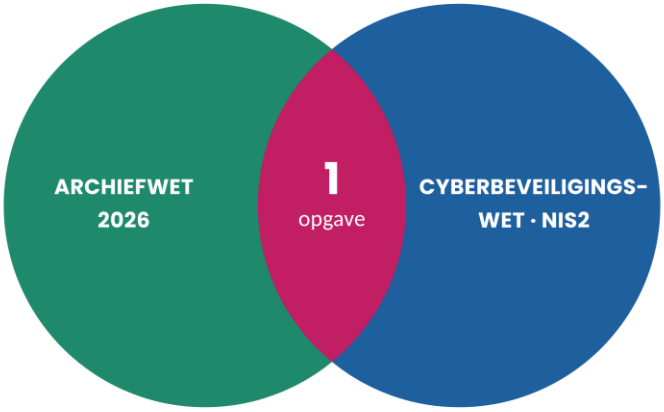
KENNISGROEP INFORMATIEWETTEN VAN KIA

Twee wetten, één opgave

De Archiefwet 2026 en NIS2 (Cyberbeveiligingswet) integraal aanpakken



Een handreiking voor bestuurders en informatieprofessionals bij de overheid.

Kennisgroep Informatiewetten (KIA) Versie 1 · september 2026 · definitieve versie

Managementsamenvatting

Voor bestuurders die eerst alleen deze pagina lezen

De overheid staat voor één samenhangende opgave. Twee wetten die kort na elkaar in werking treden, de Archiefwet 2026 (per 1 januari 2027) en de Cyberbeveiligingswet die de Europese NIS2-richtlijn implementeert (voorzien per 15 augustus 2026), stellen fundamentele eisen aan hetzelfde domein: het verantwoord beheren van digitale systemen en van de informatie daarin. Wie ze afzonderlijk aanpakt, investeert dubbel of laat lacunes bestaan. Wie ze verbindt, vergroot effectiviteit, legitimiteit en draagvlak.

121	**1.430**	**50%**	**€ 10 mln**
ransomware-incidenten in Nederland in 2024 (minimaal, NCSC)	datalekmeldingen door cyberaanvallen in 2024 (AP)	rijksbrede overheidsorganisaties met beveiliging niet op orde (Rekenkamer)	maximale boete voor essentiële entiteiten onder NIS2

De kern

- **Behandel het als één opgave.** Eén programma, één data governance board en één risicokader voor beide wetten.
- **Richt in by design.** Beveiliging én archivering vanaf het moment waarop informatie ontstaat, niet achteraf.
- **Verbind de disciplines.** Informatiebeveiliging en informatiebeheer werken samen, met scherp belegde rollen.

Wat het van u als bestuurder vraagt

- Persoonlijke verantwoordelijkheid: onder de Cyberbeveiligingswet keurt u de maatregelen goed, houdt u toezicht en volgt u verplichte scholing. Boetes lopen op tot € 10 miljoen; bestuurders riskeren daarnaast een persoonlijke boete.
- Versterkt toezicht: de Archiefwet 2026 introduceert nieuwe handhavingsbevoegdheden, waaronder een meldplicht en de mogelijkheid tot boetes.
- Een positieve boodschap: dezelfde investering in governance, beleid en gedrag dekt beide wetten en versterkt tegelijk uw dienstverlening, uw verantwoording en het vertrouwen van burgers.

Hoofdstuk 8 bevat een stappenplan in acht stappen en drie fasen dat u direct kunt inzetten. De hoofdstukken daarvoor onderbouwen de opgave; de hoofdstukken daarna wijzen de weg naar bestaande kennisproducten.

Inhoud

Over deze handreiking

- Deze handreiking brengt vier werkdocumenten van de Kennisgroep Informatiewetten samen in één geheel. De inhoud is feitelijk geactualiseerd en aangevuld met kennisproducten van het Nationaal Archief en aanverwante organisaties.
- **Actueel per september 2026.** De Archiefwet 2026 (Stb. 2026, 149) treedt in werking op 1 januari 2027. De Cyberbeveiligingswet is nog niet in werking; inwerkingtreding wordt voorzien rond 15 augustus 2026, na instemming van de Eerste Kamer.
- **Wetsverwijzingen.** Artikelverwijzingen volgen de structuur van de gepubliceerde Archiefwet 2026 (Stb. 2026, 149); raadpleeg voor de details de wettekst en de bijbehorende lagere regelgeving.

01 In één oogopslag

De bestuurlijke kernboodschap

Twee wettelijke kaders stellen binnen korte tijd fundamentele eisen aan de wijze waarop de overheid met digitale informatie en informatiebeveiliging omgaat: de Cyberbeveiligingswet, de Nederlandse uitwerking van de Europese NIS2-richtlijn, en de Archiefwet 2026. Beide raken hetzelfde domein, namelijk het verantwoord beheren van digitale systemen en van de informatie die daarin besloten ligt.

De werkelijke opgave schuilt niet in de wetten afzonderlijk, maar in hun onderlinge samenhang. NIS2 dwingt tot controle en bescherming; de Archiefwet 2026 dwingt tot transparantie en duurzame toegankelijkheid. Wie de raakvlakken niet in samenhang oppakt, investeert dubbel in overlappende maatregelen of ziet juist wezenlijke lacunes over het hoofd.

Wat succesvolle uitvoering vraagt

- **Geïntegreerde data governance:** één sturingslijn voor beide wetten.
- **Inrichting by design:** in de ontwerpfase van informatiesystemen wordt al rekening gehouden met eisen vanuit beveiliging én archivering
- **Doelgerichte samenwerking:** tussen informatiebeveiliging en informatiebeheer, met scherp belegde rollen.

De urgentie, onderbouwd

Cyberdreiging: het NCSC registreerde voor 2024 minimaal 121 ransomware-incidenten in Nederland; het Cybersecuritybeeld Nederland 2025 spreekt van een riskante mix in een onvoorspelbare wereld.

Datalekken: de Autoriteit Persoonsgegevens ontving in 2024 ruim 1.430 datalekmeldingen door cyberaanvallen; bij veel ransomware-incidenten werd bovendien data gestolen.

