MANAGEMENTGIDS / EDITIE 2027

Aantoonbare compliance in 2027

Van voldoen naar aantonen, zonder extra complexiteit.

Een managementgids voor bestuurders, CISO's, IT-managers, privacy officers en compliance officers

01

Beleid

Wat geldt er, en waarom?

02

Toegang

Wie mag wat, en hoe lang?

03

Gebruik

Werkt het in de dagelijkse praktijk?

04

Bewijs

Kunnen we het vandaag laten zien?

Wetgevingskalender 2027, een vierlagenmodel, een zelfbeoordeling en een roadmap per kwartaal.

MANAGEMENTSAMENVATTING

Compliance wordt in 2027 een bewijsvraag

Beleid hebben is niet meer genoeg. Toezichthouders, auditors en klanten vragen of u kunt laten zien dat uw maatregelen elke dag werken.

Met de Cyberbeveiligingswet en de Wet weerbaarheid kritieke entiteiten, beide van kracht sinds 15 augustus 2026, is 2027 het eerste volledige jaar waarin de Nederlandse uitwerking van NIS2 en CER geldt. DORA is voor de financiële sector inmiddels staande praktijk. Eind 2027 volgen de hoog-risicoregels van de AI Act en de hoofdverplichtingen van de Cyber Resilience Act.[1][3][4][5]

AI die kaders stellen in de kern dezelfde vraag: kunt u aantonen wie toegang had, wat er is gedeeld, welk beleid gold en wanneer is ingegrepen? Deze gids helpt u die vraag te beantwoorden zonder extra bureaucratie. Begin daarom met vijf besluiten.

Besluit	Wat u vastlegt
Scope	Welke wetten op uw organisatie van toepassing zijn, en voor welke diensten en ketenpartners.
Eigenaarschap	Eén eigenaar per controle, met mandaat en een vaste plek in de bestuursagenda.
Kapstok	Eén GRC- of ISMS-omgeving waarin beleid, risico's, controles en bewijs samenkomen.
Uitwisseling	Een vaste, gecontroleerde route voor het delen van gevoelige informatie met externe partijen.
Bewijsritme	Hoe vaak u de werking toetst, en hoe snel bewijs beschikbaar moet zijn voor een auditor.

In deze gids

01 Het vraagstuk 02
02 Wat er in 2027 verandert 03
03 De complianceparadox 04
04 Complexiteit en schaduw-IT 05
05 Beleid 06
06 Toegang 07
07 Gebruik 08
08 Bewijs 09
09 De bewijsketen 10
10 Zelfbeoordeling 11
11 Roadmap 2027 12
12 De rol van Msafe 13

Leesroute: bestuurders lezen pagina 1 tot en met 5 en de roadmap op pagina 12. Het werkblad op pagina 11 is bedoeld voor de eigenaar van een documentstroom.

01 / HET VRAAGSTUK

Van voldoen naar aantonen

De kernvraag verschuift. Niet meer "voldoen we?", maar "kunnen we dat elke dag laten zien, met objectief bewijs?".

Wat is aantoonbare compliance?

Aantoonbare compliance is de mate waarin een organisatie met objectief bewijs kan laten zien dat haar maatregelen werken. Het gaat niet om de vraag of er beleid is, maar of u kunt reconstrueren wat er is gebeurd: welke controle gold, wie toegang had, welke actie is uitgevoerd en met welk resultaat.

Dat bewijs bestaat uit logs, audit trails, rapportages en vastgelegde besluiten. Hoe meer daarvan automatisch ontstaat in het dagelijkse werk, hoe minder tijd u kwijt bent aan het achteraf verzamelen ervan.

Waarom het een bestuursvraagstuk is

De Cyberbeveiligingswet legt de eindverantwoordelijkheid nadrukkelijk bij het bestuur. Bestuurders moeten de maatregelen goedkeuren, toezien op de uitvoering en zelf een training volgen.[1] DORA kent een vergelijkbare lijn voor financiële instellingen.[3]

Daarmee is bewijs geen taak meer van alleen IT of compliance. Het bestuur moet zelf kunnen uitleggen welke risico's het accepteert en waarom.

