INFORMATIEBEVEILIGING
MAGAZINE

DOSSIER 1

Apeldoorn- IT congres 2025

DOSSIER 2

Richtlijnen, normen en zekerheid

JAARGANG 26 - 2026 - EDITIE 1

Auteur: Stijn Eijkman is mede-eigenaar van Vestingborg BV, Uw Partner voor Informatiebeveiliging en Kwaliteit. Hij is bereikbaar via seijkman@vestingborg.nl

Pragmatische implementatie van ISO 27001 bij het midden- en kleinbedrijf

Kleinere bedrijven staan voor de uitdaging om gevoelige informatie te beschermen met vaak beperkte middelen, terwijl zowel cyberincidenten als het ontbreken van aantoonbare informatiebeveiliging grote gevolgen kunnen hebben voor bedrijfscontinuïteit en reputatie.

ISO 27001 is essentieel voor bedrijven omdat het een gestructureerd informatiebeveiligingsbeleid levert om risico's effectief te beheersen en de integriteit van gegevens te waarborgen. De norm is daarnaast een strategisch verkoopinstrument dat vertrouwen opbouwt en vaak een noodzakelijke voorwaarde is voor contracten. De implementatie is ook voor kleinere bedrijven realiseerbaar door een kostenbewuste en 'lean' aanpak met standaard templates en beperkte consultancy, waardoor het haalbaar is met een beperkt budget. Cruciaal is dat de focus ligt op efficiëntie en onderhoudsgemak: door het gebruik van centrale platforms en simpele documentatie wordt bureaucratie voorkomen en blijft het ISMS als continu beheersproces actueel.

Het invoeren van een goed informatiebeveiligingsbeleid op basis van de internationaal erkende ISO 27001-norm biedt juist voor deze MKB-organisaties veel profijt, omdat het een gestructureerde aanpak biedt om risico's te beheersen en informatie effectief te beschermen. Bovendien fungeert een ISO 27001-certificaat als een internationaal erkend keurmerk dat klanten, opdrachtgevers en partners overtuigt van de volwassenheid van je informatiebeveiliging, wat in aanbestedingen en bij nieuwe opdrachten een steeds belangrijkere voorwaarde is om in aanmerking te komen.

Om succesvol te zijn met beperkte middelen, is een kostenbewuste en 'lean' aanpak cruciaal. Dit wordt bereikt door slim gebruik te maken van standaard templates en door slechts beperkt externe consultancy in te schakelen. Deze strategie maakt het mogelijk om snel een kant-en-klare basis te vullen met de eigen bedrijfsprocessen, wat onnodige overhead voorkomt. Ook is de basis gelegd voor een effectieve implementatie van bijvoorbeeld ISO 9001 of ISO 14001 (1).

De Vier Belangrijkste Redenen voor ISO 27001

ISO 27001 is een internationaal erkend kader dat organisaties helpt om informatiebeveiliging op een aantoonbare, systematische en duurzame wijze in te richten. Er zijn meerdere dwingende argumenten om deze norm te implementeren, waarbij de prioriteiten per organisatie verschillen:

1. **Gegevensbeveiliging en Risicobeheer:** de norm helpt bij het beschermen van gegevens door processen te verbeteren en risico's te beheren. Dit omvat het **systematisch detecteren van kwetsbaarheden**, het beheersen van IT-risico's, het verkleinen van de risico's op beveiligingslekken, en het minimaliseren van mogelijke schade en vervolgkosten. Bovendien waarborgt het de vertrouwelijkheid van informatie (1)(2).
2. **Wettelijke Conformiteit en Kostenreductie:** ISO 27001 draagt bij aan de naleving van wettelijke regelgeving, zoals de Algemene Verordening Gegevensbescherming (AVG). Het biedt een gestructureerde methode om aan deze en andere internationaal erkende conformiteitseisen te voldoen. Door risicobeheer te verbeteren, verkleint men de kans op een datalek en kunnen boetes worden vermeden, wat bijdraagt aan lagere kosten (3) (4).
3. **Reputatie en Concurrentievoordeel:** de certificering verbetert de reputatie van de organisatie doordat wordt aangetoond dat de noodzakelijke stappen zijn gezet om gegevens te beschermen. Dit verhoogt het vertrouwen van partners, klanten en het publiek, en versterkt zakelijke relaties. Door deze erkende norm te voeren, onderscheidt de organisatie zich van concurrenten, wat een concurrentievoordeel oplevert (5).
4. **Operationele Efficiëntie:** operationele voordelen omvatten de mogelijkheid tot het veilig uitwisselen van gevoelige informatie met partners en klanten. Ook draagt het bij aan een hogere productiviteit door duidelijkheid te scheppen over wie voor welke informatie verantwoordelijk is, waardoor efficiënter gewerkt kan worden (5).