Overheid kwetsbaar: de Algemene Rekenkamer stelde vast dat de helft van de rijksbrede overheidsorganisaties de informatiebeveiliging niet op orde had en telde in 2023 negen onvolkomenheden bij informatiebeheer.

Informatiehuishouding: het ACOI concludeerde in 'Alles is niets' dat meerjarenplannen voor de digitale informatiehuishouding te vrijblijvend zijn.

Wat dit voor u als bestuurder betekent

- Onder de Cyberbeveiligingswet draagt u als bestuurder persoonlijke verantwoordelijkheid: u keurt de maatregelen goed, houdt toezicht en volgt verplichte scholing. De boetes lopen op tot € 10 miljoen voor essentiële entiteiten en € 7 miljoen voor belangrijke entiteiten; daarnaast riskeren bestuurders een persoonlijke boete.
- De Archiefwet 2026 versterkt het toezicht op informatiebeheer aanzienlijk en introduceert nieuwe handhavingsbevoegdheden, waaronder een meldplicht en de mogelijkheid tot boetes.
- De boodschap is bovenal positief: dezelfde investering in governance, beleid en gedrag dekt beide wetten. Wie het als één opgave benadert, wint aan grip, aantoonbaarheid en vertrouwen.

02 De twee wetten in het kort

Wat ze inhouden en waar ze staan

Archiefwet 2026: in werking op 1 januari 2027

De Archiefwet 2026 vervangt de sterk verouderde Archiefwet 1995 en is toegesneden op het digitale tijdperk. De Eerste Kamer stemde op 12 mei 2026 in; op 19 juni 2026 volgde publicatie in het Staatsblad (Stb. 2026, 149).

Kernwijzigingen

Duurzame toegankelijkheid (hoofdstuk 4 en art.4.1): overheidsorganen nemen passende maatregelen om documenten duurzaam toegankelijk te maken en te houden; deze maatregelen worden vastgelegd in de beheerregeling (art. 4.2)

Overbrengingstermijn (art. 5.4): van twintig naar tien jaar, gerekend vanaf het opmaken of ontvangen van een document.

Openbaarheid en beperkingen (hoofdstuk 7, art. 7.2): documenten worden na overbrenging in beginsel openbaar; veertien specifieke beperkingsgronden vervangen de drie brede gronden uit 1995.

Archivaris (hoofdstuk 6, art. 6.3): het aanwijzen van een archivaris wordt verplicht en de positie van de archivaris wordt versterkt, met gemoderniseerde eisen aan kennis en deskundigheid. Bij het Rijk vervult de rijksarchivaris deze rol; de zittende algemene rijksarchivaris wordt geacht te zijn aangewezen. Provincies, gemeenten en waterschappen die bij inwerkingtreding geen archivaris hebben, wijzen er binnen twee jaar een aan.

Versterkt toezicht: onder meer een meldplicht en de mogelijkheid tot boetes.

Ondersteuning: een meerjarig implementatieprogramma van OCW loopt tot 2030, met kennisproducten, instrumenten en opleidingen.

Cyberbeveiligingswet (NIS2): verwacht augustus 2026

De Cyberbeveiligingswet (Cbw) implementeert de Europese NIS2-richtlijn (EU 2022/2555) en vervangt de Wet beveiliging netwerk- en informatiesystemen (Wbni). De Tweede Kamer aanvaardde het voorstel op 15 april 2026; de Eerste Kamer heeft de behandeling nog onder handen. Inwerkingtreding wordt voorzien rond 15 augustus 2026. Voor de sector overheid geldt de BIO2 (Baseline Informatiebeveiliging Overheid 2) als normenkader voor de zorgplicht; nadere uitwerking volgt in het Cyberbeveiligingsbesluit (Cbb).

Kernverplichtingen

Zorgplicht: passende en evenredige maatregelen om cyberrisico's te beheersen.

Meldplicht: significante incidenten melden via het portaal van het Nationaal Cyber Security Centrum (NCSC): een vroegtijdige waarschuwing binnen 24 uur en een melding met eerste analyse binnen 72 uur.

Registratieplicht: opname in het entiteitenregister bij het NCSC.

Bestuurdersaansprakelijkheid: het bestuur keurt maatregelen goed, houdt toezicht en volgt verplichte scholing.

Toezicht overheid: de Rijksinspectie Digitale Infrastructuur (RDI); voor gemeenten verloopt dit via de IBD en VNG, met gebruik van de ENSIA-methodiek.

De meldplicht onder NIS2 in drie stappen

Twee bewegingen, één richting

- **Archiefwet 2026:** transparantie en duurzame toegankelijkheid, zodat informatie vindbaar, beschikbaar, leesbaar, interpreteerbaar, betrouwbaar en toekomstbestendig is en blijft.
- **NIS2 en Cbw:** controle en bescherming, zodat (informatie in) systemen en diensten veilig en beschikbaar blijven.
- **Samen leveren beide wetten** een overheid die haar informatie zowel beschermt als verantwoordt.

03 Waar de wetten elkaar raken

Het integratievraagstuk

De wetten zijn complementair, maar botsen soms in hun prioriteiten. Juist op de raakvlakken ontstaan de belangrijkste risico's, en tegelijk de grootste kansen om maatregelen slim te combineren.

Drie spanningsvelden

- Openbaarheid tegenover beveiliging: informatie moet toegankelijk zijn voor burgers, journalisten en onderzoekers, en tegelijk beschermd tegen ongeautoriseerde toegang.
- Snelheid tegenover zorgvuldigheid: NIS2 vraagt om een waarschuwing binnen 24 uur en een melding binnen 72 uur, terwijl een zorgvuldige afweging over bewaren en publiceren tijd vergt.
- Wissen tegenover bewaren: na een incident is het vanuit beveiliging soms wenselijk gegevens te wissen, terwijl de Archiefwet voorschrijft wat bewaard moet blijven. Let op het woordgebruik: wissen is een beveiligingshandeling, vernietigen is een archiefhandeling die alleen mag op grond van een vastgesteld selectiebesluit.

