OUTVIE
Connecting Knowledge & Networking

Schrijf u in en ontvang een gesigneerd exemplaar van zijn nieuwste boek:

3-daagse training

Cyber Risk & Compliance Management

Voorbij compliance naar een effectieve, praktische cybersecurityaanpak

Deze hands-on training biedt u:

- Een **volledige update** van de meest actuele wetgeving zoals NIS2 en DORA.
- Concrete maatregelen om boetes en juridische aansprakelijkheid te voorkomen.
- **Unieke praktijkcases** van o.a. TomTom: leer van echte situaties.
- Checklists en tools voor een concreet beveiligingsplan.

Ook mogelijk als **InCompany**

Krijg les van deskundige docenten

waaronder

Brenno de Winter
De Winter Information Solutions

Godfried Boshuizen
CC Security

Cassandra Moons
TomTom

Arjen de Graaf
DNB

18 PE-uren

Data 23, 30 september en 5 oktober 2026
Locatie Amsterdam & Online
Website outvie.nl/cyber-risk-management

Golf aan ransomware treft Nederlandse organisaties. Zorg dat u voorbereid bent.

De Nederlandse infrastructuur is kwetsbaar. Volgens het Nationaal Cyber Security Centrum (NCSC) zijn organisaties onvoldoende voorbereid op digitale verstoringen en aanvallen. Vitale sectoren als zorg, energie en overheid lopen steeds groter risico op ontwrichting.

Organisaties hebben geen keuze meer: zij *moeten* voldoen aan strengere cybersecurity-eisen. Nieuwe wetgeving, zoals NIS2 en DORA, verplicht organisaties om hun digitale weerbaarheid te versterken. Bestuurders kunnen persoonlijk aansprakelijk worden gesteld bij nalatigheid.

Van regels naar resultaat: praktische training voor échte impact
Weet u hoe u de complexe regelgeving vertaalt naar concreet beleid? Twijfelt u over draagvlak of juiste aanpak?

De training Cyber Risk & Compliance Management biedt u praktische tools en actuele kennis om risico's te beheersen en eisen effectief te implementeren.

U leert beleid opstellen, incidenten managen en bewustzijn duurzaam borgen. Met handige checklists, voorbeelden en frameworks maakt u uw organisatie juridisch én operationeel weerbaarder.

Na afloop van de training:

- Gaat u naar huis met een praktisch plan om uw eigen organisatie cyberveilig te maken.
- Bent u volledig op de hoogte van de meeste actuele wet- en regelgeving.
- Kunt u duidelijke keuzes maken welke risico's u accepteert en welke u aanpakt.
- Overtuigt u uw bestuurders om meer budget te krijgen (dring aan op bestuurdersaansprakelijkheid!).
- Creëert u meer bewustwording bij uw collega's.
- Leer hoe u samenwerking in de keten versterkt om risico's écht te beheersen.

Tijdens de training werkt u samen aan praktijkgerichte vraagstukken en wisselt u ervaringen uit met andere deelnemers.

Na afloop heeft u geen standaard plan op papier, maar een plan van aanpak dat past bij de context van uw organisatie. U weet hoe u toezichtverwachtingen en wettelijke verplichtingen zoals NIS2 en DORA omzet in werkbare stappen, en hoe u dit kunt vertalen naar beleid, verantwoording en samenwerking met IT en bestuur.

Voor wie is deze training?

- Security managers
- (Chief) Information security officers (CISO's, ISO's), Security officers (SO'S)
- Beleidsmedewerker informatiebeveiliging

De training is ook te volgen voor professionals die betrokken zijn bij cybersecuritybeleid van hun organisatie, zoals:

- Privacy officers/FG's
- Manager servicedesk
- Compliance manager
- IT adviseur/ consultant
- IT Auditor

Online leeromgeving
Alle presentaties, video's, artikelen en huiswerk staan op onze online leeromgeving. Zo heeft u alle cursusinformatie op één plek! Hier kunt u ook contacthouden met andere deelnemers, of vragen stellen aan uw docent. U ontvangt het trainingsmateriaal bij de start van de training.

