

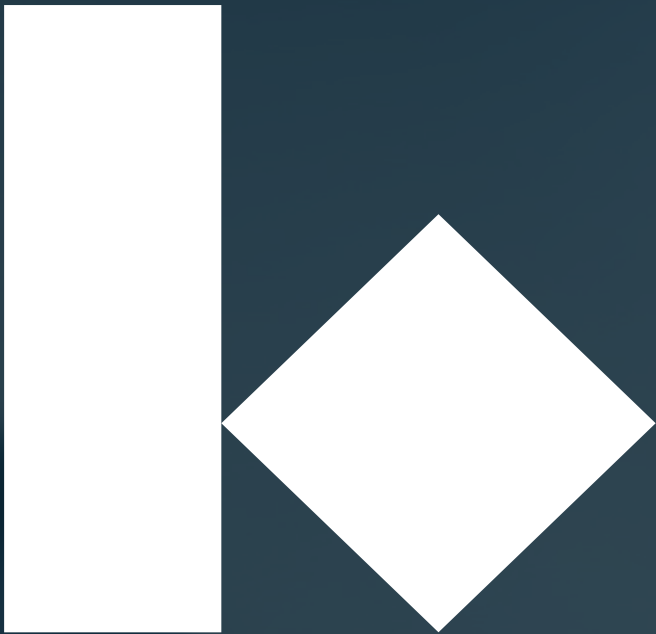


Informatiebeveiliging met ISO 27001 of NEN 7510

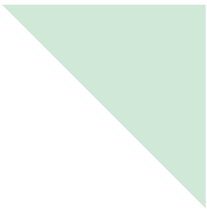
Het wat en waarom van een Information Security
Management System (ISMS)

Bekijk het op
kader.nl

 **kader**
Consultancy & Interim



Bekijk het op
kader.nl



In de brochure vind je

Waarom is het belangrijk om je informatie te beveiligen?	4
Informatiebeveiliging: in elke branche anders	5
Normen beter bekeken	7
Een ISMS implementeren: de 5 stappen van Kader	9
IJzersterke informatiebeveiliging met een ISMS	10
Over Kader Group	11
Ook interessant voor jou?	12

Contact

Heb je na het lezen van de informatie nog vragen, of wil je een offerte aanvragen?
Neem dan gerust contact met ons op.

Telefoonnummer 088 – 99 51 320
kader.nl | sales@kader.nl

Wij helpen je graag!

Waarom is het belangrijk om je informatie te beveiligen?

Cyberincidenten zijn in ons sterk gedigitaliseerde land aan de orde van de dag. Een vlugge blik op de website [DataLekt.nl](https://www.datalekt.nl) en je vindt meldingen van een 1-miljoen-kostende cyberaanval bij een aardappelveredelaar, diefstal van gevoelige documenten bij het Internationaal Strafhof, een ransomware-aanval bij een groot wellnesscentrum en een vervalste digitale factuur bij een gemeente. En – schrik niet – dit vond plaats in een tijdsbestek van één week!

Bovendien is er in toenemende mate wet- en regelgeving die goede beveiliging van persoonsgegevens en bedrijfsinformatie verplicht stelt. Denk maar aan de Algemene Verordening Gegevensbescherming (AVG) of de Europese Netwerk- en Informatiebeveiligingsrichtlijn¹ (NIS2). Hier komt bij dat opdrachtgevers of afnemers soms eisen stellen aan informatiebeveiliging. Ook is er bij organisaties vaak een interne wens om de beveiliging van gegevens te waarborgen. Beveiliging is immers ook onderdeel van de kwaliteit van je dienstverlening.

Wat is een Information Security Management System?

Om er zeker van te zijn dat informatieveiligheid binnen jouw organisatie goed geregeld is én continu aandacht krijgt, kun je een Information Security Management System (ISMS)

implementeren. Dit kun je doen aan de hand van één van deze standaarden:

- ISO 27001, een internationale, generieke norm voor informatiebeveiliging.
- NEN 7510, een Nederlandse norm voor informatieveiligheid in de zorg.
- NIST Cybersecurity Framework, een Amerikaanse norm voor informatiebeveiliging.
- IEC 62443, een internationale norm voor beveiliging van industriële cybersecurity.

