

ENSIA 2025/2026 Audit

Informatiebeveiliging en verantwoording voor een betrouwbare overheid

Een toelichting op onze aanpak voor de ENSIA audit.
Wij staan voor pragmatische auditoren die met u
meedenken en efficiënte audits tegen een
scherp tarief.

Auditvision
De Expert in
ENSIA audits. De auditor
die naast u zit in
het ENSIA traject
en niet tegenover u.



Auditvision
IT-auditors

Uw partner voor een
betrouwbare overheid

Inhoud

Hoofdstuk 1	Introductie	3
	<i>Wat is ENSIA?</i>	3
	<i>ENSIA als Sleutel tot Digitale Veerkracht</i>	3
Hoofdstuk 2	Waarom AudITvision?	4
	<i>Wat ons onderscheidt?</i>	4
Hoofdstuk 3	Onze aanpak in 7 fasen	5
Hoofdstuk 4	Het normenkader	9
Hoofdstuk 5	Uitbesteding en externe partijen	10
	<i>DigiD</i>	10
	<i>Suwinet</i>	10
	<i>Onze werkwijze</i>	10
	<i>Geen assurancerapport? AudITvision voert aanvullend onderzoek uit</i>	10
Hoofdstuk 6	Transparante kosten en tarieven	11

Hoofdstuk 1 Introductie

Gemeenten dragen een grote verantwoordelijkheid in het veilig omgaan met informatie. ENSIA, de Eenduidige Normatiek Single Information Audit, helpt hen om hier op uniforme en inzichtelijke wijze over te rapporteren. AudITvision ondersteunt gemeenten bij deze verantwoording met een scherpe, betrouwbare én samenwerkingsgerichte auditaanpak.

Wat is ENSIA?

ENSIA is een gestandaardiseerde verantwoordingsmethode voor gemeenten op het gebied van informatiebeveiliging. ENSIA biedt gemeenten een efficiënte manier om verantwoording af te leggen over hun informatieveiligheid, gebaseerd op de Baseline Informatiebeveiliging Overheid (BIO). Het is een gezamenlijk initiatief van gemeenten, de Vereniging

van Nederlandse Gemeenten (VNG), en de ministeries van BZK en SZW.

Met ENSIA kunnen gemeenten eenmalig en op uniforme wijze verantwoording afleggen, zowel aan de gemeenteraad als aan de rijksoverheid. Dit vereenvoudigt de rapportageverplichtingen, biedt inzicht in de staat van informatieveiligheid en sluit aan op de planning en control-cyclus van gemeenten. Gemeentebesturen krijgen hierdoor beter overzicht over de informatieveiligheid en kunnen waar nodig bijsturen en verantwoording afleggen aan de gemeenteraad.

Via ENSIA leggen gemeenten verantwoording af over informatieveiligheid aan het hoogste politieke orgaan, de gemeenteraad. Tegelijkertijd voldoen zij aan de

eisen van de rijksoverheid voor het gebruik van landelijke voorzieningen. ENSIA is niet alleen van toepassing op gemeenten, maar wordt ook gebruikt door provincies, waterschappen en enkele onderdelen binnen de rijksoverheid.

ENSIA als Sleutel tot Digitale Veerkracht

ENSIA speelt een cruciale rol bij het verbeteren van de digitale weerbaarheid van gemeenten en het waarborgen van de betrouwbaarheid en veiligheid van informatie(systemen). Met ENSIA kunnen gemeenten voldoen aan hun verantwoordingsplicht, proactief sturen op informatieveiligheid en bijdragen aan een veilige, betrouwbare overheid die haar burgers en ondernemers optimaal ondersteunt.



Hoofdstuk 2 **Waarom AudITvision?**

Bij AudITvision geloven we dat een ENSIA-audit méér moet opleveren dan een verplicht vinkje of een rapport. Een goede audit geeft richting, versterkt het bestuurlijk vertrouwen én helpt uw organisatie structureel vooruit. Daarom kiezen steeds meer gemeenten voor AudITvision als hun ENSIA-partner.

Wat ons onderscheidt?