Uw docenten

Brenno de Winter, *ICT expert, eigenaar De Winter Information Solutions*
Met diepgaande kennis van informatiebeveiliging, privacybescherming en complexe juridische vraagstukken, biedt hij praktische inzichten en oplossingen. Brenno is bekend om zijn expertise in NIS2-compliance, cybersecuritybeleid en auditmethodologieën zoals Miauw. Als voormalig Journalist van het Jaar koppelt hij scherpe analyses aan heldere communicatie, waarmee hij professionals inspireert om kritische en verantwoordelijke keuzes te maken in de digitale wereld.

Godfried Boshuizen, *OT & IT Cyber security principal, CC Security*
Met bijna 30 jaar ervaring in beveiliging opereert Godfried Boshuizen op het snijvlak van OT en IT. Hij heeft uitgebreide ervaring in de maritieme sector en industrie en is een technische CISO met hands-on expertise in complexe infrastructuren. Bij FERM Rotterdam verdiepte hij zich in de NIS2-richtlijn en aankomende wetgeving. Godfried combineert technische knowhow met strategisch inzicht, waardoor hij beveiligingsproblemen effectief aanpakt en proactieve maatregelen implementeert voor kritieke infrastructuren.

Cassandra Moons, *Head of Compliance & Data Protection Officer, TomTom*
Cassandra is Head of Compliance | Data Protection Officer bij TomTom, specialist in navigatiesoftware, locatietechnologie en digital maps. Zij is verantwoordelijk voor advies en toezien op compliance ten aanzien van internationale privacy wet-en regelgeving, en daarnaast zijn ook product compliance en corporate compliance aandachtsgebieden voor haar Cassandra is een doorgewinterde juridische en compliance professional gespecialiseerd in AI, connected auto's, navigatiesoftware en locatietechnologie. Ze heeft rechten gestudeerd aan de Universiteit van Leiden en is sinds eind 2018 werkzaam bij TomTom. Daarvoor heeft ze als in-house legal counsel ervaring opgedaan bij verschillende divisies van ING en Coolblue. Cassandra spreekt regelmatig op internationale privacy / AI conferenties en seminars.

Arjen de Graaf, *Chief Information Officer, De Nederlandsche Bank*
Arjen de Graaf is als CIO verantwoordelijk voor de digitale transformatie bij De Nederlandsche Bank. Met ruime ervaring op programma- en bestuursniveau in diverse sectoren, stuurt hij complexe verandertrajecten aan en vertaalt hij strategische doelstellingen naar concrete resultaten. Arjen heeft een bewezen staat van dienst in het versterken van digitale weerbaarheid en het realiseren van effectieve samenwerking tussen IT, beleid en bestuur. Daarbij is het resultaat voor hem net zo belangrijk als de weg er naartoe.

Programma

Woensdag 23 september 2026 | 09:00 - 17:00

De basis van cybersecurity: regels en principes

MODULE 1 - De spelregels voor cybersecurity: Wetten, normen en praktijk

- Introductie in de wereld van normen en wetten (zoals CBW, AI Act, NIS2, ISO 27001, BIO2) en wat die betekenen voor uw organisatie.
- Wat is het verschil tussen NIS2 en CBW? We leggen het helder uit.
- Wie valt er onder deze wetten? De belangrijkste vragen bij de naleving.
- De juridische kant: Hoe gaat u om met de complexe wetgeving in Europa?
- Praktische checklists om direct mee aan de slag te gaan.

Docent: ***Brenno de Winter,*** *ICT expert, eigenaar De Winter Information Solutions*

De visie vanuit data protection over compliance
Wat is er belangrijk is bij de samenwerking tussen Security en DPO/Privacy bij de invoering van nieuwe wetgeving?
Gastdocent: ***Cassandra Moons,*** *Head of Compliance & Data Protection Officer, TomTom*

MODULE 2 - Essentiële beveiligingsmaatregelen voor compliance en weerbaarheid

Welke basismaatregelen zijn noodzakelijk voor een effectieve cybersecurity-aanpak? Ontdek de essentiële maatregelen om uw organisatie veilig te houden en collega's mee te krijgen in een sterke beveiligingscultuur.

