



The road to ISO 27001 in eight steps

Tom De Cubber, CySLOK

From the decision to start through to the certificate, there are eight steps, and it usually takes six to twelve months. This page explains what happens at each step and what is expected of you as a business owner.



Eight steps from decision to certificate

Expect six to twelve months

That may seem long. But for most businesses cybersecurity comes second, because the core business has to keep running at full speed. If it is genuinely urgent for your organisation's survival, it can be done in four to six months. Be aware, though, that in most cases this is fairly unrealistic.

Eight steps, each with your role

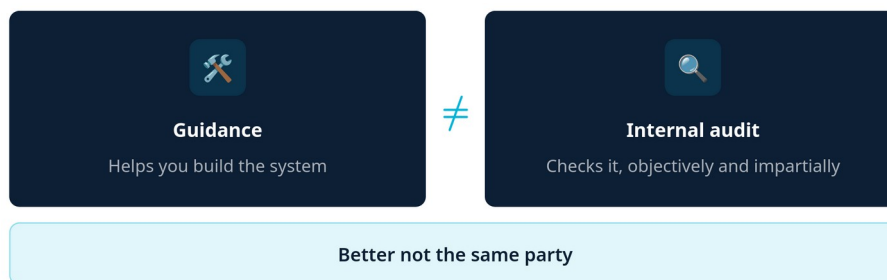
- 1** **Decide and set the scope.** You decide why you are starting and which part of your business the system covers.
Your role: make the decision and free up the time to actually carry it out, or to have it carried out.
- 2** **Map what would bring your business to a halt.** Which information and systems are indispensable, what can go wrong with them, and how bad would that be?
Your role: help decide what really matters to your business.
- 3** **Choose measures.** For each important risk you choose what you do about it, and you record why you take some measures and not others.
Your role: decide which risk you accept.
- 4** **Put it into practice and keep it alive.** Write down the agreements, explain to employees why they exist, and check whether it works. This is the longest step.
Your role: visibly back the agreements.
- 5** **Internal audit.** Someone who did not build the system checks whether it works as intended and meets the standard.
Your role: take the findings seriously.
- 6** **Management review.** Senior management sits down, looks at the results, the audit and the risks, and decides what needs adjusting.
Your role: this is your step.
- 7** **Certification audit.** An independent, officially accredited organisation checks your system in two rounds: first how it is set up, then whether it works in practice.
Your role: be available for the interviews.
- 8** **Maintain.** Every year there is a surveillance audit, and every three years a full recertification.
Your role: keep using the system, even when no audit is coming up.

A certificate is not mandatory. You can stop after step 6: you then have the system, without the certificate.

Whoever builds it does not check it

The road includes two roles that you are better off not giving to the same party.

The first is guidance: someone who helps you build the system. The second is the internal audit: a check that confirms, or refutes, that the system meets the standard and really protects you. The standard requires that check to be objective and impartial, and whoever helped build the system can hardly judge their own work impartially. So my advice is to have the internal audit done by someone from outside who was not involved in building it.



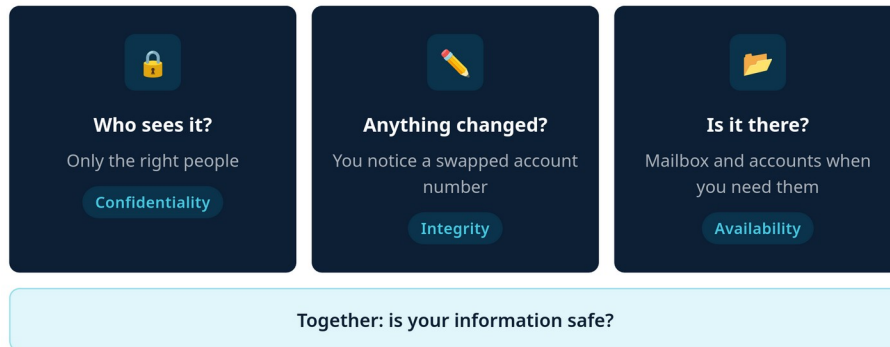
Two roles, kept apart

Before the certification audit starts, at least one internal audit and one management review must have been completed. I actually consider that internal audit more important than the certification audit. A good internal audit does not just tell you where you stand today. Drawing on the internal auditor's knowledge and experience, it also tells you where a limited effort will take you the furthest.

At any one organisation I take on one of the two roles: guidance during the implementation or the internal audit. If I take on the guidance, I can arrange for someone from my network with sufficient experience to do the internal audit, or you choose an internal auditor yourself. That keeps the two roles separate.

Start with what would bring your business to a halt

Want to do something today, even without a full programme? List the three things that would bring your business to a halt if they failed: a system, a supplier, a file or a person. That is where ISO 27001 starts on a small scale, even if you never get certified.



Three questions to ask about each of those three things

Book a short call: <https://cyslok.be/#contact>. No obligation. We look together at whether ISO 27001 makes sense for your business, and where best to start.