

**Speciaal ontwikkeld
voor de (semi)overheid!**

2-daagse praktijktraining

Risicomanagement voor privacy & informatiebeveiliging

Leer risico's concreet te maken en overtuig uw organisatie tot actie

Met deze training:

- ▶ Beheert u met een integrale aanpak effectief privacy- en securityrisico's.
- ▶ Leert u hoe u bewustwording, eigenaarschap en overtuigingskracht binnen uw organisatie vergroot.
- ▶ Weet u wat AI-privacyrisico's zijn en hoe u deze beheerst.
- ▶ Ontvangt u praktijkvoorbeelden en direct toepasbare oplossingen

Ook mogelijk als
InCompany



**Krijg les van experts
uit het vakgebied**



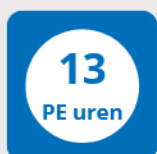
Menno Methorst
L2P



Arjan Kremer
Perium B.V.



Femke Hendrikx
Gemeente Amersfoort



**Data
Locatie
Website**

**13 & 14 april 2026
Amsterdam & online
outvie.nl/risicomanagement-privacy**

Meer data, meer risico: versterk uw grip op privacy en informatiebeveiliging

Overheden verzamelen en koppelen meer persoonsgegevens dan ooit, waardoor de kans op fouten en datalekken toeneemt. Het recente datalek bij Bevolkingsonderzoek Nederland (juli 2025), waarbij gegevens van bijna half miljoen deelnemers werden blootgesteld, toont de kwetsbaarheid. Zulke incidenten ondermijnen het vertrouwen van burgers en benadrukken de noodzaak van zorgvuldig risicomanagement.

Daarnaast omarmen overheidsinstanties steeds vaker AI-systemen, die ook serieuze privacy en informatiebeveiligingsrisico's met zich meebrengen. Uit onderzoek van de Algemene Rekenkamer blijkt dat bij meer dan 50% van de gebruikte AI-systemen in de overheid, geen risicoafweging is gemaakt.

Welke van deze kwesties herkent u in uw werk?

- Bent u in staat om privacy- en informatiebeveiligingsrisico's te herkennen, beoordelen en prioriteren?
- Wordt AVG-naleving bemoeilijkt door andere belangen?
- Hoe waarborgt u dat uw organisatie de BIO-verantwoordelijkheden (of andere geldende normen) strikt naleeft om boetes en imagoschade te voorkomen?
- Ervaart u weerstand bij het bestuur of management om privacy- en beveiligingsrisico's serieus te nemen en budget vrij te maken?

Tijdens deze training:

- Zet u een organisatiebreed risicomanagement-systeem op dat aansluit op BIO2-, NIS2- en AVG-verplichtingen.
- Identificeert, beoordeelt en prioriteert u met behulp van praktische methoden en risicomatrices huidige en toekomstige privacy- en securityrisico's.
- Communiceert u overtuigend over risico's en creëert u eigenaarschap bij bestuur, management en proceseigenaren.
- Analyseert, beheerst en integreert u AI-risico's in het bestaande risicomanagementbeleid en governance-structuur.
- Weet u hoe leiders complexe uitdagingen aanpakken en kent u direct toepasbare voorbeelden en best practices.

Voor wie?

De training is voor medior en senior professionals in privacy, data en informatiebeveiliging die verantwoordelijk zijn voor risicomanagement binnen overheid, zorg, onderwijs of andere semipublieke sector.

- Privacy officers
- Functionaris Gegevensbescherming
- Data protection officers
- Head of privacy / data
- Information Security Officers / CISO's
- Chief Information Officer / CIO
- Informatiebeveiligingsadviseur
- Risk officers
- Informatiemanager / Informatie-analisten
- Datamanagers / Data-analisten
- Chief data officer
- Data security officers

▶ Na deze training analyseert u privacy-, security- en AI-risico's scherp(er) en vertaalt u deze naar effectieve maatregelen. U neemt regie over de borging van AVG- en BIO-verantwoordelijkheden waarmee u aantoonbaar de weerbaarheid van uw organisatie verhoogt. Met onderbouwde adviezen over privacy en security overtuigt u uw bestuur en management en versterkt u uw rol binnen uw organisatie.

► Uw docenten en gastsprekers



Menno Methorst, *Senior Information Security Advisor, L2P*

Menno is een gepassioneerde professional op het gebied van risico- en informatiebeveiligingsmanagement met ervaring als CISO in complexe, multinationale organisaties. Met zijn unieke achtergrond in onderwijs, theater en consultancy zet hij zich in om de beveiligingscommunity te laten groeien en organisaties te helpen om het volgende niveau van risico- en beveiligingsvolwassenheid te bereiken met een creatieve, maar pragmatische aanpak.