Hoewel de standaarden qua doelgroep en invulling wat van elkaar verschillen, is de uitkomst na implementatie altijd: een managementsysteem voor informatiebeveiliging. Een managementsysteem is een combinatie van afspraken en maatregelen in de organisatie waardoor je de continue verbetering (Plan-Do-Check-Act) institutionaliseert en borgt, waarbij afspraken en maatregelen worden gedocumenteerd en resultaten geregistreerd. Een ISMS is interessant voor alle soorten organisaties: van groot tot klein en van voedselabrikanten tot ziekenhuizen. In deze whitepaper gaan we dieper in op het wat en waarom van een ISMS.

In deze whitepaper

- ✓ *Informatiebeveiliging: in elke branche anders*
- ✓ *Normen beter bekeken*
- ✓ *Een ISMS implementeren: de 5 stappen van Kader*
- ✓ *De voordelen van een ISMS*

¹ <https://www.digitaleoverheid.nl/overzicht-van-alle-onderwerpen/nis2-richtlijn/>



Informatiebeveiliging: in elke branche anders

Elk domein kent zijn unieke uitdagingen en risico's. Hieronder belichten we de meest voorkomende risico's in verschillende sectoren.

Maakindustrie

De maakindustrie kampt met specifieke risico's zoals diefstal van intellectueel eigendom, bedrijfsspionage en aanvallen op industriële besturingssystemen (ICS/SCADA). De productieafhankelijkheid van digitale processen maakt deze sector kwetsbaar voor cyberaanvallen die productielijnen kunnen stilleggen.

Zorg

In de zorgsector is de beveiliging van patiëntgegevens cruciaal. Risico's omvatten ongeoorloofde toegang tot persoonsgegevens, ransomware-aanvallen op ziekenhuissystemen, en datalekken door verouderde technologie.

Overheid

Overheidsinstanties moeten omgaan met een breed scala aan informatieveiligheidsrisico's, waaronder geavanceerde aanhoudende bedreigingen (APT's), phishing-aanvallen en datalekken met gevoelige burgerinformatie. Ook hebben overheden te maken met het (digitaal) beveiligen van essentiële infrastructuur, zoals watervoorziening, bruggen en sluizen. De vertrouwelijkheid, integriteit en beschikbaarheid van overheidsdiensten staan hier op het spel.

Financiële dienstverlening

Banken en financiële instellingen zijn een populair doelwit van cybercriminaliteit, inclusief fraude, datalekken en DDoS-aanvallen. De financiële sector is bovendien gebonden aan strikte regelgeving rondom dataprivacy en cybersecurity.

Logistiek

In de logistieke sector ligt de focus op het volgen en beveiligen van de goederenstroom, bescherming tegen onderschepping van vracht, en het waarborgen van de integriteit van de toeleveringsketen. Cyberaanvallen op logistieke systemen kunnen leiden tot aanzienlijke verstoringen en tot het verlies van bedrijfskritische gegevens.

Detailhandel

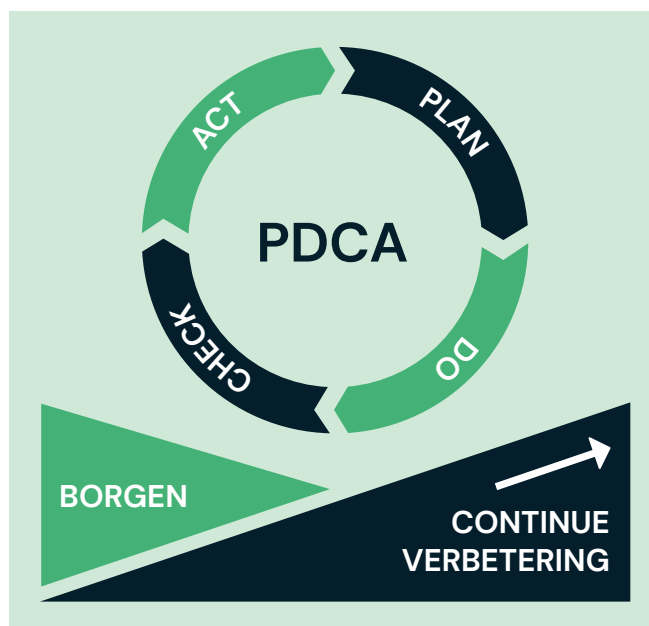
Voor de detailhandel zijn punten van zorg onder meer creditcardfraude, diefstal van klantgegevens en inbreuken op e-commerce-platformen. Deze sector moet extra waakzaam zijn voor de integriteit van POS (Point Of Sale) systemen en online betaalverkeer.