Wie om bewijs vraagt

Bewijs is niet alleen voor de toezichthouder. Ook klanten, verzekeraars en ketenpartners vragen er steeds vaker om, bijvoorbeeld in aanbestedingen en leveranciersbeoordelingen. Wie bewijs op orde heeft, wint daarmee ook tijd in de verkoop.

Vrager	Typische vraag	Bewijs dat overtuigt
Toezichthouder	Zijn de maatregelen passend en werken ze?	Risicoanalyse, besluiten, testresultaten en incidentdossiers.
Auditor	Werkt deze controle over de hele periode?	Logs en rapportages per controle, met datum en eigenaar.
Klant of ketenpartner	Hoe gaat u om met onze gegevens?	Certificering, verwerkersafspraken en een audit trail per overdracht.
Bestuur	Welk restrisico accepteren wij?	Een actueel overzicht per controle, met open punten en besluiten.

02 / WETGEVING EN TIJDLIJN

Wat er in 2027 verandert

2027 is geen jaar van nieuwe wetten, maar van toetsing. De regels liggen er. Nu volgt de vraag of ze in de praktijk werken.

15 aug 2026
VAN KRACHT

Cyberbeveiligingswet en Wet weerbaarheid kritieke entiteiten. Registratie bij het NCSC is verplicht.[1][2]

11 sep 2026
VAN KRACHT

Meldplicht van de Cyber Resilience Act voor fabrikanten van producten met digitale elementen.[5]

2 dec 2027
GEPLAND

AI Act: verplichtingen voor zelfstandige hoog-risico-AI-systemen (bijlage III).[4]

11 dec 2027
GEPLAND

Cyber Resilience Act: de meeste verplichtingen gaan gelden.[5]

Kader	Status november 2026	Wat u in 2027 moet kunnen aantonen
Cbw (NIS2)	Van kracht sinds 15 augustus 2026 voor ruim 8.000 organisaties in 18 sectoren.[1]	Zorgplicht in de praktijk, tijdige meldingen (24 uur, 72 uur, eindrapport binnen een maand) en betrokkenheid van het bestuur.[13]
Wwke (CER)	Van kracht sinds 15 augustus 2026; ongeveer 500 organisaties zijn aangewezen als kritieke entiteit.[1]	Weerbaarheid van de dienstverlening, ook fysiek en in de keten.
DORA	Van toepassing sinds 17 januari 2025 in de financiële sector.[3]	ICT-risicobeheer, incidentrapportage, weerbaarheidstesten en grip op ICT-dienstverleners.
AI Act	Transparantieverplichtingen gelden; hoog-risico uitgesteld door de Digital Omnibus.[4]	Een register van AI-toepassingen en voorbereiding op 2 december 2027 (bijlage III) en 2 augustus 2028 (bijlage I).
CRA	Meldplicht sinds 11 september 2026.[5]	Bij inkoop: eisen aan leveranciers van software en verbonden producten.
AVG	Blijft de basis voor elke verwerking van persoonsgegevens.[6]	Verantwoordingsplicht: passende beveiliging en een sluitend verwerkingsregister.

Peildatum 2 november 2026. Controleer de actuele stand van wet- en regelgeving voordat u besluiten neemt. Deze gids is geen juridisch advies.

03 / DE COMPLIANCEPARADOX

Meer rapportage, minder weerbaarheid

De valkuil van strengere regels is dat organisaties reageren met meer documenten en complexere processen. Dat maakt ze niet veiliger, maar trager.

> "Je kunt niet innoveren in een organisatie die alleen nog bezig is om morgen geen boete te krijgen. We zijn vergeten dat naleving bedoeld is om beter te worden, niet alleen om veilig te blijven."
>
> THIJS VAN DER LINDEN, COO VAN MSAFE

Het mechanisme in de bestuurskamer

Verlies vermijden weegt zwaarder dan de ambitie om te winnen. Boetes, datalekken en reputatieschade zijn concreet. Onder NIS2 kunnen boetes voor essentiële entiteiten oplopen tot 10 miljoen euro of 2% van de wereldwijde jaaromzet.[13] Innovatie voelt daarnaast onzeker.