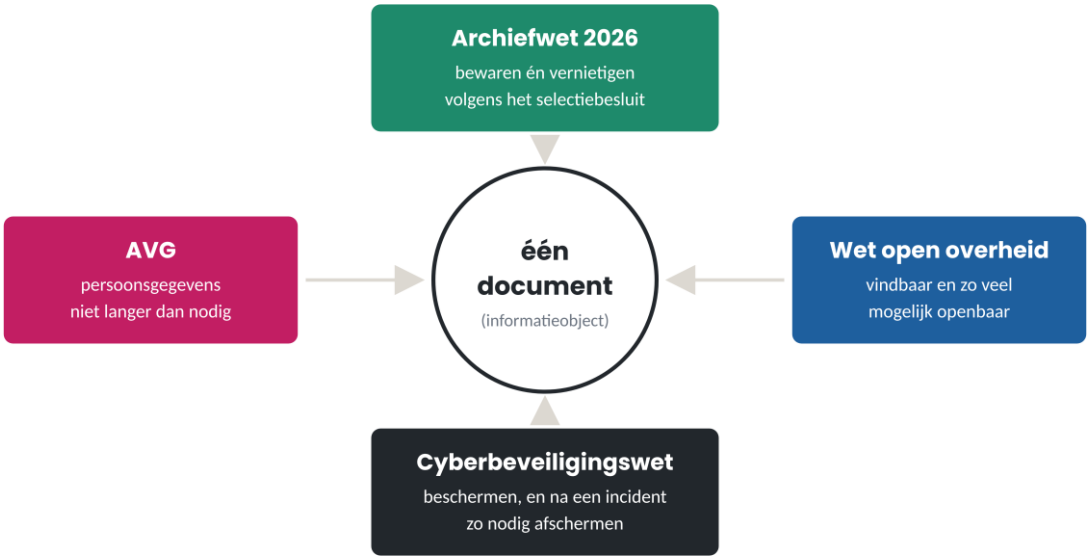
Waarom de raakvlakken doorslaggevend zijn

Een beveiligingsincident (NIS2) kan rechtstreeks leiden tot onherstelbaar verlies van informatie (dit raakt de duurzame toegankelijkheid onder de Archiefwet). Omgekeerd bemoeilijkt een gebrek aan overzicht — een randvoorwaarde voor duurzame toegankelijkheid onder de Archiefwet — de detectie van beveiligingsincidenten (NIS2). Gijzelsoftware die systemen versleutelt, treft zowel de continuïteit als de duurzame toegankelijkheid.

Incidentresponsplannen (NIS2) en continuïteitsplannen voor de digitale informatiehuishouding (Archiefwet) horen daarom naadloos op elkaar aan te sluiten.

De scherpste botsing: bewaren, vernietigen en openbaarheid

Op één en hetzelfde document werken vier verplichtingen tegelijk, en ze wijzen niet dezelfde kant op. Datzelfde stuk informatie heet in de Archiefwet 2026 een document, in de Archiefwet 1995 archiefbescheiden en in het DUTO-raamwerk en het dagelijkse vakjargon een informatieobject; de Cyberbeveiligingswet spreekt over gegevens in netwerk- en informatiesystemen. De Archiefwet 2026 verplicht duurzame toegankelijkheid: bepaalde informatie blijft blijvend bewaard, andere informatie wordt tijdig en verantwoord vernietigd op grond van het selectiebesluit (hoofdstuk 5). De AVG eist juist dat persoonsgegevens niet langer worden bewaard dan noodzakelijk. De Wet open overheid (Woo) vraagt dat informatie snel vindbaar en actief openbaar is. De Cyberbeveiligingswet (NIS2) wil informatie beschermen en na een incident zo nodig afschermen of isoleren.



De botsing zit in één woord: weg. Wissen na een incident is iets wezenlijk anders dan vernietigen onder de Archiefwet. Wissen is een beveiligingsmaatregel, gericht op het schoon opleveren van een systeem. Vernietigen is een archiefhandeling die alleen mag op grond van het vastgestelde selectiebesluit. Wat volgens dat selectiebesluit bewaard moet blijven, mag dus niet verdwijnen om een systeem na een aanval schoon op te leveren; het wordt eerst veiliggesteld. Wat op grond van de AVG niet langer bewaard mag worden, moet juist tijdig en aantoonbaar worden vernietigd. Proportionaliteit en een actueel selectiebesluit (voorheen selectielijst) bepalen de uitkomst. Richt die afweging by design in, in het ontwerp van proces en systeem. Dan liggen de keuzes vooraf vast en zijn ze grotendeels te automatiseren: bewaartermijn, classificatie en logging worden meegegeven op het moment dat informatie ontstaat. Achteraf lukt dat maar gedeeltelijk, onder tijdsdruk, met meer handwerk en tegen hogere kosten.

Uit de praktijk

- In april 2025 raakten alle ministeries betrokken bij een datalek doordat metadata bij de omzetting naar een publicatieformat onvoldoende werden opgeschoond, waardoor namen en gebruikersnamen van ambtenaren herleidbaar waren; het lek werd op 8 april 2025 gemeld bij de Autoriteit Persoonsgegevens (Kamerbrief BZK, april 2025). Het voorbeeld toont hoe informatiebeheer, openbaarheid en beveiliging samenvallen in één handeling.
- Zo pakt dat uit: na een aanval met gijzelsoftware wil de leverancier een schone omgeving opleveren en het besmette postbusarchief wissen. Dat mag niet zonder meer. Wat volgens het selectiebesluit bewaard moet blijven, gaat eerst veiliggesteld naar de schone omgeving (Archiefwet). Persoonsgegevens waarvan de bewaartermijn is verstreken, gaan juist wél weg en dat wordt vastgelegd (AVG). Documenten die onder een Woo-verzoek vallen, blijven vindbaar (Woo). En de forensische logging blijft beschikbaar voor de melding (Cyberbeveiligingswet). Eén handeling, vier toetsen, één besluit.

De kern in één zin

- Behandel NIS2 en de Archiefwet 2026 niet als twee losstaande trajecten, maar als één integrale opgave voor een overheid die veilig én transparant is.

04 Verdiepende vergelijking

Governance · Risico's · Aanpak · Advies

De volgende vier tabellen plaatsen de wetten naast elkaar op de thema's die er in de praktijk toe doen. Kijk daarbij niet uitsluitend naar de letter van de wet, maar evenzeer naar de geest ervan.