- De belangrijkste basismaatregelen voor het voldoen aan de regels en een goede cyberhygiëne.
- Essentiële cybersecuritymaatregelen voor elke organisatie: van risicobeheer tot toegangscontrole.
- Compliance in de praktijk: Hoe stelt u basismaatregelen effectief in, ongeacht de grootte van uw organisatie?
- Hands-on praktijkvoorbeelden en checklists die u helpen cybersecurity compliance structureel te borgen in uw organisatie.

Docent: ***Godfried Boshuizen,*** *OT & IT Cyber security principal, CC Security*

Programma

Woensdag 30 september 2026 | 09:00 - 17:00

Omgaan met risico's en problemen: wat te doen bij een cyberaanval

MODULE 3 - Risico's in kaart brengen

- Risicoanalyses uitvoeren: Welke documenten en tools heeft u nodig?
- Risico's afwegen: Welke risico's kunt u accepteren en welke moet u aanpakken?
- Welke risico's moet u in kaart brengen? Hoe bepaalt u de grenzen van risicoanalyse binnen uw organisatie?
- Inzicht in risicobeheerstrategieën: Hoe neemt u de juiste beslissingen in een complexe IT- en OT-omgeving?
- *Praktijk:* Oefenen met een risico-inventarisatie.

Praktijkopdracht: Oefen met het maken van een risico-inventarisatie die u daarna kunt toepassen op uw eigen organisatie

Docent: ***Brenno de Winter,*** *ICT expert, eigenaar 'De Winter Information Solutions'*

MODULE 4 - Als het misgaat – een plan voor incidenten, crises en business continuïteit

Leer hoe u met de juiste voorbereiding en aanpak snel kunt reageren, effectief communiceert en de bedrijfscontinuïteit waarborgt.

- Een crisisorganisatie opzetten: Hoe zorgt u voor snelle communicatie en herstel na een incident? (Hin en Hon-modellen)
- Effectief incidentbeheer: Stappen voor herstel en open communicatie tijdens een crisis.
- Het belang van openheid: Hoe geeft u openheid van zaken tijdens incidenten, zonder uw organisatie in gevaar te brengen?
- Crisiscommunicatie en herstel: Hoe bent u snel weer 'back in business' na een cyberincident?
- Handige checklists voor incidentbeheer
- Beperk uitval en waarborg de bedrijfscontinuïteit bij aanvallen

Docent: ***Brenno de Winter,*** *ICT expert, eigenaar 'De Winter Information Solutions'*

Praktijkopdracht: Zet de contouren op van een incident respons plan voor uw organisatie

Programma

Maandag 5 oktober 2026 | 09:00 - 17:00

Samenwerken aan veiligheid: bewustwording, beleid, en ketenaanpak

MODULE 5 - De menselijke factor: bewustwording, gedragsverandering en phishing preventie

Technische maatregelen alleen zijn niet genoeg; mensen blijven de zwakste schakel in cybersecurity. Ontdek hoe u bewustwording vergroot, risicobesef versterkt en medewerkers en bestuurders in beweging krijgt om écht veiliger te werken.

De visie van een CIO in de bancaire sector. Van bestuurstafel tot werkvloer: awareness als sleutel tot digitale continuïteit
Security-awareness is geen afvinkoefening, maar een strategische noodzaak. Hoe zorgt u ervoor dat alle lagen van de organisatie doordrongen raken van het belang van digitale weerbaarheid? Ontdek hoe u awareness duurzaam verankert in beleid, gedrag en cultuur – en hoe u beveiliging ontwikkelt tot een gedeelde verantwoordelijkheid binnen de hele organisatie.