Het resultaat is een cultuur van risicovermijding in plaats van risicobeheersing. Zo ontstaat een digitale variant van bureaucratie: processen die vooral bestaan om te kunnen aantonen dat ze bestaan.

Wat er dan misgaat

- De aandacht verschuift van detectie naar documentatie.
- Nieuwe technologie blijft hangen in de pilotfase.
- Budget gaat naar audits in plaats van naar preventie.
- Medewerkers zoeken omwegen rond processen die te zwaar zijn.

De les uit het securitydomein

Een systeem kan volledig compliant zijn en toch kwetsbaar. Regels volgen is noodzakelijk, maar niet voldoende. Securityteams sturen daarom op werking, niet op documenten. Dat principe werkt ook voor compliance.

Uit de Chief Ethics and Compliance Officer Survey van KPMG blijkt dat compliance officers van grote Nederlandse bedrijven meer toezicht verwachten, en dat datakwaliteit, privacy en cybersecurity bovenaan hun agenda staan.[11]

Beslisvraag: welke rapportage in uw organisatie bestaat alleen nog omdat hij altijd al bestond, en welk bewijs ontstaat vanzelf in het werk?

04 / COMPLEXITEIT EN SCHADUW-IT

De veilige route moet de makkelijkste zijn

Compliance gaat zelden mis omdat er geen beleid is. Het gaat mis omdat beleid in de praktijk te ingewikkeld wordt.

62%

van de onderzochte datalekken had een menselijke component, zoals een fout, misbruik of social engineering.

Verizon DBIR 2026[8]

£750.000

boete voor de Police Service of Northern Ireland, na het per ongeluk publiceren van gegevens van 9.483 medewerkers.

ICO, oktober 2024[9]

Hoe schaduw-IT ontstaat

Zodra medewerkers moeten werken met omslachtige processen, extra stappen en losse portals, zoeken ze een snellere route. Een privé-cloud, een onbeheerde link of een gratis transferdienst voelt efficiënt. De organisatie verliest daarmee het zicht op toegang, logging en bewaartermijnen. Het Britse NCSC noemt schaduw-IT daarom expliciet een risico.[10]

Mensen zijn niet het probleem

Het hoge aandeel menselijk handelen betekent niet dat medewerkers het probleem zijn. Het betekent dat processen die perfect menselijk handelen vereisen kwetsbaar blijven. In het PSNI-incident stond een verborgen tabblad in een spreadsheet. De toezichthouder benadrukte dat eenvoudige procedures het incident hadden kunnen voorkomen.[9]

Wat bestuurders kunnen doen

- Meet hoeveel stappen de veilige route kost, en vergelijk dat met de onveilige.
- Vraag afdelingen welke tools zij buiten IT om gebruiken, zonder sanctie.
- Maak verbieden pas mogelijk als er een even makkelijk alternatief is.
- Koppel awareness aan het proces, niet aan een jaarlijkse e-learning.

Beslisvraag: als een medewerker vandaag een groot dossier met een externe partij moet delen, welke route kiest hij dan echt?

05 / LAAG 1: BELEID

Begin bij het doel van de controle

Beleid werkt pas als het meetbaar is. Niet de checklist, maar het waarom achter een controle bepaalt de impact.

Leg beleid, risicoregister, controles en eigenaren vast in één GRC- of ISMS-omgeving. Koppel uw controles aan kaders als ISO/IEC 27001 en het NIST Cybersecurity Framework. Zo voldoet u met één set maatregelen aan meerdere wetten, in plaats van per wet een eigen administratie op te bouwen.[7]

Formuleer per controle drie dingen: het doel, de norm en het bewijs. Een controle zonder bewijsdefinitie is een voornemen. Een controle zonder doel wordt een vinkje.

Maak classificatie bruikbaar

Een classificatie met acht niveaus wordt niet gebruikt. Drie of vier niveaus, met per niveau een concrete deelafspraak, werken beter dan een perfecte indeling die niemand kent.

