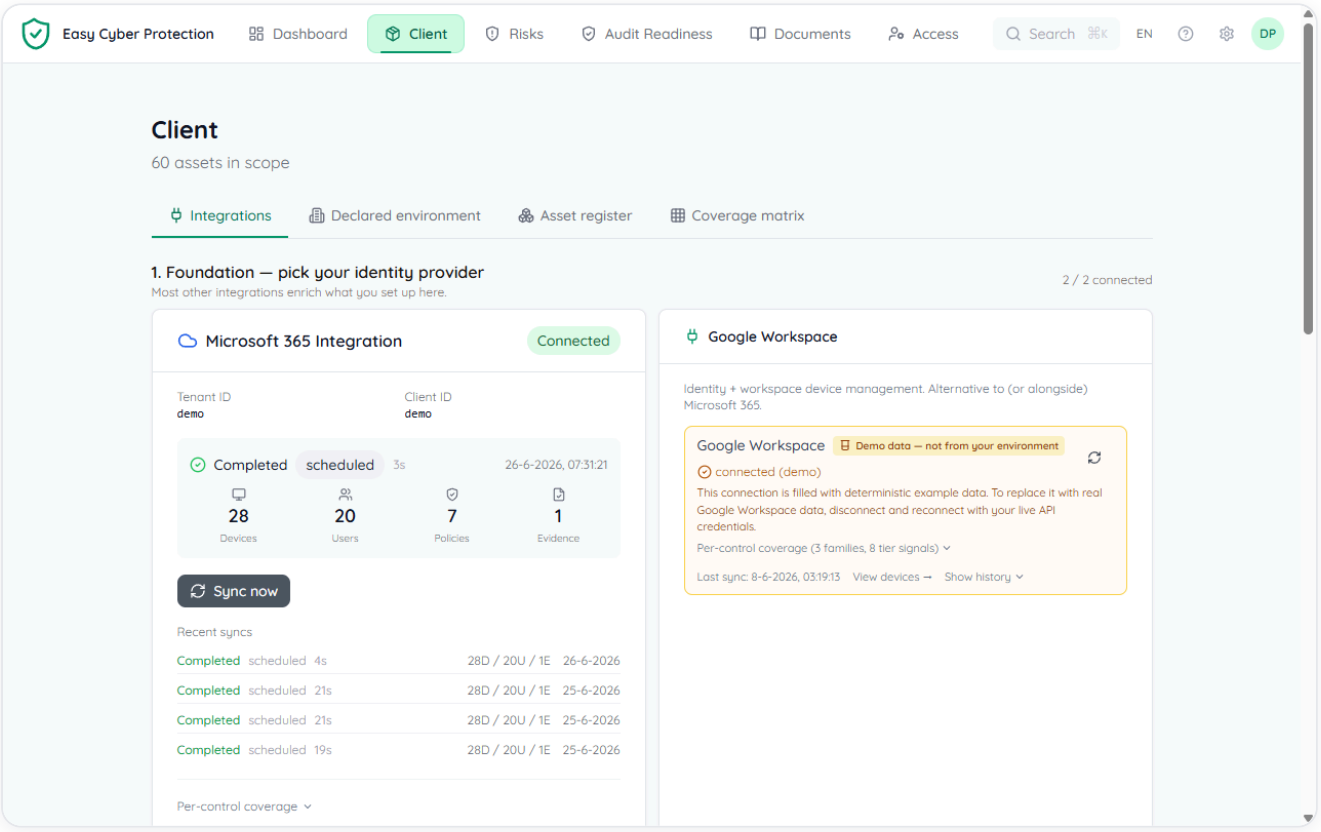
THE ONE CITATION THAT MATTERS

atwork.safeonweb.be — CyberFundamentals, the CCB's official framework

CyFun is published by Belgium's Centre for Cybersecurity. Easy Cyber Protection implements it exactly and exports the same CCB self-assessment workbook a CAB auditor opens, so you never touch the by-hand spreadsheets.

3.1 Step 1: Integrate the tools the client already runs

This is the moment that makes the whole service viable. Connect the client's Microsoft 365, their EDR, their RMM, and the other tools they already pay for, and Easy Cyber Protection reads the live configuration and maps each piece of evidence to the CyFun controls it satisfies. No screenshots, no copy-paste, no policy written yet.