4.1 Governance: welke beleidsstukken worden geraakt?

Thema	Archiefwet 2026	NIS2 en Cbw	Overeenkomst
Geraakte kaders	• Bewaarstrategie, beheerregeling, archiefverordening en waarderingsbeleid • Aanwijzen van een archivaris (verplicht) • Beleid voor openbaarheidsbeperkingen, procedures voor uitzondering op overbrenging en een migratieplan vooraf • Afspraken met ketenpartners	• Informatiebeveiligings- en privacybeleid, plus risicomanagement • Crisis- en continuïteitsmanagement en kwaliteitszorg • IT- en changemanagement en ketenpartnerbeleid • BIO2 als normenkader	• Op strategisch én tactisch niveau wordt een groot aantal beleidsstukken geraakt • Borg het beleid in de PDCA-cyclus (plan, do, check, act) en verbind die met de planning- en controlcyclus: de PDCA-cyclus levert de inhoud, de P&C-cyclus het bestuurlijke moment. Randvoorwaarde RVW01 van het DUTO-raamwerk legt dezelfde koppeling • Een kwaliteitssysteem is noodzakelijk

4.2 Risico's: wat is nog onvoldoende uitgewerkt?

Thema	Archiefwet 2026	NIS2 en Cbw	Verschil en overeenkomst
Passende maatregelen en aansprakelijkheid	• Leg passende maatregelen aantoonbaar vast in de beheerregeling; zonder vastlegging ontbreekt bewijslast bij inspectie • Risico op onvoldoende oog voor alle organisaties die onder de wet vallen • Verantwoordelijkheden per rol zijn vaak onvoldoende helder	• Risico op overbeveiliging; werk daarom met een plan op hoofdlijnen • Bestuurders zijn persoonlijk aanspreekbaar • Bij nalatigheid kan een toezichthouder meekijken via een aanwijzing	• Verschil: NIS2 kent expliciete persoonlijke bestuurdersaansprakelijkheid, terwijl de Archiefwet 2026 het toezicht versterkt met een meldplicht en boetes • Overeenkomst: in beide gevallen dreigt imago- en reputatieschade; beleg daarom helder wie waarvoor verantwoordelijk is

4.3 Aanpak: strategisch en operationeel

Thema	Archiefwet 2026	NIS2 en Cbw	Overeenkomst

Wat te doen	• Strategisch: richt duurzame toegankelijkheid by design en risicogericht in, als onderdeel van de digitale strategie • Operationeel: pas archiveren by design toe in processen, applicaties en systemen • Verkort de overbrengingstermijn van twintig naar tien jaar en investeer in bewustwording van mensen én systemen	• Stel contactpersonen aan en formuleer ketenpartnerbeleid, een risicoanalyse en classificatie • Richt een incidentaanpak en beleid voor de fysieke omgeving in • Stuur actief op risico's en compliance, stel de risicobereidheid vast en rapporteer periodiek	• Stel op meerdere thema's een aanpak op die medewerkers ook daadwerkelijk uitvoeren • De ABRO 2026 en dezelfde DUTO-randvoorwaarden (RVW 01, 03, 05 t/m 09, 11 en 12) zijn voor beide wetten relevant

4.4 Advies: route, middelen en mandaten

Thema	Archiefwet 2026	NIS2 en Cbw	Overeenkomst
Aan bestuur en professionals	• Maak informatiebeheer onderdeel van de digitale strategie en borg eigenaarschap, mandaat en middelen • Pas archiveren by design toe en werk volgens vastgestelde kaders • Leg verantwoordelijkheden en mandaten vast en zorg voor voldoende capaciteit en middelen (DUTO-randvoorwaarde RVW04: voldoende en deskundig personeel), wat ook de zorgplicht onder de Cbw dient	• Veranker NIS2 in de bestaande governance (BIO2, ISMS en risicomanagement) • Geef een bestuurlijke opdracht voor integrale implementatie en mandateer de CISO en CIO • Rapporteer structureel aan directie en bestuur	• Kies één integraal governancemodel en behandel NIS2 en de Archiefwet niet apart, met inrichting by design als overkoepelend principe • Kies een holistische aanpak met CIO, CISO en informatiebeheer, onder centrale coördinatie • Investeer in keten- en leveranciersturing; een 0-meting bijvoorbeeld aan de hand van een DUTO-risicobeoordeling brengen overlap en hiaten in kaart

05 Strategisch kader per wet

Elf kernvragen, naast elkaar

Beide wetten raken de gehele organisatie: governance, informatiebeheer, informatiebeveiliging, privacy, bedrijfsvoering en bestuurlijke verantwoordelijkheid. Onderstaande tabel beantwoordt elf kernvragen kort en scherp voor beide wetten.

Kernvraag	Archiefwet 2026	NIS2 en Cbw
1. Wat houdt de wet in?	Duurzaam toegankelijk beheer van overheidsinformatie gedurende de volledige levenscyclus. Duurzaam toegankelijk betekent onder meer dat overheidsinformatie betrouwbaar is.	Versterking van de digitale weerbaarheid langs drie pijlers: zorgplicht, bestuurlijke verantwoordelijkheid en meldplicht, aangevuld met een registratieplicht.
2. Wat is het doel?	Onder meer de uitvoering van publieke taken en de verantwoording daarover, onderzoek en erfgoed.	Uniformiteit, weerbaarheid en continuïteit van kritieke diensten binnen de Europese Unie.
3. Wat organisatorisch inrichten?	Een integraal stelsel van informatiebeheer, informatiebeveiliging en privacy, met heldere governance, processen en systemen.	Een informatiebeveiligingsmanagementsysteem (ISMS): risicomanagement, securityoperaties, een crisis- en incidentorganisatie en asset- en informatieregisters.
4. Beleid en kaders opstellen?	Ja. Op strategisch, tactisch en operationeel niveau; zonder vastgesteld beleid is aantoonbare naleving onmogelijk.	Ja, als bewijslast bij toezicht. Dit ligt vaak bij de CISO en de CIO, niet primair bij informatiebeheer.