Maak uitzonderingen tijdelijk

Elke uitzondering krijgt een eigenaar, een reden en een einddatum. Een permanente uitzondering is in feite nieuw beleid, en moet ook zo worden besloten.

Beslisvraag	Wat u vastlegt	Bewijs
Welke informatie is kritisch?	Classificatie met maximaal vier niveaus en voorbeelden per niveau.	Gepubliceerde richtlijn en periodieke steekproef.
Hoe lang bewaren we?	Bewaartermijnen per type informatie en per route.	Automatische verwijdering en logregel per verwijdering.
Wat mag niet naar buiten?	Uitgesloten bestandstypen en gegevens, met uitzonderingsproces.	Technische blokkade en register van uitzonderingen.
Wie beslist bij twijfel?	Informatie-eigenaar per domein, met vervanger.	Vastgelegde besluiten met datum en motivering.

Tip: gebruik vaste ID's per controle (bijvoorbeeld BEL-03) in al uw systemen. Zo herleidt u elk logbericht direct naar de maatregel waar het bij hoort.

06 / LAAG 2: TOEGANG

Laat rechten meebewegen

Toegang die niet meer nodig is, moet automatisch verlopen. Handmatig intrekken schiet er in de praktijk bijna altijd bij in.

Bepaal wie bij welke informatie mag, intern en extern. Single Sign-On en MFA zijn de standaard. Met automatische provisioning via SCIM worden accounts aangemaakt, aangepast en verwijderd zodra iemand in dienst komt, van functie wisselt of vertrekt.

Voor externe ontvangers geldt hetzelfde principe: toegang hoort bij een doel en een termijn, niet bij een persoon voor onbepaalde tijd.

Verifieer de ontvanger

Een verkeerd e-mailadres is een van de meest voorkomende oorzaken van datalekken. Een extra verificatiestap voor de ontvanger, zoals een code via de telefoon, maakt het verschil tussen een vergissing en een incident.

Toets de afloop

Controleer niet alleen of toegang wordt verleend, maar ook of hij afloopt. Een steekproef op verlopen links en vertrokken medewerkers levert sterk bewijs op.

Moment	Maatregel	Bewijs
Instroom	Account via SSO en SCIM, rechten op basis van rol.	Provisioninglog met datum en rol.
Doorstroom	Oude rechten vervallen bij functiewissel.	Wijzigingslog en periodieke rechtenreview.
Uitstroom	Account geblokkeerd binnen de afgesproken termijn.	Deprovisioninglog en steekproef.
Externe ontvanger	Verificatie, vervaldatum en intrekbare toegang.	Audit trail per overdracht en per ontvanger.
Beheerder	Aparte beheeraccounts met MFA en logging.	Beheerlog en kwartaalreview.

07 / LAAG 3: GEBRUIK

Kies de route op controlebehoefte

Hier ontstaan de meeste risico's: in de dagelijkse samenwerking met klanten, leveranciers, auditors en ketenpartners.

Elke route heeft een eigen sterkte. E-mail is geschikt voor communicatie, een samenwerkingsplatform voor intern werk. Voor het delen van gevoelige informatie met externe partijen is een route nodig die toegang, termijn en logging centraal regelt.

Kies werkwijzen die naadloos in het dagelijkse werk passen. Kan een medewerker vanuit zijn eigen mailprogramma veilig delen, dan heeft hij geen reden om uit te wijken naar een bijlage of een gratis dienst.

Maak grote bestanden geen uitzondering

Bouwtekeningen, medische beelden en due-diligencedossiers zijn vaak te groot voor e-mail. Juist daar ontstaan omwegen. Zorg dat de veilige route ook de grote bestanden aankan.

Train herkenbare afwegingen

Oefen met echte situaties: een verzoek van een onbekend adres, een haastige auditor, een dossier met bijzondere persoonsgegevens. Dat werkt beter dan algemene regels.

Route	Primair gebruik	Controlevraag
E-mailbijlage	Communicatie, kopie in mailbox	Wat gebeurt er na verzending, en wie stuurt het door?
Samenwerkingsplatform	Samen werken aan documenten	Wie houdt welke gastentoegang bij, en hoe lang?
Secure file transfer	Gevoelige uitwisseling met externen	Welke vervaldatum, verificatie en audit trail gelden?
Gratis transferdienst	Niet goedgekeurd	Waarom kozen medewerkers deze route, en wat ontbrak?