Inhoudelijk sterk én normgericht

Ons team bestaat uit 12 ervaren specialisten, waaronder 5 Register EDP-auditors (RE's). We hebben diepgaande kennis van zowel de BIO

(Baseline Informatiebeveiliging Overheid) als ISO/IEC 27001. Daardoor zijn we in staat om technische en organisatorische maatregelen scherp te beoordelen én te vertalen naar praktische adviezen die passen bij de gemeentelijke context.



Kwaliteit zonder 'afvinklijstjes'

Wij toetsen op basis van risico's, niet op papierwerk. Onze aanpak is grondig, maar altijd met oog voor proportionaliteit en bestuurlijke relevantie. Geen

bureaucratie, wél inzicht en houvast. Daarmee voegen we échte waarde toe aan uw informatiebeveiliging.



Samenwerking centraal

We werken als partner, niet als controleur. We denken mee over realistische verbetermaatregelen, adviseren opbouwend en zijn altijd beschikbaar voor overleg. Ook ná de audit

blijven we betrokken: met een jaarlijkse evaluatie bespreken we wat goed ging, waar het beter kan en hoe we het volgende ENSIA-jaar slimmer inrichten.



Ervaring met complexe situaties

Uitbesteding, samenwerkingsverbanden of ketenverantwoordelijkheid? Wij zijn vertrouwd met zowel de carve-out als de inclusive benadering, en helpen u om

verantwoord om te gaan met externe rapportages en taken. Daarbij houden we altijd rekening met de eisen uit de BIO en de kaders van de ENSIA-verklaring.



Geen verrassingen, wél duidelijkheid

Bij AudITvision geldt: afspraak is afspraak. We hanteren vaste prijzen, geen meerwerk, en blijven flexibel als de planning wijzigt. Ook extra toelichtingen of

sparmomenen zijn gewoon inbegrepen. Transparantie en betrouwbaarheid staan bij ons voorop.

"Het prettige aan AudITvision is dat ze niet alleen controleren, maar echt willen bijdragen aan verbetering. Kritisch waar nodig, maar altijd constructief en professioneel."

- Informatieadviseur, gemeente (middelgroot)

Hoofdstuk 3 Onze aanpak in 7 fasen

Ons doel is om gemeenten op de juiste manier te ondersteunen bij het uitvoeren van de ENSIA-audit voor het verantwoordingsjaar 2025. De audit richt zich op de naleving van de Baseline Informatiebeveiliging Overheid (BIO) en andere relevante normen. De reikwijdte omvat alle processen en systemen die onder de ENSIA-verantwoordingsplicht vallen.

Als AudITvision zijn we graag betrokken vanaf het begin van de verantwoordingsperiode. Op die manier zorgen we ervoor dat we op de hoogte zijn van alle ontwikkelingen binnen de gemeente en kunnen we indien nodig tijdig anticiperen op ontwikkelingen. We zullen gedurende de gehele periode ook als vraagbaak functioneren als u vragen heeft over de audit. U krijgt één aanspreekpunt die u altijd kunt benaderen.



1. Voorbereiding

Mei – augustus 2025
Creëert een stevige basis voor audit



2. Zelfevaluatie

September – december 2025
Gemeente voert intern controle uit



3. Interim controle (indien gewenst)

November 2025 – februari 2026
Tussentijdse terugkoppeling omtrent DigiD en Suwinet



4. De audit, verantwoording en verbetering

Januari – maart 2026
Formele verantwoording wordt ingediend



5. Verantwoording aan B&W en toezichthouders

30 april 2026
Rapportages worden voorgelegd



6. Opstellen en versturen verslaglegging

Mei – juli 2026
Verslag wordt aangeboden aan provincie



7. Jaarlijkse evaluatie

Bespreken van verbeterpunten voor de volgende cyclus

“AudITvision heeft voor ons onderzoek gedaan naar maar liefst 7 DigiD-koppelingen, waaronder enkele complexe meervoudige koppelingen. Het team schakelde snel, dacht actief mee en werkte transparant en professioneel. We hebben de samenwerking als zeer prettig en flexibel ervaren, inhoudelijk sterk én toegankelijk in communicatie. We zouden AudITvision zonder twijfel opnieuw inschakelen.”