Kernvraag	Archiefwet 2026	NIS2 en Cbw
5. Aanpassing van processen?	Vrijwel zeker: registratie, classificatie, bewaren en vernietigen, toegang, migratie en herstel, geïntegreerd in aanbesteding en systeemontwikkeling (by design). Zie ook de DUTO-processen registreren, bewaren, vernietigen, migreren en ter beschikking stellen.	Vrijwel zeker: inkoop en leveranciers, incident- en changemanagement, projectmanagement en de datalevenscyclus, met Security by Design.
6. Afstemming met welke rollen?	Bestuur en directie; CIO, CISO, informatiebeheer, privacyfunctionaris en FG, en enterprise architect; operationele teams en leveranciers.	Dezelfde rollen, volgens het Three Lines of Defense-model, waarbij CIO en CISO het voortouw nemen, samen met informatiebeheer, privacy, HR, communicatie en juridische zaken. Deze informatiedomeinen vallen onder compliance.
7. Governance herzien?	Ja: borg informatiebeheer structureel, met heldere verantwoordelijkheden, bestuurlijke sturing en controlemechanismen.	Ja: board accountability, cyberrisico's in het enterprise risk management, strakkere rapportagelijnen en meer mandaat voor de CISO.
8. Opleiding, houding en gedrag?	Bewustwording, training over archivering en dossiervorming en managementtraining; groei naar een cultuur van zorgvuldig informatiebeheer.	Doorlopende bewustwording (phishing en social engineering), specifieke training voor IT en security en verplichte kennisopbouw voor het bestuur.
9. Binnen 1 jaar of meerjarig?	Meerjarig: governance en beleid zes tot twaalf maanden; processen en systemen één tot twee jaar; volledige volwassenheid twee tot drie jaar of langer.	Meerjarig: basis compliance vaak zes tot twaalf maanden; volledige volwassenheid twee tot drie jaar. Een doorlopend verbetertraject, geen eenmalige actie.
10. Informatiebeheerstrategie aanpassen?	Ja: sterkere integratie met beveiliging, privacy, risicomanagement en digitale continuïteit, met meer nadruk op classificatie en metadata.	Ja: informatiebeheer en cybersecurity raken verweven, met strengere eisen aan classificatie, bewaartermijnen en logging.
11. Impact op de IV-strategie?	Groot en structureel: systemen ondersteunen archivering en metadata, Archiveren by design wordt standaard en de focus ligt op duurzaam toegankelijkheid: overheidsinformatie beschermen én toegankelijk houden.	Groot en structureel: Security by Design wordt standaard, met investeringen in monitoring, herbeoordeling van leveranciers en beschikbaarheid onder aanval.

Overeenkomsten en verschillen

- **Overeenkomst:** beide wetten vragen om proactief handelen en inrichten (by design) en om samenwerking tussen informatiebeheer, informatiebeveiliging, privacy en ICT binnen één integraal stelsel.
- **Verschil:** de Archiefwet wordt grotendeels uitgevoerd door informatiebeheer, terwijl NIS2 zwaarder leunt op privacy, informatiebeveiliging en bestuur.

06 Risico's en beheersmaatregelen

Van risico naar maatregel naar advies

Aan vrijwel elk risico kleeft de consequentie van boetes en reputatieschade. We betrekken hierbij nadrukkelijk ook de maatschappelijke risico's, want daar draait het uiteindelijk om: een overheid die zowel veilig als transparant is. De verwijzingen (B en TO) koppelen elk risico aan de adviezen in hoofdstuk 7.

Risico	Kern	Maatregel	Advies
Compliance wel opgesteld, niet ingericht	NIS2 art. 21 en 23	Integraal governancemodel: één data governance board (CISO, CIO, informatiebeheer, CRO, archivaris en FG). Beveiliging en archivering by design.	B1 · B2 · TO3
Onvoldoende inzicht in kwetsbaarheid bij leveranciers	NIS2 art. 21 lid 2 sub d; Archiefbesluit	Ketenbeveiliging: neem contractuele beveiligingseisen op bij leveranciers.	TO1
Operationele verstoring door de incidentmeldplicht	Snelle melding binnen 24 uur; NIS2 art. 23	Stel een helder draaiboek op en oefen dit gezamenlijk en periodiek.	TO3
Onvoldoende toezicht, waardoor fouten zich herhalen	NIS2 art. 21; Archiefwet art. 4.2	Herbeoordeel risico's periodiek, voer interne audits uit, toon een aantoonbare PDCA-cyclus en borg bestuurlijk toezicht.	B3
Diensten niet meer tijdig geleverd door gijzelsoftware	Onvolwassen securityproces	Integraal risicomanagement: breng cyber- en informatierisico's samen in één framework (bijvoorbeeld ISO 27001 met archiefnormen).	B1 · B2 · TO3
Persoonlijke of gevoelige gegevens komen op straat	Datalek	Cyberhygiëne en training; passende maatregelen per documentcategorie, inclusief tijdige vernietiging.	B2
Balans tussen privacybescherming en historisch behoud	Achteraf ordenen werkt niet	Beheer digitale informatie vanaf creatie op orde (by design).	B1
Snellere overbrenging (tien jaar) met risico op kwaliteitsverlies	Overbrenging: art. 5.4	Weeg af of stukken nog nodig zijn en vraag zo nodig ontheffing van de overbrengingsverplichting aan.	TO3
Tekort aan gekwalificeerd personeel	Archivaris en professionalisering	Zet structureel in op training en bewustwording en stel een archivaris aan.	TO2
Afschermen en beschikbaar stellen op elkaar afstemmen	Op te lossen met DUTO-functies (maskering en metagegevensbeheer); geen tegenstelling	Regel afscherming via de DUTO-functie maskering (bij het proces ter beschikking stellen) en leg logging vast via de functie metagegevensbeheer. Modeleis R09 uit het DUTO-proces registreren vraagt om toegangs-, gebruiks- en beveiligingsmetagegevens, zodat toegang tot en gebruik van informatieobjecten traceerbaar zijn. Combineer securityaudits en archiefinspecties in één auditcyclus.	B1 · TO3
Incidentrespons versus bewaarplicht	Data wissen versus bewaren	Koppel incident en archief: incidenten worden gelogd (NIS2) en blijven duurzaam toegankelijk (Archiefwet). Ontwikkel hiervoor gezamenlijk een procedure en pas proportionaliteit toe.	B2 · TO2 · TO3
Versnipperde systemen	Archivering vraagt om overzicht. Een passende maatregel kan zijn dat je architectuurprincipe als Common Ground toepast.	Zorg voor een actueel overzicht van processen, overheidsinformatie, applicaties, standaarden en hun samenhang (DUTO-randvoorwaarde RVW08); dat geeft inzicht, ook onder de Cyberbeveiligingswet. Combineer DMS, archivering en logging in samenhangende systemen en vermijd losse tools.	TO2 · TO3