Deze argumenten – betere processen, risicovermindering, compliance, vertrouwen en commercieel voordeel – komen in vrijwel elk succesvol certificeringstraject terug.

Drijfveren en Rolverdeling bij Implementatie

Bij de introductie en implementatie van een Informatie Security Management Systeem (ISMS) binnen een klein bedrijf spelen verschillende rollen met hun eigen motivering een essentiële rol. Het is essentieel om deze verschillende perspectieven te begrijpen voor een succesvolle implementatie met voldoende draagvlak:

- Commercieel Directeur: voor deze rol is ISO 27001 primair een strategisch verkoopinstrument. Het certificaat is vaak noodzakelijk om nieuwe opdrachten te verwerven of bestaande relaties te behouden, aangezien zakelijke klanten en aanbestedingen informatiebeveiliging als contractvoorwaarde stellen.
- Operationeel Directeur (COO): de COO ziet de norm als een solide kader voor de operatie. De invoering van een ISMS kan operationele processen, zoals documentbeheer en bedrijfscontinuïteit, verbeteren. Dit vereist echter wel een extra tijdsinvestering voor

zaken als audits, documentatie en trainingen. De norm dwingt tot betere procedures en duidelijkere verantwoordelijkheden en vereist een cultuur van voortdurende verbetering in plaats van een incidentele inspanning.

- Projectmanager/Consultant: bij het gebrek aan voldoende interne capaciteit wordt vaak een externe projectleider ingeschakeld. De focus van de consultant ligt op efficiëntie en onderhoudsgemak. De implementatie moet zo effectief mogelijk verlopen, en de documentatie moet zo simpel mogelijk zijn om de opvolging te vereenvoudigen. Het motto in dit proces is "keep it simple": processen, verantwoordelijkheden en systemen moeten helder, toegankelijk en bij voorkeur in één centrale omgeving worden vastgelegd. Dit waarborgt eenvoudige opvolging en continuïteit.
- Medewerkers: alle medewerkers spelen een fundamentele rol in het functioneren van het ISMS. ISO 27001 benadrukt dat informatiebeveiliging niet alleen een taak van IT is, maar van iedereen binnen de organisatie. Medewerkers moeten zich bewust zijn van het beleid, de procedures kennen en hun dagelijkse werkzaamheden uitvoeren in overeenstemming met vastgestelde richtlijnen. Hun gedrag — zoals het rapporteren van incidenten, het veilig omgaan met data of het volgen van trainingen — draagt direct bij aan het succes van het ISMS en de continuïteit van de beheersmaatregelen.

Hoewel de drijfveren per rol verschillen, benadrukken ze gezamenlijk het belang van een 'lean' implementatie. De gekozen aanpak moet voldoende structuur bieden voor vertrouwen, compliance en commerciële waarde, zonder te leiden tot onnodige bureaucratie of verspilde middelen. Dit betekent slim gebruikmaken van standaarden, hergebruik van bestaande processen en het inzetten van een centraal platform voor beheer en documentatie.

Het ISMS binnen ISO 27001

Binnen de ISO 27001-norm vormt het Information Security Management System (ISMS) het centrale raamwerk voor het beheersen van informatiebeveiliging. Een ISMS is een **systematisch en risicogebaseerd geheel van beleid, processen, procedures en beheersmaatregelen** waarmee een organisatie informatie-risico's identificeert, beoordeelt, behandelt en continu verbetert, zodat de vertrouwelijkheid, integriteit en beschikbaarheid van gegevens gewaarborgd zijn. Het ISMS helpt organisaties om niet slechts ad-hoc reacties op incidenten te geven, maar om informatiebeveiliging structureel in de dagelijkse bedrijfsvoering te integreren en te borgen (1).

ISO 27001 gebruikt hiertoe de **gemeenschappelijke structuur voor ISO-managementsystemen** zoals vastgelegd in **Annex L**. Dit vaste raamwerk omvat de essentiële onderdelen van een managementsysteem, zoals context en scope, leiderschap, planning, ondersteuning, uitvoering, prestatie-evaluatie en verbetering (1).