Omdat we vanuit Kader al deze branches (én bedrijven uit andere sectoren!) begeleiden bij ISMS-implementaties, zijn we goed op de hoogte van deze en andere veelvoorkomende branchespecifieke risico's. En: met de best practices. Hierdoor kunnen we op een pragmatische manier adviseren over relevante beheersmaatregelen. Dat kunnen zowel preventieve maatregelen zijn, als detectieve of corrigerende maatregelen. Hierbij is de boodschap: *één maatregel is geen maatregel*. Naast IT-maatregelen, moet je ook kijken naar maatregelen bij leveranciers/partners, HR-beleid en de fysieke beveiliging van gebouwen: kunnen buitenstaanders bijvoorbeeld zomaar een kantoor binnenlopen en een blik werpen op papieren met belangrijke informatie die ergens op een bureau liggen?



Plan – Do – Check – Act

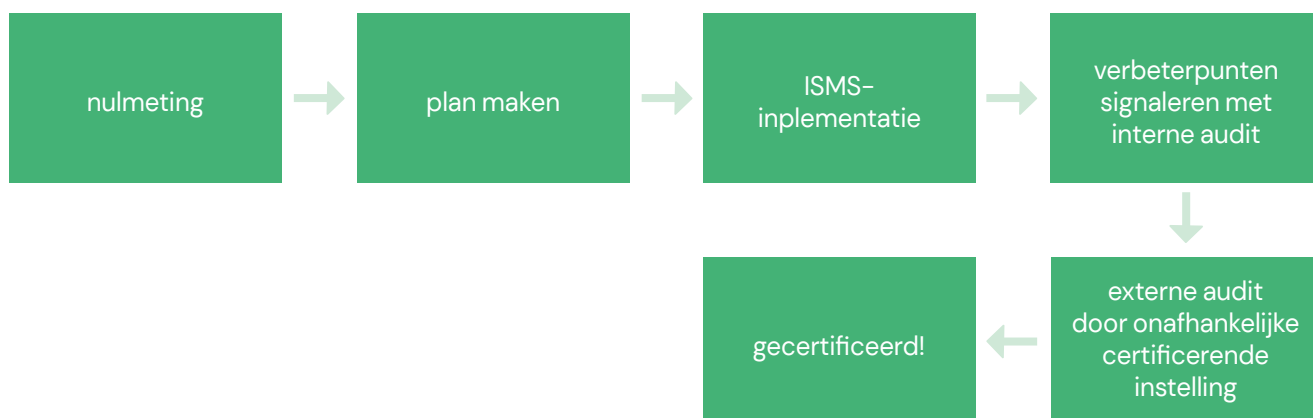
Eenmalige maatregelen nemen is niet genoeg. De wereld verandert immers continu. Een ISMS gaat daarom uit van de zogenaamde PDCA-cyclus (Plan, Do, Check, Act). Je kijkt hierbij naar cyberwetgeving en –dreigingen van buitenaf én naar behoeften van binnenuit. Waar wil de organisatie naartoe? Welke processen en aspecten zijn daarbij bedrijfskritisch en moeten in kaart gebracht worden (*plan*)? Wat moet je verbeteren en hoe reageer je adequaat op beveiligingsincidenten (*do*)? Zijn de risicoanalyses aanwezig en is de beveiliging op orde (*check*)? En waar moet er bijgestuurd en aangescherpt worden (*act*)? Continu anticiperen en verbeteren is het uitgangspunt om goed te kunnen acteren op steeds veranderende dreigingen.



Voortdurend verbeteren met een certificeringscyclus

Ook het certificeringsproces is cyclisch: een ISMS is niet iets dat je in één keer implementeert en waarmee je daarna 'klaar bent'. De certificeringscyclus ziet er als volgt uit:

Na een nulmeting en het maken van een plan, start de **ISMS-implementatie** → Hierna signaleer je verbeterpunten met een **interne audit** → En doet een certificerende instelling een **externe audit** → Gefeliciteerd, je organisatie is nu **gecertificeerd!** → Daarna controleer je jaarlijks of je nog aan de eisen van de norm voldoet, of iedereen zich aan de gemaakte procesafspraken houdt en of er iets verbeterd kan worden met een **interne audit** → Elke drie jaar wordt je managementsysteem volledig onder de loep genomen door de certificerende instelling om je te **hercertificeren** voor de volgende drie jaar. Op deze manier weet je dus echt zeker dat je continu aan (nieuwe) eisen en regelgeving voldoet en dat je voortdurend blijft verbeteren!