- Informatieadviseur, gemeente (middelgroot)

1

Fase 1: Voorbereiding

Periode: Mei – Augustus 2025

Deze fase is gericht op het creëren van een stevige basis voor de ENSIA-audit. De gemeente stelt een project-team samen, brengt de scope en betrokken systemen in kaart, en zorgt dat het normenkader actueel is. De ENSIA-coördinator richt de portal in, en medewerkers worden geïnformeerd en getraind.

De ENSIA-vragenlijsten zijn vanaf 1 juli 2025 beschikbaar voor de gemeenten en zij hebben tot 31 december 2025 de tijd om de vragenlijsten in te vullen en op te leveren. Inleveren kan pas als alle vragen zijn beantwoord.

Activiteiten

Mei/juni 2025

- Startbijeenkomst met alle betrokkenen
- Inventarisatie van processen, systemen en risico's
- Aanschrijven leveranciers en (sub)service-organisaties

Juni/juli 2025

- Actualiseren van het normenkader (BIO, ENSIA-eisen)
- Opstellen auditplanning en communicatieplan
- Juli – augustus 2025
- Training van betrokken medewerkers over ENSIA en de BIO
- Inrichten van ENSIA-portal met actuele gegevens
- Verzamelen en ordenen van bestaande documentatie en beleid

2

Fase 2: Zelfevaluatie

Periode: September – December 2025

De gemeente voert een zelfevaluatie uit, verzamelt bewijslast en voert interne controles uit. De ENSIA-coördinator binnen de gemeente beantwoordt alle vragenlijsten in ENSIA namens de gemeente. Specifieke domeinen zoals de RvIG (BRP en Reisdocumenten), BWKI (Suwinet), Logius (DigiD), en DGBRW (BAG, BGT, BRO) hebben hun eigen vragenlijsten. Voor deze systemen wordt de BIO-vragenlijst of een domeinspecifieke vragenlijst gehanteerd, afgestemd op de behoeften van elk domein. Eventuele tekortkomingen worden geanalyseerd en verbetermaatregelen opgesteld.

Activiteiten

September/oktober 2025

- Start van de interne controle en self-assessment
- Verzamelen van bewijsstukken voor elk normonderdeel
- Oktober/november 2025
- Uitvoeren interne audit door CISO en ENSIA-coördinator
- Analyse van bevindingen en identificatie tekortkomingen
- Opstellen en documenteren van verbetermaatregelen

Hoewel AuditVision als ENSIA-auditor geen formeel oordeel uitspreekt over de inhoud of uitvoering van het gemeentelijk verbeterplan, vinden wij het wél van belang om te toetsen of de door de gemeente vastgestelde bevindingen daadwerkelijk zijn geadresseerd. Wij kijken of deze bevindingen zijn opgenomen in het verbeterplan, of ze realistisch zijn en of ze in verhouding staan tot de gesignaleerde risico's.

Eventuele tekortkomingen die tijdens onze audit naar voren komen, brengen wij actief onder de aandacht van de opdrachtgever. Dit stelt het college in staat om – waar nodig – de bevindingen te verwerken in het verbeterplan én in de collegeverklaring. Zo dragen we bij aan een zorgvuldig en transparant verantwoordingsproces.



3

Fase 3: Interim controle (indien gewenst)

Periode: November 2025 – Februari 2026

De IT-audit kan (pas) worden afgerond nadat de vragenlijsten zijn ingeleverd en de collegeverklaring is opgesteld door de gemeente. De gemeente heeft echter vaak de behoefte om tussentijds een terugkoppeling te ontvangen van de IT-auditor over de status van DigiD en Suwinet binnen de gemeente. Indien gewenst kunnen we een pre-audit of interim audit uitvoeren waarbij wij de DigiD en Suwinet-normen tussentijds toetsen, het proces van oplevering beoordelen en de uitkomsten rapporteren aan de gemeente. De gemeente wordt op deze wijze in de gelegenheid gesteld de nodige verbeteringen door te voeren alvorens de vragenlijsten definitief worden ingeleverd.



4

Fase 4: De audit, verantwoording en verbetering

Periode: Januari – Maart 2026

In deze fase vindt de audit plaats en wordt de formele verantwoording ingediend. De auditresultaten worden besproken met bestuurders en de gemeenteraad. Daarnaast vindt een evaluatie plaats van het auditproces en worden verbetermaatregelen geïmplementeerd ter voorbereiding op de volgende auditcyclus.