Kernonderdelen van een ISMS

ISO 27001 schrijft de volgende elementen voor die, samen met de risicoanalyse en continue verbetering, samen het ISMS vormen (1):

- **Managementsysteemvereisten (ISO 27001 clauses 4–10):** deze hoofdstukken omvatten respectievelijk: context van de organisatie, leiderschap, planning, ondersteuning, uitvoering, prestatie-evaluatie en verbetering.
- **Risicobeoordeling en risicobehandeling:** systematisch bepalen wat de risico's zijn en welke maatregelen passend zijn.
- **Ondersteunende documentatie:** beleid, processen, werkinstructies en andere ondersteunende documenten.
- **Controls (Annex A):** een catalogus met 93 mogelijke controls om risico's te mitigeren, gerangschikt in vier thema's: organisatorisch, menselijk, fysiek en technologisch.
- **Registraties en auditrapportages:** vastlegging van controles, afwijkingen, audits en verbeteracties.
- **Management reviews**: periodieke evaluatie door de directie van effectiviteit en voortgang van het ISMS. Dit is een formele bespreking waarbij onder andere de voortgang, beveiligingsincidenten, auditresultaten en verbeterpunten worden bekeken. Doel is strategische bijsturing en het aantonen van commitment van de directie, waardoor het ISMS verbonden blijft met de bedrijfsstrategie.

ISO 27001 maakt gebruik van de gemeenschappelijke structuur voor ISO-managementsystemen (Annex L), wat inhoudt dat onderdelen zoals context, scope, planning en verbetercyclus vergelijkbaar zijn met andere normen zoals ISO 9001 of ISO 14001. Hierdoor worden processen als risicomanagement, interne audits en management reviews herbruikbaar in geval van uitbreiding met andere normen (1).

PDCA – De motor van het ISMS

Een kenmerk van het ISMS is dat het **geen incidenteel project is,** maar een **continu werkend systeem** dat periodiek wordt beoordeeld en aangepast. Dit wordt ondersteund door de PDCA-benadering (Plan-Do-Check-Act) van ISO 27001 (1) (6), die borgt dat informatiebeveiliging dynamisch blijft meebewegen met veranderende risico's, technologieën en bedrijfsdoelen:

1. **Plan-fase:** in deze fase worden de risicoanalyse uitgevoerd, informatiebeveiligingsdoelstellingen vastgesteld en de **V**erklaring **v**an **T**oepasselijkheid (**VvT**) opgesteld met de te implementeren beheersmaatregelen.
2. **Do-fase:** de in de VvT gekozen controls uit Annex A worden geïmplementeerd en medewerkers worden getraind om de maatregelen effectief toe te passen.
3. **Check-fase:** de effectiviteit van het ISMS wordt periodiek gecontroleerd via interne audits, monitoring en de directiebeoordeling.
4. **Act-fase:** op basis van deze evaluaties worden afwijkingen en non-conformiteiten gecorrigeerd en verbetermaatregelen doorgevoerd, zodat het ISMS continu verbetert.

Deze cyclische en gestructureerde aanpak zorgt ervoor dat het managementsysteem **levend blijft** en zich kan **aanpassen aan veranderende risico's en eisen**. Belangrijke aandachtspunten hierbij zijn:

- ISO 27001 vereist dat er een **controleschema** wordt ingericht om periodiek alle elementen van het ISMS te toetsen en assessments uit te voeren, zodat je weet dat alles blijft werken zoals gepland (6).
- Incidentbeheer en wijzigingsbeheer zijn integraal onderdeel van de PDCA-cyclus omdat ze bijdragen aan continue verbetering en risicobeheersing. Incidentbeheer richt zich op het tijdig detecteren, melden, analyseren en oplossen van beveiligingsincidenten, waarna de geleerde lessen worden gebruikt om processen en controls te verbeteren. Wijzigingsbeheer zorgt ervoor dat veranderingen aan systemen en processen gecontroleerd worden gepland, beoordeeld, getest, geautoriseerd en gemonitord, zodat risico's beheerst blijven en de integriteit van het ISMS behouden blijft tijdens opeenvolgende PDCA-fasen (6).
- Om de voortgang en samenwerking te borgen, is het aan te bevelen om een **periodiek securityoverleg** in te richten met alle betrokkenen, met een vaste agenda en actielijst om ontwikkelingen te bespreken en acties op te volgen.

Controls en de Verklaring van Toepasselijkheid (VvT)

ISO 27001 bevat in Annex A een catalogus van 93 controls die men kan toepassen om geïdentificeerde risico's te mitigeren. De organisatie bepaalt via de risicoanalyse welke maatregelen relevant zijn. De VvT beschrijft met onderbouwing welke controls zijn gekozen en welke zijn uitgesloten. Het vormt daarmee een verbindend document tussen risicoanalyse en implementatie (1) (2) (6).