Normen beter bekeken

Heel fijn bij het opstellen van een ISMS: je hoeft het wiel niet opnieuw uit te vinden. Er zijn namelijk nationale en internationale standaarden die je organisatie helpen bij het inrichten van een ISMS. De bekendste standaarden zijn ISO 27001, NEN 7510, het NIST-raamwerk en IEC 62443. Deze standaarden geven je een goede leidraad bij het inrichten van je PDCA-cyclus en bij het nemen van specifieke beveiligingsmaatregelen.

ISO 27001

ISO 27001 is een internationale norm die wereldwijd erkend is en toegepast wordt. De norm is ontwikkeld door ISO, de International Standardization Organization. Met ISO 27001-certificering maak je aantoonbaar dat je organisatie **informatieprocessen** continu beheerst en dat je de vertrouwelijkheid, integriteit en beschikbaarheid van bedrijfskritische informatie borgt. De norm is zo opgebouwd dat het niet uitmaakt of jouw organisatie in de maakindustrie zit, een overheidsinstelling is of een zakelijk dienstverlener. ISO 27001 is te implementeren in alle soorten organisaties: groot of klein.

NEN 7510

Zorginstellingen en beheerders van persoonlijke gezondheidsinformatie kiezen vaak voor NEN 7510. Deel 1 van NEN 7510 heeft dezelfde basis als ISO 27001: het borgen van de vertrouwelijkheid, integriteit en beschikbaarheid van bedrijfskritische informatie. Deel 2 is een aanvulling op ISO 27001 en legt de focus op **persoonlijke gezondheidsinformatie**.

NEN 7510 is een Nederlandse norm. In de Nederlandse wet staat namelijk dat patiëntgegevens op een adequate manier moeten worden beveiligd. De Inspectie Gezondheidszorg en Jeugd gebruikt NEN 7510 voor het toetsen op die adequate informatiebeveiliging bij alle Nederlandse organisaties die patiëntgegevens verwerken. Dan kun je denken aan ziekenhuizen of tandartsen, maar ook bijvoorbeeld IT-bedrijven of marketingbureaus met zorginstellingen als klant. Het certificeren volgens de norm is niet verplicht, maar het voldoen aan de eisen uit NEN 7510 wél.

NIST-raamwerk

Het NIST Cybersecurity Framework, ooit bedoeld voor Amerikaanse overheidsinstanties, is opgezet door het National Institute of Standards and Technology. Het model is deels gebaseerd op andere standaarden zoals ISO 27000, maar ook de CIS Critical Security Controls en COBIT. Inmiddels is het ook populair buiten de Verenigde Staten bij zowel kleine als grotere bedrijven. Organisaties leren met het NIST-raamwerk cyberbeveiligingsrisico's beter te begrijpen, beheren en verminderen, als ook hun netwerken en gegevens te beschermen.

Een groot verschil met andere ISMS-standaarden is dat het NIST-model **niet een certificeerbare norm** is. Er is geen sprake van een eisenpakket, audits en een certificaat. Het voordeel hiervan is, dat je wél de structuur van een ISMS hebt, maar ook veel flexibiliteit.

IEC 62443

IEC 62443 is een internationale standaardreeks die zich richt op de beveiliging van **industriële controlesystemen (ICS)**. Zulke systemen worden gebruikt bij operationele technologie en kritieke infrastructuren binnen onder andere de productie-, energie- en transportsector. De standaard is ontwikkeld door de International Electrotechnical Commission (IEC). IEC 62443 bevat richtlijnen en best practices voor systemen tegen cyberdreigingen en voor het beschermen van industriële netwerken. Door de richtlijnen van deze standaard te volgen, kunnen bedrijven kwetsbaarheden verminderen en de betrouwbaarheid en integriteit van hun industriële controlesystemen verbeteren.