Voor gevoelige domeinen zoals DigiD en Suwinet stelt de coördinator een collegeverklaring op die vervolgens door ons als auditor wordt getoetst. Dit resulteert in:

- Een collegeverklaring voor DigiD en Suwinet.
- Rapportages voor de BAG, BGT, en BRO.
- Samenvattingen voor BRP en Reisdocumenten.
- Een volledige ENSIA-rapportage voor de gemeenteraad. De collegeverklaringen en verantwoordingsrapportages worden aangeboden aan het college van B&W voor een overzichtelijke en betrouwbare verantwoording.

Activiteiten

Januari/februari 2026

- Uitvoering van de externe ENSIA-audit
- Bespreken van de (concept) auditbevindingen met management
- Januari/februari 2026
- Finaliseren van de auditrapportage
- Voorbereiden van de bestuurlijke verantwoording

Maart 2026

- Indienen van de ENSIA-verantwoording via de ENSIA-portal
- Presenteren van de resultaten aan de gemeenteraad en college

5

Fase 5: Verantwoording aan B&W en Toezichthouders

Maart 2026

- Evaluatie van het ENSIA-proces met alle betrokkenen
- Bijwerken van informatiebeveiligingsbeleid op basis van bevindingen
- Voorbereidingen treffen voor verantwoordingsjaar 2026/2027

Na goedkeuring van de collegeverklaringen en verantwoordingsrapportages door het College van B&W, worden de documenten geüpload in het ENSIA-systeem. Rapportages voor BRP en Reisdocumenten worden via de Kwaliteitsmonitor van RvIG gedeeld. Deze tijdige verantwoording zorgt dat alle toezichthouders uiterlijk op 30 april 2025 de benodigde rapportages ontvangen.

Activiteiten

30 april 2026

- Uiterlijke datum indienen rapportages

6

Fase 6: Opstellen en versturen Verslaglegging

Vanaf mei wordt in het jaarverslag van de gemeente in een aparte paragraaf aandacht besteed aan de informatiebeveiliging. Dit overzicht helpt het College om helder te rapporteren aan de gemeenteraad. Na goedkeuring door de gemeenteraad worden de jaarstukken vóór 15 juli door het college aan de provincie gestuurd.

Activiteiten

1 mei 2026

- Start opstellen en beoordelen jaarverslag

15 juli 2026

- Uiterlijke datum versturen jaarstukken aan Provincie

7

Fase 2: Jaarlijkse evaluatie: leren en verbeteren

Periode: September – December 2025

Bij AudITvision stopt het traject niet na het indienen van de ENSIA-verantwoording. Wij hechten veel waarde aan continue verbetering en voeren daarom jaarlijks een evaluatiegesprek met onze klanten. Tijdens deze sessie bespreken we wat er goed ging in het auditproces, waar knelpunten zaten, en welke onderdelen efficiënter of effectiever kunnen.

We kijken samen terug op de samenwerking, de interne voorbereiding, de kwaliteit van de aangeleverde documentatie en de communicatie. Daarnaast bespreken we hoe we het volgende ENSIA-jaar slimmer kunnen inrichten – zowel voor de gemeente als voor ons als auditor.

Deze evaluatie is niet verplicht, maar wordt door onze klanten als zeer waardevol ervaren: het versterkt de samenwerking, verhoogt de auditkwaliteit en helpt gemeenten om structureel te groeien in hun informatiebeveiliging en ENSIA-volwassenheid.

“Het evaluatiegesprek met AudITvision gaf ons concrete handvatten om het volgende ENSIA-jaar beter en efficiënter aan te pakken. Hun aanpak is scherp, betrokken en opbouwend.”

- Informatieadviseur, gemeente (middelgroot)



Hoofdstuk 4 Het normenkader

Een ENSIA-audit betreft een assurance-opdracht gericht op het geven van een oordeel met een redelijke mate van zekerheid, conform Richtlijn 3000 A (Attestopdracht). Het college van burgemeesters en wethouders komt met een collegeverklaring waarover de IT-auditor met redelijke mate van zekerheid een oordeel geeft.

Beoogde gebruikers van deze collegeverklaring en het assurancerapport (oordeel) van de IT-auditor zijn de gemeenteraad en de departementen die toezien op de informatieveiligheid van DigiD en Suwinet.