Beslisvraag: welke documentstromen met externe partijen lopen nu via een route waarover u achteraf geen bewijs heeft?

08 / LAAG 4: BEWIJS

Van logregel naar bruikbaar dossier

Een audit trail is pas waardevol wanneer het incidentteam of de auditor de overdracht ermee kan reconstrueren.

Zorg dat elke relevante actie automatisch een spoor achterlaat: wie verstuurde wat, aan wie, wanneer werd het geopend en wanneer verliep de toegang. Maak dat bewijs exporteerbaar naar uw SIEM- of GRC-omgeving, zodat het niet in losse systemen blijft hangen.

Bepaal vooraf welke vragen u binnen een uur wilt kunnen beantwoorden. Dat dwingt keuzes af over logging, bewaartermijn en toegang tot de logs zelf.

Oefen het reconstrueren

Kies één fictieve overdracht en reconstrueer die met het incidentteam. Wat ontbreekt, wordt een verbeterpunt met een eigenaar.

Houd meldtermijnen haalbaar

Onder de Cbw geldt voor significante incidenten een vroegtijdige waarschuwing binnen 24 uur. Onder de AVG meldt u een datalek binnen 72 uur. Snel bewijs maakt het verschil tussen een onderbouwde melding en een schatting.[6][13]

Tijd	Fictief oefendossier OD-2027-01
09:00	Medewerker deelt een dossier met een externe adviseur, met verificatie en vervaldatum.
09:04	Ontvanger verifieert zich en downloadt het dossier.
11:30	Medewerker meldt dat een bijlage niet voor deze ontvanger bedoeld was.
11:34	Toegang ingetrokken; audit trail toont één download om 09:04.
12:15	Privacy officer beoordeelt de meldplicht op basis van het exportbestand.

Oefenscenario, geen klantcase.

09 / DE BEWIJSKETEN

Eén maatregel, meerdere kaders

Wie bewijs organiseert per wet, bouwt dubbel werk. Wie bewijs organiseert per controle, beantwoordt meerdere wetten tegelijk.

Een bruikbare bewijsredenering volgt altijd dezelfde keten:

Verplichting
Wat vraagt de wet of de klant?

Risico
Wat kan er misgaan?

Maatregel
Welke controle beperkt het?

Werking
Is de controle getest?

Bewijs
Waar staat het spoor?

Besluit
Wie accepteert het restrisico?

Voorbeeld: externe bestandsoverdracht

Maatregel	Ondersteunt onder meer	Bewijs
Versleutelde overdracht met verificatie van de ontvanger	AVG art. 32, Cbw zorgplicht, ISO/IEC 27001 A.5.14	Configuratie en audit trail per overdracht.
Rolgebaseerde en tijdgebonden toegang	ISO/IEC 27001 A.5.15 en A.5.18, DORA ICT-risicobeheer	Provisioninglogs en verlopen links.
Logging van alle acties	ISO/IEC 27001 A.8.15, Cbw meldplicht, AVG art. 5 lid 2	Exporteerbare logs per bestand en ontvanger.
Centrale bewaartermijnen	AVG opslagbeperking, sectorale bewaarplichten	Beleidsinstelling en verwijderlog.

Indicatieve koppeling ter illustratie. De juiste toewijzing hangt af van uw scope en risicoanalyse.[6][7]

Zo werkt u met de keten

Begin bij de maatregel, niet bij de wet. Leg per maatregel vast welke verplichtingen hij ondersteunt, en verwijs vanuit elk kader naar dezelfde controle. Verandert een wet, dan past u de verwijzing aan in plaats van een nieuw proces te bouwen.

Laat de keten eindigen bij een besluit. Een gat in het bewijs is geen ramp, zolang iemand met mandaat het restrisico bewust accepteert of een verbetering inplant. Dat besluit is zelf ook bewijs.