Connect the tools the client already runs, and the evidence flows in and maps itself to the controls.

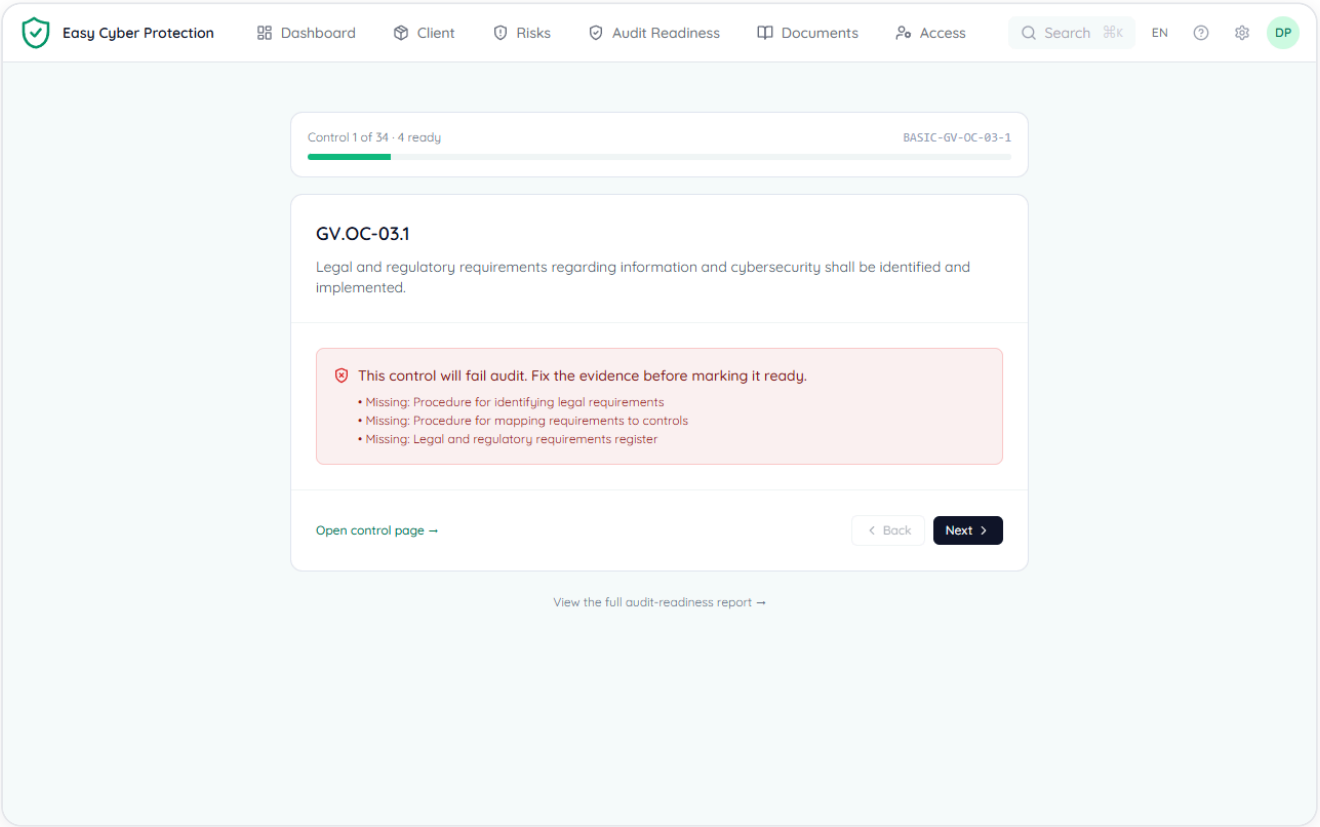
The payoff is the head start. In the demo client, simply connecting the tools puts **22 of the 34 controls** at a passing score and the client at **65% audit-ready**, before anyone has written a single policy. That is the single biggest reason to run this on the platform instead of by hand: most of the technical evidence already exists in the client's environment, and the platform harvests it for you.

3.2 Step 2: Define the landscape

Audit-readiness is judged against a defined scope, so the platform needs to know what it is protecting. The Client tab holds the asset and entity register: the devices, users, suppliers, applications, and networks in scope. Most of it arrives automatically from the integrations in Step 1; you confirm the counts and add anything the tools cannot see, such as an external supplier or a physical site. A clear landscape is what makes the audit scope unambiguous.