De uitvoering van de ENSIA audit dient in opdracht van

het college plaats te vinden. Doel van de ENSIA-audit is het verkrijgen van voldoende geschikte assurance-informatie om een oordeel met redelijke mate van zekerheid te verschaffen of de Collegeverklaring ENSIA inzake informatiebeveiliging van DigiD en Suwinet (inclusief de bijlage(n) bij de Collegeverklaring ENSIA DigiD en Suwinet waarnaar in de collegeverklaring wordt verwezen) van de gemeente, in alle van materieel belang zijnde aspecten, juist is. Hierbij zijn de eisen vanuit de regelgeving voor DigiD en Suwinet leidend.

De criteria voor een ENSIA IT-audit betreffen de normen inzake DigiD (Norm ICT-beveiligingsassessments DigiD en Suwinet voor gemeenten. De criteria worden ook in

de collegeverklaring kenbaar gemaakt en zijn daarmee toegankelijk voor de gebruikers. Het gaat om opzet en bestaan van de maatregelen per 31 december 2025 alsmede opzet, bestaan en werking van een aantal maatregelen (over een periode van 6 maanden – periode 1 juli – 31 december 2025) in het kader van DigiD-assessments.

Eventuele veranderingen / verbetermaatregelen in de periode tussen 31 december 2025 en de datum van afgeven van het assurancerapport dient het College in principe in de collegeverklaring toe te lichten. De verbetermaatregelen / het verbeterplan betreft de auditor in zijn onderzoek.



Hoofdstuk 5 Uitbesteding en externe partijen

DigiD

Wanneer gemeenten taken rondom DigiD hebben uitbesteed, volgt AudITvision de gangbare carve-out methode. Wij baseren ons op de assurancerapporten die de externe dienstverleners aanleveren. Deze rapporten worden door ons niet inhoudelijk getoetst, maar wij verwijzen ernaar in de ENSIA-auditrapportage. Via de ENSIA-tooling zorgen we dat deze documenten op de juiste wijze worden opgenomen en beschikbaar zijn voor toezichthouders.



Suwinet

Ook bij uitbesteding van processen waarbij Suwinet-gegevens worden gebruikt, blijft de gemeente eindverantwoordelijk. AudITvision beoordeelt in dat geval het werk van andere (interne of externe) IT-auditors, bijvoorbeeld in samenwerkingsverbanden. Onze voorkeur gaat uit naar de carve-out benadering,

mits ondersteund met een betrouwbaar assurance-rapport. Wij hanteren hierbij de vereisten uit Richtlijn 3000, waaronder toetsing op deskundigheid, onafhankelijkheid en kwaliteit van het uitgevoerde werk.

Onze werkwijze

AudITvision adviseert om bij uitbesteding altijd te zorgen voor een geldig assurancerapport (volgens Richtlijn 3000, ISAE 3402 of vergelijkbaar). Dit maakt het voor ons mogelijk om een zorgvuldige en onderbouwde ENSIA-audit uit te voeren op basis van de carve-out methode, zonder dat de verantwoordelijkheid bij de gemeente verloren gaat.

Geen assurancerapport?

AudITvision voert aanvullend onderzoek uit

Indien een externe partij géén geldig assurancerapport kan overleggen (bijvoorbeeld conform Richtlijn 3000 of ISAE 3402), kan AudITvision – in opdracht van de gemeente – aanvullend onderzoek uitvoeren bij de betreffende partij. Dit gebeurt volgens de **inclusive benadering**, waarbij onze auditor direct onderzoek doet naar de naleving van ENSIA-normen binnen de uitbestede processen.

Voorwaarde is dat de contractuele afspraken tussen de gemeente en de externe partij deze auditactiviteiten toestaan. Als dat het geval is, neemt AudITvision de volledige vaktechnische verantwoordelijkheid voor het onderzoek, inclusief risicoanalyse, controleaanpak, dossierreview en beoordeling van bevindingen. Indien de externe partij al werkzaamheden heeft verricht op basis van ENSIA-normen, kunnen wij die meenemen in onze beoordeling, mits deze goed zijn onderbouwd in de rapportage (bijv. via een bijlage zoals bij een SOC 2 of ISAE 3402 type 2 rapport).