Daarnaast zijn er nog normen die niet tot een ISMS leiden, maar waarbij informatiebeveiliging wél een rol speelt. Hieronder lees je op welke gebieden al deze standaarden overeenkomen, en waarin ze van elkaar verschillen.

ISO 27701

ISO 27701-certificering toont aan dat je bewust omgaat met **privacy en persoonsgegevens** en deze veilig verwerkt. ISO 27701 is een certificeerbare uitbreiding op de ISO 27001-norm. Deze uitbreiding bevat richtlijnen en eisen voor inrichting, implementatie, onderhoud en het continu verbeteren van een Privacy Information Management System (PIMS). Met een ISO 27701-certificaat voldoe je ook aan eisen uit de Algemene Verordening Gegevensbescherming (AVG). De ISO 27701-certificering verduidelijkt daarnaast rollen en verantwoordelijkheden binnen de organisatie.

ISO 9001

De bekende ISO-norm 9001 is een **kwaliteitsmanagementsysteem** (ook wel KMS genoemd), waarbij de eisen van de klant en klanttevredenheid centraal staan. In een KMS staat precies welke processen en activiteiten van belang zijn. Dat is waardevolle informatie voor een ISMS omdat je hiermee meteen kunt bepalen welke data kritisch is. ISO 9001 en ISO 27001/NEN 7510 vullen elkaar dus aan! Bovendien: niet leveren, deels leveren of te laat leveren door een cyberincident, staat gelijk aan slechte kwaliteit leveren. Informatieveiligheid is dus onlosmakelijk verbonden met kwaliteitsmanagement.

ISO 22301

Een BCMS volgens ISO 22301 is een **bedrijfscontinuïteitsmanagementsysteem**. Hiermee breng je als organisatie de belangrijkste risico's in kaart voor wanneer zich een crisissituatie of calamiteit voordoet. Bij certificatie wordt door steekproeven beoordeeld of jouw bedrijf een compleet overzicht van alle risico's heeft, optimaal voorbereid is op ernstige verstoringen en uitzicht heeft op een snel herstel, met beperkte schade. Die verstoringen kunnen trouwens van alles zijn: van een gebouwbrand tot een griepgolf. Incidenten rondom informatieveiligheid vallen er ook onder.

Normen combineren: een goed idee

ISO 27001/NEN 7510, ISO 27701, ISO 9001 en ISO 22301 zijn zogenoemde managementsysteemnormen, en hebben een [Harmonized Structure](#). Dit betekent dat ze zijn ontwikkeld volgens het zogenaamde plug-in-model. Hierdoor sluiten de normen aan op een set kerneisen die voor al die normen hetzelfde is. Implementeer je meerdere van deze HS-normen binnen jouw organisatie? Dan zorgt de vaste opbouw voor een integrale benadering, betere procesbeheersing, grotere flexibiliteit en een sterkere focus op risicomanagement.



Een ISMS implementeren: de 5 stappen van Kader

Kader begeleidt jouw organisatie in vijf praktische stappen naar ISMS-certificering, waarbij we de (inter)nationale standaarden als leidraad gebruiken, maar bovenal uitgaan van de (primaire) processen van jouw organisatie. Door de dienstverlening en processen van jouw organisatie centraal te stellen bij het inrichten van het ISMS, ben je namelijk nog meer in staat om de juiste beveiligingsmaatregelen te nemen. Zonder een papieren 'compliance tijger' te creëren.



Stap 1: nulmeting

De eerste stap is het fundament van het verdere stappenplan: de nulmeting. We beoordelen in hoeverre jouw organisatie al invulling geeft aan de betreffende ISMS-standaard. Wat is de intrinsieke motivatie om de informatiebeveiliging te verbeteren? Wat is het beleid? En wat wordt er al gedaan en gerapporteerd? Verder kunnen jouw werknemers door deze nulmeting alvast kennismaken met de inhoud en de reikwijdte van het ISMS. We bespreken verschillende processen, procesbeschrijvingen, procedures en instructies en toetsen die aan de bijbehorende standaard: ISO 27001, NEN 7510 of het NIST-raamwerk. Kader kijkt hierbij naar de bedrijfsprocessen die specifiek zijn voor jouw organisatie en neemt ook mee wat er georganiseerd is op andere vakgebieden, zoals kwaliteit of machineveiligheid. De resultaten verwerken we in een rapportage en een plan van aanpak.

