



Het traject naar ISO 27001 in acht stappen

Tom De Cubber, CySLok

Van de beslissing om te beginnen tot een certificaat telt het traject acht stappen, en het duurt doorgaans zes tot twaalf maanden. Op deze pagina leest u bij elke stap wat er gebeurt en wat er van u als zaakvoerder verwacht wordt.



Acht stappen van beslissing tot certificaat

Reken op zes tot twaalf maanden

Dat lijkt lang. Maar voor de meeste bedrijven is cyberveiligheid bijzaak, want de kernactiviteit moet op volle kracht doorgaan. Is het voor het voortbestaan van uw organisatie echt dringend, dan kan het in vier tot zes maanden. Opgelet: in de meeste gevallen is dat vrij onrealistisch.

Acht stappen, met bij elke stap uw rol

1	Beslissen en afbakenen. U beslist waarom u eraan begint en voor welk deel van uw bedrijf het systeem geldt. Uw rol: de beslissing nemen en de tijd vrijmaken om het ook effectief uit te (laten) voeren.
2	In kaart brengen wat uw bedrijf stillegt. Welke informatie en systemen zijn onmisbaar, wat kan ermee misgaan, en hoe erg is dat? Uw rol: mee bepalen wat voor uw bedrijf echt telt.
3	Maatregelen kiezen. Bij elk belangrijk risico kiest u wat u eraan doet, en u legt vast waarom u bepaalde maatregelen wel en andere niet neemt. Uw rol: beslissen welk risico u aanvaardt.
4	Invoeren en laten leven. Afspraken vastleggen, medewerkers uitleggen waarom ze bestaan, en opvolgen of het werkt. Dit is de langste stap. Uw rol: zichtbaar achter de afspraken staan.
5	Interne audit. Iemand die niet zelf aan het systeem bouwde, controleert of het werkt zoals bedoeld en aan de norm voldoet. Uw rol: de bevindingen ernstig nemen.
6	Bespreking door de directie. De directie zit samen, bekijkt de resultaten, de audit en de risico's, en beslist wat er bijgestuurd wordt. Uw rol: dit is uw stap.
7	Certificatie-audit. Een onafhankelijke, officieel erkende organisatie kijkt in twee rondes na: eerst hoe uw systeem is opgezet, daarna of het in de praktijk werkt. Uw rol: beschikbaar zijn voor de gesprekken.
8	Onderhouden. Elk jaar volgt een opvolgingsaudit, om de drie jaar een volledige hercertificatie. Uw rol: het systeem blijven gebruiken, ook als er geen audit op komst is.

Een certificaat is niet verplicht. U kunt na stap 6 stoppen: dan heeft u het systeem, zonder het certificaat.

Wie bouwt, controleert niet

In het traject zitten twee rollen die u best niet bij dezelfde partij legt.

De eerste is de begeleiding: iemand die u helpt het systeem op te bouwen. De tweede is de interne audit: een controle die bevestigt, of weerlegt, dat dat systeem aan de norm voldoet en u echt beschermt. De norm vraagt dat die controle objectief en onpartijdig gebeurt, en wie het systeem mee opbouwde, kan zijn eigen werk moeilijk onpartijdig beoordelen. Mijn raad is daarom om de interne audit te laten doen door iemand van buiten, die niet bij de opbouw betrokken was.



Twee rollen, apart gehouden

Voordat de certificatie-audit begint, moeten er minstens een interne audit en een bespreking door de directie achter de rug zijn. Ik vind die interne audit zelfs belangrijker dan de certificatie-audit. Een goede interne audit zegt niet alleen waar u vandaag staat. Ze zegt ook, op basis van de kennis en ervaring van de interne auditor, waar u met beperkte inspanning de grootste stap vooruit zet.

Bij een organisatie neem ik een van beide rollen op: de begeleiding bij de invoering of de interne audit. Neem ik de begeleiding op, dan kan ik zorgen dat iemand uit mijn netwerk met voldoende ervaring de interne audit doet, of u kiest zelf een interne auditor. Zo blijven beide rollen gescheiden.

Begin met wat uw bedrijf stillegt

Wilt u vandaag al iets doen, ook zonder traject? Zet de drie dingen op een rij die uw bedrijf stilleggen als ze uitvallen: een systeem, een leverancier, een bestand of een persoon. Daar begint ISO 27001 in het klein, ook als u nooit certificeert.



Drie vragen bij elk van die drie dingen

Plan een kort gesprek: <https://cyslok.be/nl/#contact>. Vrijblijvend. We bekijken samen of ISO 27001 voor uw bedrijf zinvol is, en waar u het best begint.