De controls kunnen ook gekozen worden op basis van **contractuele of wettelijke eisen**, of omdat ze in de praktijk als best practice gelden. Dit zorgt ervoor dat het ISMS maatwerk blijft en aansluit bij de specifieke context en het risicoprofiel van de organisatie.

Efficiëntie door Tooling en Templates

Om de implementatie en onderhoudskosten laag te houden, zeker bij kleinere organisaties, zijn gestandaardiseerde templates en softwareplatforms zeer nuttig.

Een kant-en-klaar ISO 27001-template biedt een basisstructuur inclusief voorbeeldprocedures en beleid, waardoor organisaties snel van start kunnen. Een dergelijk template bevat doorgaans alle verplichte elementen, zoals beleid, formats voor managementreviews en risicoanalyseformulieren. Het is echter cruciaal dat deze generieke teksten worden aangepast en verrijkt met de concrete afspraken en processen van het eigen bedrijf. Kleine organisaties vullen zo'n template aan met hun eigen HR- en IT-processen en voegen alleen specifieke werkinstructies of controles toe die voortvloeien uit de risicobeoordeling (6).

Ook een centraal samenwerkingsplatform of wiki versnelt zowel het onderhoud als de implementatie. Dit dient als de centrale plek voor alle ISMS-documentatie en actiepunten. Dit zorgt ervoor dat medewerkers eenvoudig toegang hebben tot actuele procedures en beleid, en het voorkomt dat informatie lokaal gaat "verstoffen". Een goed opgezet platform kan taken automatiseren, zoals voortgangsrapportages en reviewafspraken, wat de samenwerking bevordert en het ISMS actueel houdt doordat auditresultaten, incidentmeldingen en documentwijzigingen inzichtelijk en navolgbaar zijn.

Succesfactoren: Leiderschap, Cultuur en Communicatie

Een succesvolle ISO 27001-implementatie is afhankelijk van actieve betrokkenheid van het management en een sterke beveiligingscultuur.

Topmanagement moet **daadwerkelijk leiderschap en commitment tonen** voor het Information Security Management System (ISMS). Dit betekent dat het informatiebeveiligingsbeleid en de doelstellingen integraal worden ondersteund en afgestemd op de bedrijfsstrategie, en dat er voldoende middelen — tijd, budget, personeel en tools — beschikbaar worden gesteld voor implementatie en onderhoud.

Door actief te **communiceren** over het belang van informatiebeveiliging en successen te delen, creëert de directie een cultuur waarin beveiliging serieus wordt genomen en gedragen door de hele organisatie. Niet alleen tijdens de implementatie, maar ook daarna, zodat het hele team begrijpt waarom de certificering nodig is en hoe het hen helpt.

Zonder dit mandaat en voorbeeldgedrag bestaat het risico dat het ISMS stagneert omdat noodzakelijke beslissingen, middelen of veranderingen niet worden geïnitialiseerd of gedragen door de organisatie.

Regelmatige trainingen, nieuwsbrieven en bijeenkomsten houden informatiebeveiliging op de agenda en ondersteunen deze aanpak.

Als **lessons learned** kunnen worden genoemd:

- Leg collega's uit wat ISO 27001 oplevert om **draagvlak** te creëren.
- Toon de **toegevoegde waarde** door te laten zien dat het ISMS het dagelijkse werk makkelijker maakt.
- Blijf inzetten op continue **bewustwording**, want informatiebeveiliging is een marathon, geen sprint.
- **First time right**: neem vanaf het begin de juiste beslissingen bij implementatie van het ISMS.
- Implementatie en onderhoud van ISMS is **teamwork**. Goede samenwerking met sleutelfiguren (HR, IT, sales) zorgt ervoor dat het ISMS aansluit bij de dagelijkse praktijk en realistisch en praktisch uitvoerbaar is. Door de kennis en het mandaat van verschillende afdelingen te benutten, wordt beveiliging de **gezamenlijke verantwoordelijkheid** van alle collega's.