Na de nulmeting weet je precies waar je aan toe bent en kun je besluiten of je je door Kader wil laten begeleiden naar de ISMS-implementatie. Je hebt inzicht in de verwachte tijdsbesteding, taakverdeling en kosten van eventuele certificering.

Stap 2: managementsysteem

De volgende stap is het opzetten van het ISMS. Wij zetten een praktisch hanteerbaar en efficiënt managementsysteem op dat voldoet aan de ISMS-standaard, geldende wet- en regelgeving én aan de behoefte van jouw organisatie. Kies je

voor ISO 27001 of NEN 7510? Door de Harmonized Structure is het makkelijker om te integreren met andere ISO-normen en met branche-specifieke richtlijnen. Ook kiezen we samen de meest geschikte ISMS-tooling voor jouw organisatie.

Stappen 3, 4 en 5: op naar het certificaat

Bij certificeerbare normen zoals ISO 27001 en NEN 7510 vervolgen we het stappenplan met drie stappen, op weg naar het certificaat. Stap 3: we toetsen door middel van een interne audit of het managementsysteem goed is ingevoerd. Dan volgt stap 4: de management review. Kader brengt samen met het management in kaart wat de verbetermogelijkheden zijn en welke middelen er zijn om die verbeteringen te realiseren. Tenslotte volgt de laatste stap uit het ISO-stappenplan: de begeleiding naar certificering. Kader is approved partner van een aantal gerenommeerde certificatie-instellingen. Door onze goede contacten met deze organisaties kunnen we helpen de certificatie zo snel en soepel mogelijk te laten verlopen.

Is structurele hulp bij audits of bij het up-to-date houden van het ISMS welkom? Kader-adviseurs ondersteunen je graag. Dat kan een paar dagen per jaar, of misschien wel wekelijks: maar net wat jouw organisatie nodig heeft.

IJzersterke informatie-beveiliging met een ISMS

Het proces om tot een ISMS te komen, vergt nog best wat werk. Waarom zou je zo'n systeem willen implementeren? Eigenlijk zijn er twee hoofdredenen. De eerste is meer extrinsiek: een ISMS wordt soms als harde voorwaarde gesteld door een opdrachtgever of afnemer. De tweede meer intrinsiek: je wil de veiligheid van gegevens kunnen garanderen en ziet dit als een vorm van kwaliteitswaarborging. Bovendien: als je níét voorbereid bent en niet goed reageert op een cyberincident, zou het wel eens kunnen dat het bedrijf de (financiële) gevolgen niet kan dragen.

Wat levert een ISMS nog meer op, als het goed is geïmplementeerd? Dat zetten we hieronder voor je op een rij.

- **Verbeterde reputatie en vertrouwen:** Een gecertificeerd ISMS versterkt het vertrouwen van klanten (of inwoners/patiënten etc.), partners en stakeholders. Dit kan leiden tot meer zakelijke kansen en een concurrentievoordeel.
- **Risicobeheersing:** Een ISMS helpt bij het systematisch identificeren, beoordelen en beheren van informatiebeveiligingsrisico's, waardoor je de impact van eventuele beveiligingsincidenten minimaliseert.
- **Voldoen aan wettelijke en contractuele verplichtingen:** Een ISMS zorgt ervoor dat jouw organisatie aantoonbaar voldoet aan relevante wet- en regelgeving, zoals de AVG, en aan de eisen van klanten of andere externe partijen. ISO 27001- of NEN 7510-certificering kan toegang tot nieuwe opdrachtgevers opleveren.
- **Bewustwording en betrokkenheid bij medewerkers:** Door de implementatie van een ISMS worden medewerkers zich meer bewust van de risico's en hun rol in het beveiligen van informatie. Dit bevordert een cultuur van veiligheid binnen de organisatie.
- **Continu verbeterproces:** De PDCA-cyclus (Plan-Do-Check-Act) waarop een ISMS is gebaseerd, stimuleert continue verbetering van processen en veiligheidsmaatregelen.