Risico	Kern	Maatregel	Advies
Overheidsinformatie zelf raakt verloren	Niet blijvend bewaard of te laat vernietigd	Neem blijvend te bewaren informatie op in back-up-, herstel- en continuïteitsplannen en controleer of vernietiging op tijd en aantoonbaar gebeurt. Informatie die verloren gaat, komt niet terug: dat raakt verantwoording, onderzoek en hergebruik, en bij een hack raken ook gegevens van burgers kwijt.	B1 · TO2 · TO3
Onterechte of niet-tijdige vernietiging	Selectie en vernietiging: hoofdstuk 5	Train medewerkers informatiebeheer en stem af met informatiebeveiliging, privacy en de FG; maak gezamenlijk procedures.	TO2

Pas onder meer deze (beleids)stukken integraal aan

- Visie en strategie informatiehuishouding · Beleid informatiehuishouding · Beleid informatiebeveiliging · Inkoopvoorwaarden (gezamenlijke eisen) · Calamiteitenplan (gezamenlijke oefeningen) · Auditplan (geïntegreerde auditcyclus) · Trainingsplan (beide raakvlakken) · Kwaliteitshandboek.

07 Adviezen

Van bestuurlijk tot operationeel

Bestuurlijk niveau

B1

Stel een integraal programma in

- Richt één programma in dat NIS2 en de Archiefwet 2026 in samenhang aanstuurt.
- Beleg de programmamanager rechtstreeks onder de hoogste ambtelijke leiding (secretaris-generaal, gemeentesecretaris of algemeen directeur).
- Formeer een stuurgroep met de CISO, de archivaris of IB-manager (CRO), de CIO of CDO en juridische zaken.

B2

Actualiseer de BIO2 als gemeenschappelijk fundament

- De BIO2 vormt het kader waarop zowel NIS2 als de Archiefwet 2026 voortbouwen.
- Voer één gap-analyse uit met beide wettelijke kaders als toetssteen.

B3

Leg bestuurlijke verantwoordelijkheid expliciet vast

- Wijs per wet een bestuurlijk verantwoordelijke aan en informeer het bestuur minimaal jaarlijks.
- Leg dit vast in een bestuurlijk dashboard binnen de planning- en controlcyclus.
- Het bestuur keurt de beveiligingsmaatregelen goed (Cbw) en stelt een informatiebeheerplan vast (Archiefwet 2026).

Tactisch en operationeel niveau

TO1

Actualiseer leverancierscontracten integraal

- Neem bij verlenging en nieuwe contracten de gecombineerde eisen van beide wetten mee.
- Gebruik beschikbare modelovereenkomsten (zoals de VNG-modellen of rijksbrede inkoopvoorwaarden) met verwerkers- en beveiligingsbepalingen die beide kaders afdekken.
- Het betreft vaak dezelfde leveranciers (Microsoft, Centric, PinkRoccade en SaaS-partijen); één gecoördineerde audit dekt beide domeinen.

TO2

Train management en medewerkers

- Combineer de verplichte cyberopleiding met bewustwording over verantwoord informatiebeheer.
- Één geïntegreerde leergang, 'Digitale weerbaarheid en verantwoord informatiebeheer', is efficiënter dan twee losse trajecten.
- Werk samen met communicatie, train via meerdere kanalen en bied een lonkend perspectief.

TO3

Stel een gedocumenteerde risicobeoordeling op

- De risicoanalyses van NIS2 en de Archiefwet 2026 overlappen; voer ze in samenhang uit.
- Stem de incidentrespons- en continuïteitsplannen op elkaar af.
- Voer gezamenlijke audits en procedures uit (informatiebeheer, CISO en FG), zodat er één samenhangende audit ontstaat.

Één governancemodel dat beide wetten draagt

08 Stappenplan voor integrale implementatie

In acht stappen, geordend in drie fasen

Onderstaand stappenplan vertaalt de adviezen naar een werkbare route. De acht stappen zijn geordend in drie fasen en sluiten aan op de reguliere planning- en controlcyclus. Ze zijn zo opgezet dat u met één inspanning aan twee wetten voldoet.

Fase 1 · Fundament leggen

1

Beleg eigenaarschap en richt één programma in

- Benoem een bestuurlijk opdrachtgever en één programmamanager voor beide wetten, rechtstreeks onder de hoogste ambtelijke leiding.

Koppeling met advies: **B1**

2

Breng de nulsituatie in kaart

- Voer een 0-meting en een DUTO-risicobeoordeling uit en maak een gap-analyse tegen de BIO2 en de Archiefwet 2026.
- Inventariseer systemen, informatiestromen, kritieke processen en leveranciers.

Koppeling met advies: **B2 · TO3**

3

Stel een integraal beleids- en risicokader vast

- Bundel informatiebeheer, informatiebeveiliging en privacy in samenhangend beleid, met één gedeeld risicoframework.

Koppeling met advies: **B2 · B3**

Fase 2 · Inrichten

4

Richt de governance in

- Formeer één data governance board met heldere rollen (CISO, CIO, CRO, archivaris en FG) en veranker deze in de planning- en controlcyclus.

Koppeling met advies: **B1 · B3**

5

Vertaal naar processen en systemen

- Pas beveiliging en archivering toe by design; maak hiervoor gebruik van het DUTO-raamwerk en handreiking archiveren by design
- Richt incidentmeldketen in.

Koppeling met advies: **TO3**

6

Borg de keten

- Actualiseer leverancierscontracten met verwerkers- en beveiligingsbepalingen die beide wetten afdekken en voer gezamenlijke audits uit.

Koppeling met advies: **TO1**

Fase 3 · Borgen en verbeteren

7

Investeer in mensen en cultuur

- Bied één geïntegreerde leergang, organiseer doorlopende bewustwording en borg de verplichte bestuurlijke scholing.