3.3 Step 3: Do the assessment

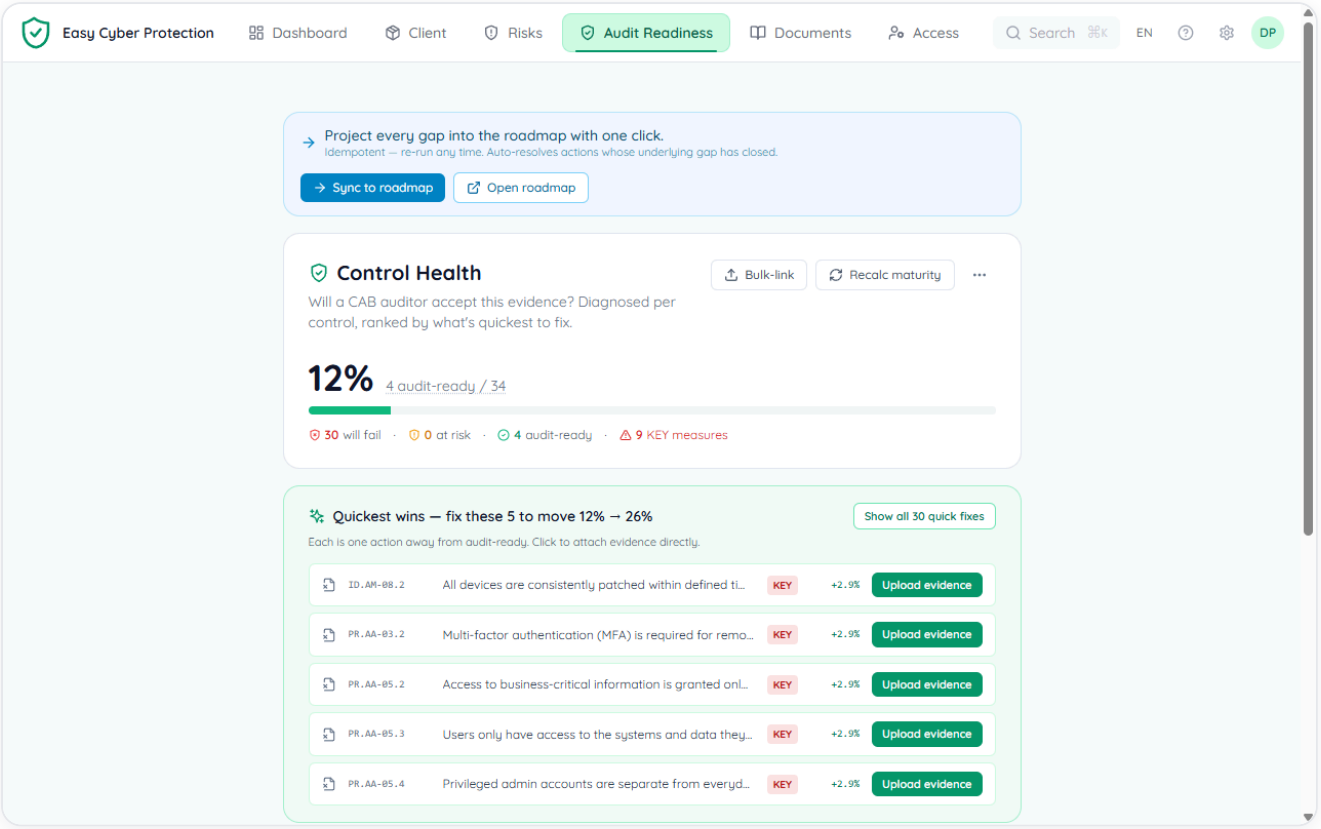
Now you work the controls. The platform walks your team through the client one control at a time, shows exactly what evidence each control needs, and will not let you mark a control audit-ready while that evidence is missing:



The guided assessment: one control at a time, with a hard gate that blocks "audit-ready" until the missing evidence is in place.

Across all 34 controls, the result is the Control Health view: every control scored on two axes, diagnosed, and ranked by what is quickest to fix, with the KEY measures that weigh

heaviest flagged.



Control Health: every control scored and diagnosed, with the quickest wins surfaced first.

Each control 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**. The platform reads the evidence and scores these for you, but it is worth understanding the scale so you can read the result and explain it to a client:

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

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