10 / ZELFBEOORDELING

Wat kunt u vandaag aantonen?

Gebruik het werkblad voor één documentstroom. Een onbekend antwoord is een onderzoekspunt, geen voldoende.

Markeer per criterium: A = ingericht én getoetst; B = ingericht, werking nog onvoldoende aangetoond; C = ontbreekt of is onbekend. Noteer de bewijsverwijzing, eigenaar en opvolgdatum in uw beheerdossier.

Controlepunt	A	B	C
1. De toepasselijke wetten en hun deadlines voor 2027 zijn vastgesteld.	○	○	○
2. Elke controle heeft een eigenaar, een doel en een bewijsdefinitie.	○	○	○
3. Het bestuur heeft de maatregelen goedgekeurd en een training gevolgd.	○	○	○
4. In-, door- en uitstroom van accounts verloopt automatisch.	○	○	○
5. Externe toegang heeft altijd een vervaldatum en is intrekbaar.	○	○	○
6. Er is één goedgekeurde route voor gevoelige uitwisseling met externen.	○	○	○
7. Elke externe overdracht is te reconstrueren met een audit trail.	○	○	○
8. Meldprocessen halen de termijnen van 24 en 72 uur, en zijn geoefend.	○	○	○
9. Leveranciers zijn beoordeeld op beveiliging, locatie en logging.	○	○	○
10. Bewijs voor een auditor is binnen één werkdag beschikbaar.	○	○	○

Gebruik geen totaalscore als geruststelling

Kies prioriteiten op risico en afhankelijkheden. Eén C op punt 7 kan zwaarder wegen dan drie B's elders. Spreek vooraf af welke tekortkomingen kritiek zijn en wie een restrisico mag accepteren.

Documentstroom / eigenaar / datum

Eigen werkblad voor interne sturing. Dit is geen gevalideerde audit, wettelijke norm of complianceverklaring.

11 / ROADMAP 2027

Vier kwartalen naar aantoonbaar

Begin klein genoeg om te leren en concreet genoeg om de uitkomst te beoordelen. Rond het jaar af vóór de deadlines van december.

Q1

Afbakenen

Scope en nulmeting

- Stel vast welke wetten gelden en welke deadlines.
- Kies één kritieke documentstroom.
- Vul het werkblad op pagina 11 in.
- Benoem eigenaren per controle.

Q2

Inrichten

Route en controles

- Richt één goedgekeurde route in voor externe uitwisseling.
- Automatiseer SSO, MFA en SCIM.
- Leg bewaartermijnen en vervaldatums centraal vast.
- Train op herkenbare situaties.

Q3

Toetsen

Werking en bewijs

- Reconstrueer een fictieve overdracht.
- Oefen de meldtermijnen van 24 en 72 uur.
- Koppel logs aan uw GRC-omgeving.
- Beoordeel leveranciers, ook op CRA-eisen.

Q4

Borgen

Besluit en verbreding

- Bespreek de resultaten met het bestuur.
- Leg restrisico's vast met een eigenaar.
- Controleer de AI-registratie vóór 2 december.
- Breid uit naar de volgende documentstroom.

Maak het besluit per kwartaal expliciet

Sluit elk kwartaal af met een kort besluit: wat is ingericht, wat is getoetst, wat blijft open en wie is eigenaar. Zo bouwt u gedurende het jaar een dossier op dat een auditor of toezichthouder zonder extra werk kan inzien.

Houd de omvang beheersbaar. Eén goed onderbouwde documentstroom zegt meer over uw volwassenheid dan tien half ingerichte. Gebruik de ervaring daarna om sneller op te schalen.

Eigen organisatiemodel ter inspiratie. Pas de volgorde aan op uw risico's en de termijnen die voor uw sector gelden.

Bestandsoverdracht als bewijsbare maatregel

Secure file transfer is geen los IT-onderwerp. Het is de plek waar gevoelige documenten de organisatie verlaten, en dus waar bewijs het hardst nodig is.