Van bestuurstafel naar werkvloer: Awareness als strategische noodzaak
Hoe zorgt u dat awareness geen afvinkoefening blijft, maar een integraal onderdeel wordt van de organisatiecultuur, waarbij zowel bestuurders als medewerkers begrijpen waarom security essentieel is?

Gastdocent: ***Arjen de Graaf,*** *Chief information Officer, De Nederlandsche Bank*

MODULE 6 - Van regels naar weerbaarheid: Cybersecurity beleid en de praktische uitvoering

Beleid telt pas mee als het wordt uitgevoerd in gedrag, processen en besluitvorming binnen de hele organisatie. Een beleid op papier is niet genoeg; het gaat om de uitvoering. Leer hoe u securitymaatregelen vertaalt naar de praktijk, draagvlak creëert voor budget en samenwerking in de keten versterkt om risico's écht te beheersen.

- Ontdek hoe u bezwaren omdraait naar productieve gesprekken
- Leer hoe u verborgen drijfveren door de juiste vragen begrijpt en weerstand aanpakt
- Krijg de tips om op een dieper niveau te overtuigen zonder te manipuleren of te pushen
- Oefen met technieken om onder druk effectief en veerkrachtig te blijven

Docent: ***Brenno de Winter,*** *ICT expert, eigenaar 'De Winter Information Solutions'*

Programma

(Vervolg) Maandag 5 oktober 2026 | 09:00 - 17:00

Samenwerken aan veiligheid: bewustwording, beleid, en ketenaanpak

MODULE 6 - Van regels naar weerbaarheid: Cybersecurity beleid en de praktische uitvoering

Beleid telt pas mee als het wordt uitgevoerd in gedrag, processen en besluitvorming binnen de hele organisatie. Een beleid op papier is niet genoeg; het gaat om de uitvoering. Leer hoe u securitymaatregelen vertaalt naar de praktijk, draagvlak creëert voor budget en samenwerking in de keten versterkt om risico's écht te beheersen.

- Hoe stelt u effectief cybersecuritybeleid op? Wat zijn de eerste stappen om compliance om te zetten in concrete plannen?
- Van compliance naar cyberweerbaarheid: Hoe voert u maatregelen in die verder gaan dan alleen voldoen aan de wet?
- Budget en uitvoering: Hoe krijgt u voldoende middelen om uw beleid uit te voeren?
- Supply chain security: Hoe zorgt u ervoor dat u als opdrachtgever voldoet aan regelgeving zoals NIS2? Hoe werkt u samen met opdrachtgevers en leveranciers om risico's te beheersen?
- Checklists en tools voor supply chain security.
- Voorbeelden van goed beleid en praktische tips.

Praktijkopdracht: Vul een RASCI-matrix in over de rollen en verantwoordelijkheden van een leverancier in uw organisatie.

Docent: ***Brenno de Winter,*** *ICT expert, eigenaar 'De Winter Information Solutions'*

Cyber Risk & Compliance Management

Voorbij compliance naar een effectieve, praktische cybersecurityaanpak

Tickets	3-daagse training	€ 2.999,-*
Data	23, 30 september en 5 oktober 2026	
Locatie	Amsterdam & Online	

**incl. koffie, thee, uitgebreide lunch en digitale leeromgeving & lesmateriaal.*

De prijs is excl. BTW

Inschrijven

- **Website**
  outvie.nl/cyber-risk-management
- **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 5455 of per e-mail via 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 via incompany@outvie.nl.

Cedeo-erkend Bedrijfsopleidingen Open

Cedeo-erkend Bedrijfsopleidingen Maatwerk

OUTVIE
Connecting Knowledge & Networking

Outvie biedt als kennis- en netwerkorganisatie al meer dan 30 jaar de meest actuele vakinhoudelijke kennis voor professionals. Onze conferenties en opleidingen, die onafhankelijk en door eigen markt-onderzoek tot stand komen, bieden inhoudelijke diepgang, praktijkgerichte oplossingen en zijn altijd interactief. 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 voorwaarden 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!