Arjan Kremer, *oprichter & CISM, Perium B.V.*

Arjan Kremer, bedrijfskundige en oprichter van Perium, biedt expertise in onder andere risicomanagement, digitale transitie en informatiebeveiliging. Met een achtergrond in IT-strategie en governance helpt hij organisaties bij het versterken van hun digitale weerbaarheid en het voldoen aan complexe regelgeving. Als toezichthouder en gastspreker deelt hij waardevolle inzichten in proportioneel risicomanagement en stimuleert hij effectief leiderschap. Zijn praktische benadering en focus op operationele efficiëntie maken hem tot een gewaardeerde adviseur.



Femke Hendrix, *FG, Gemeente Amersfoort*

Femke Hendriks is Functionaris Gegevensbescherming bij Gemeente Amersfoort. Ze heeft jarenlange ervaring als FG binnen verschillende gemeenten en is medeontwikkelaar van de training 'Privacy in gemeentelijke organisaties: invloedrijk communiceren'. Femke is sociaal, analytisch en leergierig, met een passie voor datagedreven werken binnen het publieke domein. Ze studeerde Criminologische Wetenschappen aan de Universiteit Gent.

► Programma

Dag 1 | 13 april 2026 | 9:00 - 17:00

Module 1 Risicomanagement: fundamenten & strategieën

In deze module leren deelnemers de basis van risicomanagement in relatie met de AVG, NIS2 en informatiebeveiligingsnormen als ISO 27001 en 27005. Ze ontwikkelen een effectief risicomanagementsysteem, bepalen risicobereidheid en integreren risico's in de organisatie met de PDCA-cyclus.

- Wat is risicomanagement en welke rollen en definities zijn hierbij van belang?
- Hoe zet u een organisatiebreed risicomanagementsysteem op dat aansluit bij informatiebeveiligingsnormen (ISO, NIS2, BIO) en kaders voor privacy of andere compliance-eisen?
- Hoe stelt u een gedragen risicokader op?
- Hoe stelt u de risicobereidheid en risk appetite vast?
- Wat is de rol van risicomanagement binnen de PDCA-cyclus?

Menno Methorst, *Senior Information Security Advisor, L2P*

Praktijkoefening: oefenen met risico fundamenten

Aan de hand van een case oefenen de deelnemers hoe zij risico's formuleren en effectieve mitigerende maatregelen opstellen.

Module 2 Risico identificatie, beoordeling en beheersing

In deze module leren deelnemers risico's beheersen in drie stappen. Aan de hand van realistische casussen formuleren ze effectieve mitigerende maatregelen en kiezen ze de juiste opties voor een optimale risicobeheersing.

- **Risico identificatie:** Hoe identificeert u relevante risico's binnen jouw organisatie?
- **Risicobeoordeling en analyse:** Hoe beoordeelt u risico's en welke methoden en technieken gebruik je daarbij? Hoe stelt u een risicomatrix op?
- **Risicobeheersing:** Welke controle opties zijn er (hard en soft controls, preventief en repressief)? Hoe bepaalt u goede mitigerende maatregelen en hoe voert u beheersmaatregelen effectief uit

Menno Methorst, *Senior Information Security Advisor, L2P*

Opdracht Risico identificatie, beoordeling en beheersing:

Aan de hand van een case oefenen deelnemers met het formuleren van risico's en het opstellen van effectieve mitigerende maatregelen.

► Programma

Dag 2 | 14 april 2026 | 9:00 - 17:00

Module 3 Risicomanagement van AI

In deze module past u de theorie van de tweede module toe op een veelvoorkomend onderwerp, namelijk AI-tools. U krijgt handvatten om effectief risicomanagement toe te passen voor privacygevoelige informatie bij het ontwikkelen en gebruiken van AI-systemen. Aan de orde komen de drie praktische stappen van de vorige module, inclusief relevante wetgeving en beschikbare normenkaders. Een beknopte overview software en tooling die u kunnen helpen, zoals Privacy Enhancing Technologies, staat ook op het programma deze module.

- Hoe beheerst u **AI-risico's**?
- Wat zijn de **specifieke risico's en kansen** voor privacy en Informatiebeveiliging bij de inzet van AI?
- Met welke wet- en regelgeving op het gebied van AI moet u rekening houden?
- **Welke normenkaders voor AI** zijn beschikbaar en hoe bepaal ik welke geschikt is?
- Hulp bij risicomanagement: software en tooling (o.a. Privacy Enhancing Technologies)

Arjan Kremer, *Founder (CISM) Perium b.v.*

Opdracht: Risicolijst van privacygevoelige data bij inzet van een AI toepassing.