Koppeling met advies: **TO2**

8

Monitor, evalueer en verbeter

- Werk volgens de PDCA-cyclus, herbeoordeel risico's periodiek, oefen incidenten en leg jaarlijks verantwoording af via een bestuurlijk dashboard.
- Praktisch: plan is het vaststellen van beleid, risicokader, rollen en middelen; do is by design inrichten in processen, systemen en contracten; check is één auditcyclus met KPI's uit de KIDO en een periodieke risicobeoordeling; act is bijstellen en jaarlijks verantwoorden in de planning- en controlcyclus. Zo wordt borging een ritme in plaats van een eenmalige actie.

Koppeling met advies: **B3 · TO3**

Van plan naar praktijk

- Denk groot en begin klein: kies één of twee bedrijfskritische processen als proeftuin, toon aantoonbaar resultaat en schaal van daaruit op. Zo wordt integrale naleving een groeitraject in plaats van een eenmalige verplichting.

09 Kennisproducten en hulpmiddelen

Bouw voort op bestaande kennis

U hoeft het wiel niet opnieuw uit te vinden. Het Nationaal Archief, het Leerhuis Informatiehuishouding, de toezichthouders en aanverwante kenniscentra bieden concrete instrumenten die de implementatie versnellen. Let wel: het Nationaal Archief is expertisecentrum en kan normen niet verplicht opleggen; een overkoepelend orgaan, zoals het CIO-beraad voor het Rijk of het College van Dienstverleningszaken van de VNG, kan dat wel.

Nationaal Archief: duurzame toegankelijkheid

Kennisproducten (handreikingen en normen)

DUTO-raamwerk: een praktisch hulpmiddel om nog beter de passende maatregelen te bepalen waarmee je overheidsinformatie duurzaam toegankelijk kunt maken en zo archiveren *by design* in de praktijk te brengen. Het raamwerk bevat onder meer dertien generieke randvoorwaarden voor duurzame toegankelijkheid (aangeduid als RVW01 tot en met RVW13) en beschrijft processen zoals ter beschikking stellen en vernietigen, functies en eisen waarmee duurzame toegankelijkheid bewerkstelligd kan worden. In het DUTO-raamwerk wordt duurzame toegankelijkheid ook verbonden met informatiebeveiliging en privacy. Het DUTO-raamwerk bevat ook e-learnings, infographic en architectuurplaten.

In het najaar van 2026 wordt er een module aan het raamwerk toegevoegd dat gaat over het gesprek voeren met hoger-en middenmanagement over duurzame toegankelijkheid van overheidsinformatie. Daarin wordt ook ingegaan wat de meerwaarde van duurzame toegankelijkheid is voor compliance, onder meer voor NIS2.

Handreiking DUTO-risicobeoordeling: het resultaat van een DUTO-risicobeoordeling is de basis voor integrale passende maatregelen. Het brengt het DUTO-raamwerk in de praktijk en verbindt duurzame toegankelijkheid met de risicoafwegingen die ook onder de Cyberbeveiligingswet worden gemaakt.

Handreiking Archiveren by Design: praktische richtlijnen om archivering vanaf het ontwerp in te richten.

MDTO: de norm Metagegevens voor Duurzaam Toegankelijke Overheidsinformatie, opvolger van TMLO en TMR;

Architectuurschets DUTO: de essentiële architectuurkeuzes voor een structureel betere informatiehuishouding.

Voor een overzicht van kennisproducten zie: **Catalogus kennisproducten | Nationaal Archief**
En zie Expertisecentrum | Nationaal Archief
Ook team DUTO: DUTO | Nationaal Archief

Kwaliteit en governance van informatiebeheer

Kwaliteitssystemen

KIDO: de handreiking Kwaliteitssysteem Informatiebeheer Decentrale Overheden (VNG, IPO en Unie van Waterschappen), die voortbouwt op de DUTO-eisen en de kwaliteitseis van de Archiefwet invult; gebruik daarbij ook de KPI's van de VNG voor sturing en verantwoording.

RODIN: het referentiekader voor de opbouw en (zelf)evaluatie van de digitale beheeromgeving.

Informatiebeveiliging: NIS2 en de BIO2

Normen en hulpmiddelen

BIO2: het normenkader voor de zorgplicht van de overheid onder de Cyberbeveiligingswet.

CIP: het Centrum voor Informatiebeveiliging en Privacybescherming levert thema-uitwerkingen bij de BIO en handreikingen, onder meer voor dataclassificatie.

IBD: de Informatiebeveiligingsdienst voor gemeenten biedt operationele producten, een baseline-toolkit en incidentondersteuning (CSIRT).

Zelfevaluatie en quickscan (NCSC en RDI): bepaal of uw organisatie onder de wet valt en of de maatregelen volstaan.

Samen Digitaal Veilig en ENSIA: kosteloze webinars en hulpmiddelen, plus een beproefde verantwoordingsstructuur voor gemeenten.

Architectuur en standaarden die beide werelden verbinden

Referentiekaders

NORA: de Nederlandse Overheid Referentie Architectuur, met thema's voor duurzame toegankelijkheid en voor security en privacy by design.

GEMMA en Common Ground: de gemeentelijke referentiearchitectuur waarin informatiebeheer en beveiliging samenkomen.

Forum Standaardisatie: de pas-toe-of-leg-uit-lijst met open standaarden voor gegevensuitwisseling en beveiliging.

Advies en achtergrond

- ACOI, 'Alles is niets': advies over meerjarenplannen voor de digitale informatiehuishouding.
- KIA Kennisbank en kennisplatforms: de plek waar professionals kennisproducten en praktijkervaring delen.
- Meerjarig implementatieprogramma Archiefwet (OCW, tot 2030): kennis, instrumenten, handreikingen en opleidingen voor de gehele overheid.