Het Certificeringstraject en Continuïteit

ISO 27001 is geen eenmalige prestatie, maar een continu beheersproces, gestructureerd rond een **vaste driejarige auditcyclus** (2). Dit garandeert dat het ISMS actief wordt onderhouden volgens het PDCA-principe. De cyclus verloopt als volgt:

1. **Jaar 1: Initiële Certificeringsaudit:** deze audit bestaat uit twee fasen. Fase 1 beoordeelt de compleetheid en opzet van het ISMS (documentbeoordeling). Fase 2 beoordeelt de praktische werking en naleving van alle processen en beheersmaatregelen (implementatiebeoordeling). Bij een positief resultaat wordt het certificaat voor drie jaar toegekend.
2. **Jaar 2 en 3: Tussenaudits (Surveillance Audits):** dit zijn verplichte, minder uitgebreide jaarlijkse controles. De focus ligt op het aantonen van het continue onderhoud van het ISMS, het opvolgen van eerder vastgestelde afwijkingen, en het uitvoeren van essentiële processen zoals de Directiebeoordeling en Interne Audits. Als deze succesvol zijn, blijft het certificaat geldig.
3. **Einde Jaar 3/Begin Jaar 4:** hercertificeringsaudit: Dit is opnieuw een uitgebreide audit, vergelijkbaar met Fase 2. Hier wordt de algehele volwassenheid en effectiviteit van het complete ISMS getoetst. Bij goedkeuring wordt de cyclus verlengd en begint deze opnieuw.

De driejarige cyclus verzekert belanghebbenden dat de organisatie informatiebeveiliging ziet als een continu beheersproces en niet als een tijdelijk project. De norm vereist hiervoor het plannen van voortdurende interne audits en management reviews.

Een ISO 27001-certificaat brengt blijvende financiële en structurele verplichtingen met zich mee. Organisaties moeten jaarlijks budget reserveren voor onderhoud. Dit omvat de jaarlijkse interne en externe audits, de kosten voor tools voor monitoring en de tijdsinvestering van medewerkers voor procesverbeteringen en risicorondes. De norm vereist dat men leert van fouten; elke geconstateerde non-conformiteit of beveiligingsincident moet leiden tot corrigerende maatregelen en bijstelling van beleid of processen. Het ISMS moet consistent en gestructureerd worden onderhouden om het beoogde beveiligingsniveau op peil te houden.

Verband met Andere Normen en Wetgeving

Dankzij de gemeenschappelijke Annex L-structuur van ISO-managementsystemen is het voor een klein bedrijf relatief eenvoudig om processen zoals risicomanagement, interne audits en managementreviews; te hergebruiken voor andere normen ,zoals: **ISO 9001 (kwaliteit), ISO 14001 (milieu) of ISO 27701 (privacy)**, zodat de investering in je ISMS meerdere rendementen oplevert (1) (7).

Hoewel ISO 27001 een solide en internationaal erkend fundament legt voor informatiebeveiliging, gaat wet- en regelgeving zoals de **Cyberbeveiligingswet** en Europese **NIS2-richtlijn** verder met verplichte governance-, zorg- en meldplichten voor organisaties die daartoe behoren; ISO 27001 helpt je dan veel voorbereidend werk al op orde te hebben, maar de specifieke wettelijke eisen moet je apart in kaart brengen, zeker als je levert aan klanten die onder die regels vallen (4) (5). Daarnaast kunnen opdrachtgevers specifieke attestaties zoals **SOC 2-rapportages** vragen als bewijs van beheersmaatregelen, vooral in internationale IT-ketens.

In al deze gevallen blijft ISO 27001 waardevol als basis, maar het loont ook te bekijken welke aanvullende **markt- of juridische vereisten** relevant zijn voor jouw bedrijf — want een solide informatiebeveiligingsbeleid opent niet alleen deuren, het houd je ook klaar voor wat er op je afkomt, óók als klein bedrijf (7).

Referenties

1. NEN: Alle info over de ISO-normen en de Annex-L structuur:
   - https://www.nen.nl/ict/digitale-ehtiek-en-veiligheid/cyber-privacy/informatiebeveiliging
   - https://www.nen.nl/veelgestelde-vragen-over-iso-iec-27001
   - https://www.nen.nl/nen-en-iso-iec-27001-2023-en-313608
   - https://www.nen.nl/managementsystemen
2. Duijnborgh Certification: het certificatieproces: https://dbcert.nl/
3. Autoriteit Persoonsgegevens: onderwerpen als AVG en Privacy: https://www.autoriteitpersoonsgegevens.nl
4. Digitale Overheid: Digitale wetgeving en richtlijnen: https://www.digitaleoverheid.nl
5. Ondernemersplein: Informatie en advies van de overheid voor ondernemers: https://ondernemersplein.overheid.nl
6. Instant27001: ISO 27001 norm template: https://instant27001.com/nl/
7. Implementatie ISO 27001 en ISO 9001 bij ViPcom BV: https://www.vipcom.nl