U vindt de opdracht vóór de start van de training in de leeromgeving en levert deze uiterlijk twee werkdagen van tevoren in bij de docent.

Module 4 Van awareness naar beweging in de organisatie – een integrale aanpak

In deze module leert u, aan de hand van praktijkvoorbeelden uit Gemeente Amersfoort, hoe u privacy- en securityrisico's vertaalt naar concrete maatregelen en met overtuigende communicatie eigenaarschap versterkt binnen een integrale aanpak. U ontdekt hoe u bewustwording omzet in besluitvorming en beweging binnen uw organisatie.

- Hoe krijgt u **privacy- en securityrisico's** op de agenda zodat iedereen zich ervan bewust is?
- Hoe overtuigt u bestuur en management van de noodzaak tot actie rond privacy en informatiebeveiliging?
- Herken de **dynamiek van het krachtenveld** en hoe u daar effectief in opereert.
- Welke **advies- en communicatiestijlen** helpen om invloedrijk te adviseren?
- Hoe bereidt u een goed **bestuursadvies** voor en welke scenario's neemt u daarin op?
- Wat zijn de noodzakelijke maatregelen en wie draagt het eigenaarschap?
- Hoe zorgt u voor **blijvende aandacht en opvolging** binnen de organisatie?
- Hoe herkent u bevorderende factoren en benut u deze om beweging te creëren?
- Hoe werkt u **integraal samen** met informatiebeveiliging en andere functies aan risicomanagement?

Femke Hendriks, *FG, Gemeente Amersfoort*

Opdracht: Oefen in de vorm van een rollenspel

Overtuig het bestuur van een fictieve organisatie de privacy- en informatiebeveiligingsrisico's waar zogezegd 'nooit iets misgaat'.

Risicomanagement voor privacy & informatiebeveiliging

Leer risico's concreet te maken en overtuig uw organisatie tot actie

Tickets	2-daagse praktijktraining	€ 2.099,-*
Data	13 & 14 april 2026	
Locatie	Amsterdam & online	

** incl. koffie, thee, uitgebreide lunch, digitale leeromgeving & lesmateriaal, begeleiding en feedback. Al onze prijzen zijn exclusief btw.*

Speciaal ontwikkeld voor de (semi)overheid!

Inschrijven

- **Website**
outvie.nl/risicomanagement-privacy
- **E-mail**
aanmelding@outvie.nl
- **Telefoon**
020 - 580 54 00



Contact



Heeft u vragen, wenst u advies?

Ik help u graag verder en ben bereikbaar via: 020-580 54 55 of per e-mail: j.stevens@outvie.nl.

Jeremy Stevens, opleidingsadviseur

InCompany

Op maat gemaakt

Maatwerk voor uw team?

Outvie biedt naast de mogelijkheid van een individuele training of opleiding ook trajecten die op maat worden gemaakt voor uw organisatie. Neem daarvoor contact op met onze InCompany adviseurs via: 020 - 580 54 00 of per e-mail: incompany@outvie.nl.



Outvie biedt als kennis- en netwerkorganisatie al meer dan 30 jaar de meest actuele vakinhoudelijke kennis voor professionals. Onze events en opleidingen, die onafhankelijk en door eigen marktonderzoek tot stand komen, bieden inhoudelijke diepgang, praktijkgerichte oplossingen en interactiviteit. Dé basis voor nieuwe oplossingen en (persoonlijke) ontwikkelingen in uw organisatie. Bekijk het volledige aanbod op **www.outvie.nl**.

Algemene voorwaarden

Op alle aanbiedingen zijn onze algemene voorwaarden van toepassing. Deze zijn gedeponeerd bij de K.v.K te Amsterdam, onder nummer 64458482. De algemene voor- waarden zijn te downloaden op onze website www.outvie.nl/algemene-voorwaarden en worden op verzoek kosteloos toegezonden.

CEDEO - gecertificeerd

CEDEO is een onafhankelijke keuringsinstantie die de kwaliteit van human resources dienstverleners meet en waarborgt. Recentelijk heeft CEDEO een marktonderzoek uitgevoerd onder de klanten van Outvie. Ruim 90% van de respondenten van het onderzoek was tevreden of zeer tevreden over de trainingen van Outvie!