10 Bronnen

Geraadpleegd en geactualiseerd per september 2026

Wet- en regelgeving

› **Archiefwet 2026** · Staatsblad Stb. 2026, 149, officiële wettekst. zoek.officielebekendmakingen.nl/stb-2026-149.html

› **Nieuwe Archiefwet maakt overheid transparanter** · Rijksoverheid, inwerkingtreding 1 januari 2027. www.rijksoverheid.nl/actueel/nieuws/2026/05/12/nieuwe-archiefwet-maakt-overheid-transparanter

› **NIS2-richtlijn (EU) 2022/2555** · Europees Parlement en de Raad, 14 december 2022. eur-lex.europa.eu/legal-content/NL/TXT/?uri=CELEX:32022L2555

› **Cyberbeveiligingswet (36.764)** · Eerste Kamer, dossier en stand van de behandeling. www.eerstekamer.nl/wetsvoorstel/36764_cyberbeveiligingswet

› **Cyberbeveiligingswet (NIS2)** · NCSC, verwachte inwerkingtreding rond 15 augustus 2026. www.ncsc.nl/cyberbeveiligingswet-nis2

› **Cyberbeveiligingswet (NIS2-richtlijn)** · Digitale Overheid, overzicht, verplichtingen en BIO2. www.digitaleoverheid.nl/overzicht-van-alle-onderwerpen/cyberbeveiligingswet/

Toezicht en uitvoering

› **Vragen en antwoorden Cyberbeveiligingswet** · NCTV, status, instrumenten en kennisproducten. www.nctv.nl/onderwerpen/c/cyberbeveiligingswet/vragen-en-antwoorden

› **FAQ Cyberbeveiligingswet** · RDI, toezicht, quickscan en zelfevaluatie. www.rdi.nl/onderwerpen/cyberbeveiligingswet en Tooling Cyberbeveiligingswet Cyberbeveiligingswet (NIS2-richtlijn) - Digitale Overheid

› **Wat zijn de verplichtingen onder de Cyberbeveiligingswet?** · Digitale Overheid, overzicht van de verplichtingen voor overheden. www.digitaleoverheid.nl/overzicht-van-alle-onderwerpen/cyberbeveiligingswet

› **Algemene Beveiligingseisen voor Rijksoverheidsopdrachten (ABRO 2026)** · Van kracht sinds 1 januari 2026. open.overheid.nl/details/a13699d9-fcf4-43ef-b282-ece9519e9b81/

Nationaal Archief

› **Kennisbank Nationaal Archief** · verwijzing naar kennisproducten en andere kennisbronnen van het Nationaal Archief www.nationaalarchief.nl/archiveren/kennisbank

› **DUTO-raamwerk** · Praktisch hulpmiddel voor duurzame toegankelijkheid. www.nationaalarchief.nl/archiveren/kennisbank/duto-raamwerk

› **Randvoorwaarden (generiek deel DUTO-raamwerk)** · De randvoorwaarden voor duurzame toegankelijkheid. www.nationaalarchief.nl/archiveren/kennisbank/randvoorwaarden-generiek-deel

› **Ontwikkelagenda kennisproducten** · Nieuwe en herziene producten naar aanleiding van de nieuwe Archiefwet. www.nationaalarchief.nl/archiveren/kennisbank/ontwikkelagenda-kennisproducten

› **MDTO** · Metagegevens voor Duurzaam Toegankelijke Overheidsinformatie, de metadatanorm. www.nationaalarchief.nl/archiveren/mdto

› **KIDO** · Handreiking Kwaliteitssysteem Informatiebeheer Decentrale Overheden (VNG). vng.nl/kennisbank-grip-op-informatie/handreiking-kwaliteitssysteem-informatiebeheer-decentrale-overheden-kido

› **NORA, thema Duurzame Toegankelijkheid** · Referentiearchitectuur voor de overheid. www.noraonline.nl

› **Forum Standaardisatie** · Pas-toe-of-leg-uit-lijst met open standaarden. www.forumstandaardisatie.nl/open-standaarden

› **KIA, Nieuwe Archiefwet: wat betekent dit voor jou** · KIA. kiacommunity.nl/thoughts/27632

Cijfers en onderzoek

› **Cybersecuritybeeld Nederland 2025** · NCTV en NCSC, 'Riskante mix in een onvoorspelbare wereld'. www.ncsc.nl/producten-en-diensten/cybersecuritybeeld-nederland-csbn

› **Jaarbeeld Ransomware 2025** · NCSC, project Melissa, met de incidentcijfers. www.ncsc.nl/ransomware/jaarbeeld-ransomware-2025

› **Informatiebeveiliging en informatiebeheer bij het Rijk** · Algemene Rekenkamer, verantwoordingsonderzoek en Staat van de rijksverantwoording. www.rekenkamer.nl/onderwerpen/ict-en-digitalisering

› **Meldingen van datalekken** · Autoriteit Persoonsgegevens, jaarcijfers datalekken. www.autoriteitpersoonsgegevens.nl

› **Datalek metadata op overheidswebsites · Kamerbrief staatssecretaris BZK over het datalek bij rijksoverheid.nl, open.overheid.nl en overheid.nl, april 2025. nos.nl/artikel/2564082**

Rapporten en advies

› **ACOI, 'Alles is niets'** · Advies over meerjarenplannen voor de digitale informatiehuishouding. www.acoi.nl/publicaties

› **NIS2-informatiebrochure (juni 2025)** · Samen Digitaal Veilig. samendigitaalveilig.nl

Herkomst en verantwoording

Verdiepingstabel (25 juni 2026): de vergelijking op governance, risico's, aanpak en advies (hoofdstuk 4). Door Anastassia Adriaanse, Samira Taounza en Tomas Blansjaar.

Strategisch kader per wet: de elf kernvragen per wet (hoofdstuk 5). Door Theresa en Hester.

Adviezen: de bestuurlijke en tactisch-operationele adviezen B1 tot en met TO3 (hoofdstuk 7).

Risico's: de risicotabel met beheersmaatregelen (hoofdstuk 6).

Redactie en actualisatie: de vier stukken zijn samengevoegd tot één geheel, feitelijk gecorrigeerd (waaronder de citeertitel Archiefwet 2026, de nog niet in werking getreden Cyberbeveiligingswet en het normenkader BIO2) en aangevuld met de vier-krachten-analyse, het stappenplan, cijfers van NCSC, AP en de Algemene Rekenkamer, en kennisproducten van het Nationaal Archief.

Colofon Samengesteld door de Kennisgroep Informatiewetten van KIA. Deze handreiking bundelt en actualiseert eerdere werkdocumenten van de kennisgroep tot één samenhangend geheel. Versie 1 · september 2026, definitieve versie.