Msafe Secure File Transfer is gebouwd voor het veilig delen van gevoelige bestanden met externe partijen. Medewerkers delen vanuit Outlook met de Msafe Connector of in de webapplicatie. Ontvangers halen bestanden op met Easy Download: na een eenmalige verificatie via hun telefoonnummer, zonder account. Bestanden tot 1 TB zijn standaard, grotere op aanvraag.[12]

Msafe is gecertificeerd volgens ISO/IEC 27001:2022 en wordt gehost in Nederland. Een tool maakt een organisatie nooit automatisch compliant: daarvoor zijn ook beleid, risicoanalyse en processen nodig. Msafe levert de controles en het bewijs voor de uitwisselingsroute.

Laag	Wat Msafe ondersteunt	Wat u zelf regelt
Beleid	Centrale bewaartermijnen, vervaldatums en uitgesloten bestandstypen.	Classificatie, informatie-eigenaren en uitzonderingen.
Toegang	Single Sign-On via Microsoft Entra ID, SCIM, MFA, ontvangersverificatie en intrekbare toegang.	Rollen, rechtenreview en vertrekproces.
Gebruik	Delen vanuit Outlook, gedeelde ruimtes waarin iedereen ziet wat er met een document gebeurt, grote bestanden.	Werkafspraken en training per afdeling.
Bewijs	Volledige audit trail per bestand en ontvanger, exporteerbare rapportages en een API.	Koppeling met GRC of SIEM en het toetsritme.

Toets uw eigen documentstroom

Plan een demo of proof of concept met één documentstroom uit deze gids. We laten zien welk bewijs u na afloop direct aan een auditor kunt tonen. **msafe.co/nl/demo-aanvragen**

Productinformatie is afkomstig van Msafe B.V., peildatum november 2026. Functionaliteit en voorwaarden kunnen wijzigen.

BRONNEN EN VERANTWOORDING

Onderbouwing en verder lezen

Peildatum: 2 november 2026. Wetgeving, toezicht en officiële uitleg kunnen na deze datum wijzigen.

De gids geeft algemene informatie voor bestuurders en specialisten. Het zelfbeoordelingsmodel, het oefendossier en de roadmap zijn eigen werkmodellen van Msafe, geen wettelijke normen of gevalideerde audits.

Laat de toepassing van wet- en regelgeving op uw organisatie toetsen door uw eigen juridische of compliancefunctie. Cijfers zijn afkomstig uit de genoemde openbare bronnen.

[1] Rijksoverheid
Cyberbeveiligingswet en Wet weerbaarheid kritieke entiteiten vanaf 15 augustus 2026 van kracht, 7 juli 2026.

[2] NCSC
Registratie in het entiteitenregister via mijn.ncsc.nl.

[3] DORA
Verordening (EU) 2022/2554, van toepassing sinds 17 januari 2025.

[4] AI Act
Verordening (EU) 2024/1689, gewijzigd door de Digital Omnibus on AI (2026): bijlage III per 2 december 2027, bijlage I per 2 augustus 2028.

[5] Cyber Resilience Act
Verordening (EU) 2024/2847: meldplicht vanaf 11 september 2026, meeste verplichtingen vanaf 11 december 2027.

[6] AVG
Verordening (EU) 2016/679, art. 5 lid 2, art. 32 en art. 33.

[7] ISO/IEC 27001:2022
Bijlage A, beheersmaatregelen 5.14, 5.15, 5.18 en 8.15.

[8] Verizon
Data Breach Investigations Report 2026.

[9] ICO
Boete van £750.000 voor de Police Service of Northern Ireland, oktober 2024.

[10] NCSC (Verenigd Koninkrijk)
Shadow IT: guidance.

[11] KPMG
Chief Ethics and Compliance Officer Survey 2025.

[12] Msafe
Productinformatie Msafe Secure File Transfer, november 2026.

[13] NIS2-richtlijn
Richtlijn (EU) 2022/2555, art. 23 (meldtermijnen) en art. 34 (boetes).

Msafe B.V.
Linnaeusweg 9a
IJsselstein, Nederland

+31 88 88 53 010
info@msafe.co
msafe.co

Uitgave: Msafe B.V. | Editie 2027 | © 2026 Msafe B.V. Alle rechten voorbehouden.