- **Financiële voordelen:** Door het voorkomen van hacks, datalekken en andere beveiligingsincidenten, vermijd je hoge boetes, verlies van bedrijfsmiddelen en (herstel) kosten. Met andere woorden, het levert directe én indirecte financiële voordelen op.
- **Aanpasbaar en schaalbaar:** Een ISMS is flexibel en kan worden aangepast aan de veranderende omvang, structuur en behoeften van een organisatie, waardoor het een duurzame oplossing is.
- **Verhoogde operationele efficiëntie:** Heb je naast een ISMS ook een Privacy Information Management System (PIMS), Kwaliteitsmanagementsysteem (KMS) of Bedrijfscontinuïteitsmanagementsysteem (BCMS)? Vanuit één Integrated Management System (IMS) kun je alle invalshoeken meenemen: van kwaliteit tot bedrijfscontinuïteit en van veilig werken tot informatieveiligheid en privacy. Organisaties die op zo'n integrale manier werken, besparen vaak een hoop tijd, geld en moeite.
- **Digitale efficiëntie:** Kies je voor een digitaal ISMS, dan levert je dat veel extra efficiëntie op. ISMS-tooling met cloudfunctionaliteit maakt alle templates, beleidsstukken, processen, documenten en actiepunten online toegankelijk voor de juiste medewerkers (afhankelijk van iemands rol). Goede systemen waarmee je zo'n digitaal ISMS kunt inrichten, zijn onder andere SmartManSys en Confluence.

Kortom: met een ISMS verhoog je niet alleen de beveiliging van informatie, maar verbeter je de algehele bedrijfsvoering binnen jouw organisatie.

Benieuwd hoe een ISMS voor jouw organisatie zou kunnen werken? We gaan er graag met je over in gesprek.

Contact



Vanuit één IMS kun je alle invalshoeken meenemen: van kwaliteit tot bedrijfscontinuïteit en van veilig werken tot informatieveiligheid en privacy. Organisaties die op zo'n integrale manier werken, besparen vaak een hoop tijd, geld en moeite.



Over Kader Group

Kader Group verbetert de kwaliteit, veiligheid en duurzaamheid van organisaties, zodat een ieder goed kan zorgen voor mens, milieu en maatschappij. Dat doen we met onze consultancy & interim diensten, digitale oplossingen en opleidingen op de gebieden kwaliteit, veiligheid & gezondheid, cyber security en milieu & duurzaamheid. Onze missie: het creëren van een veilige en duurzame leefomgeving om door te geven aan toekomstige generaties. We zijn daarin pragmatisch, innovatief, persoonlijk en vakkundig. Kader Group startte in 1994 en bestaat inmiddels uit ruim 350 gedreven medewerkers.

Ook interessant voor jou?

Wil je jouw kennis verbreden of verdiepen?

Wellicht zijn onderstaande onderwerpen interessant voor jou!



Whitepaper

Kansen & bedreigingen omtrent AI

Ben je verantwoordelijk voor het beschermen van persoonsgegevens of bedrijfskritische data? Dan volg je ongetwijfeld de ontwikkelingen rondom artificial intelligence (AI). Of je nu bij de overheid werkt, in de zorg, bij een commercieel bedrijf, of in de industrie: overal wordt tegenwoordig wel met AI gewerkt. De impact van AI is dus enorm. Maar wat zijn de voordelen, waar zitten de risico's en hoe voorkom je dat jouw organisatie de grip kwijtraakt op het gebruik van AI? Je leest het in deze whitepaper.

Meer informatie



Cursus

Informatiebeveiliging

Informatiebeveiliging is hot, want we zien steeds vaker incidenten voorbijkomen. En ieder bedrijf heeft wel waardevolle informatie in huis die beschermt moet worden. Met deze driedaagse cursus leer je de informatiebeveiliging binnen jouw bedrijf op een pragmatische manier verbeteren, op basis van de ISO 27001 of de NEDN 7510 norm. We stemmen de cursus af op de behoefte die speelt binnen jouw organisatie.

Meer informatie



Blog

Krijgt mijn organisatie straks te maken met de nieuwe NIS2-richtlijn?

Op 17 oktober 2024 treedt de nieuwe NIS2-richtlijn voor netwerk- en informatiebeveiliging in werking. Want door een groeiende zorg over toenemende cyberdreigingen én de maatschappelijke afhankelijkheid van IT, zijn strengere EU-eisen nodig. Valt jouw organisatie onder deze richtlijn en welke stappen moet je dan ondernemen? Lees het in deze blog!

Meer informatie