Ons uiteindelijke doel blijft dat de externe partij op termijn een volledig assurance-rapport kan overleggen conform Richtlijn 3000 (bij voorkeur 3000A). Een ISO 27001-certificaat volstaat hiervoor niet.

De controleperiode voor serviceorganisaties (en sub-serviceorganisaties) is ook minimaal 6 maanden. Rekening houdend met de wensen van gemeentelijke aansluithouders om voldoende gelegenheid te hebben om de ENSIA tooling in te vullen, zal het assurance-rapport voor gemeenten uiterlijk 15 oktober gereed moeten zijn. Dit betekent voor serviceorganisaties die DigiD webapplicaties leveren aan gemeenten dat de controle periode in de praktijk 1 april- 30 september zal zijn.

Hoofdstuk 6 Transparante kosten en tarieven

Een veelgestelde (en begrijpelijke) vraag is: wat kost een ENSIA-audit? We horen regelmatig bedragen voorbijkomen die niet in verhouding staan tot de werkzaamheden – en dat vinden wij onnodig. AuditVision staat voor transparantie en redelijkheid, ook als het om kosten gaat.

De exacte prijs is afhankelijk van factoren zoals het aantal aansluitingen, de complexiteit van de uitbesteding en de mate van voorbereiding binnen de gemeente. Maar op basis van de honderden audits die we de afgelopen jaren hebben uitgevoerd, kunnen we duidelijke richtlijnen geven.

Voor gemeenten met 1 tot 3 DigiD- of Suwinet-aansluitingen, kunt u doorgaans rekenen op een totale doorlooptijd van 24–40 uur, afhankelijk van de situatie. We hanteren een vast uurtarief van €125,-, zonder verborgen kosten of meerwerk achteraf. Ook de hertest is geen meerwerk en zit in ons fixed tarief inbegrepen.

Wilt u vooraf een exacte inschatting ontvangen? Neem gerust contact met ons op voor een vrijblijvende offerte of intakegesprek.

Hoe zijn onze tarieven opgebouwd?

Om gemeenten vooraf duidelijkheid te geven over de kosten, werken wij met vaste prijzen per onderdeel. Zo weet u precies waar u aan toe bent – zonder verrassingen achteraf.

Hiernaast ziet u onze basisstructuur voor de ENSIA-audit (2025/2026):

Aansluitingen

Eerste DigiD aansluiting	€2.500
Extra DigiD aansluiting	+ € 1.000
Eerste Suwi aansluiting	€2.500
Extra Suwi aansluiting	+ € 1.000
ENSIA assuranceverklaring	€2.000
Extra ENSIA assuranceverklaring	+ € 1.000

Deze bedragen zijn gebaseerd op een gemiddeld traject met normale complexiteit en voorbereiding. Alles is inbegrepen: intake, planning, afstemming, toetsing, rapportage en eventuele toelichting richting bestuur of toezichthouders.

Indien na het ondertekenen van de offerte blijkt dat er koppelingen bij of af moeten dan geldt hetzelfde prijs-model.

Wilt u een maatwerkofferte ontvangen op basis van uw specifieke situatie? Neem dan gerust vrijblijvend contact met ons op.

“Wij hebben opnieuw gekozen voor AuditVision als ENSIA-auditor. In de afgelopen jaren hebben zij bewezen niet alleen vakinhoudelijk sterk te zijn, maar ook nauwkeurig, betrouwbaar en prettig in de samenwerking. Tijdens de aanbesteding scoorde AuditVision bovendien niet alleen hoog op kwaliteit, maar bleken zij ook aanzienlijk voordeliger dan andere aanbieders. Die combinatie gaf voor ons de doorslag.”

- Informatiebeveiligingsadviseur grote gemeente (Zuid-Nederland)



Wilt u een ENSIA-audit laten uitvoeren of informatie over deze verklaring?

Neem contact op, bel **088-2028700** of mail **info@auditvision.nl** om vrijblijvend te praten over de mogelijkheden en oplossingen. AuditVision helpt u graag verder!

audITvision b.v.
Van der Houven van Oordtlaan 2
7316 AH Apeldoorn
t. 088-2028700

info@auditvision.nl
www.auditvision.nl

AudITvision
IT-auditors

**Uw partner voor een
betrouwbare overheid**