

GOED TOEZICHT IN HET DIGITALE TIJDPERK

STRATEGIE, RISICO'S EN TOEZICHT
OP DIGITALISERING



MASTERCLASS VOOR
BESTUURDERS EN
TOEZICHTHOUDERS

FRIS
TOEZICHT

INTRODUCTIE

Digitalisering verandert het speelveld voor bestuur en toezicht

Technologische ontwikkelingen, en in het bijzonder kunstmatige intelligentie, veranderen organisaties in hoog tempo. Processen worden niet alleen geautomatiseerd en besluitvorming wordt niet langer alleen ondersteund door informatiesystemen. Processen en besluitvorming worden autonoom door zelflerende 'algoritmen'. Organisaties worden steeds afhankelijker van digitale infrastructuren en internationale technologiebedrijven.

Het Rapport Wennink ('De route naar toekomstige welvaart') laat zien dat investeringen in digitalisering en AI, veiligheid en weerbaarheid (cybersecurity) belangrijke domeinen zijn voor de toekomst van Nederland. Digitalisering ontwikkelt zich tot structurele factor in onze economie en samenleving. Technologie verschuift van een ondersteunende functie naar een strategische factor die direct raakt aan governance, risicobeheersing en de continuïteit van organisaties.

De inzet van digitalisering en AI heeft daarnaast gevolgen voor het personeelsbestand van organisaties. Nieuwe technologie leidt tot verschuivingen in de kennis en vaardigheden die binnen organisaties nodig zijn. Bestaande functies veranderen of verdwijnen, terwijl nieuwe expertise op het gebied van data, technologie en digitale veiligheid steeds belangrijker wordt. Voor bestuurders en toezichthouders roept dit belangrijke vragen op: hoe blijft een organisatie beschikken over de juiste kennis en competenties, en wat betekent dit voor de strategische ontwikkeling en continuïteit van de organisatie?



Daarnaast brengt digitalisering en AI nieuwe ethische vraagstukken met zich mee. Denk aan inzage in het algoritme (transparantie), bias en discriminatie van AI toepassingen, de impact van geautomatiseerde besluitvorming en de verantwoordelijkheid van organisaties om technologie zorgvuldig en verantwoord toe te passen.

Tegelijkertijd komt er steeds meer Europese wet- en regelgeving rondom digitalisering en AI. Met de invoering van de Cyberbeveiligingswet (in overeenstemming met NIS2-richtlijn) worden bestuurders nadrukkelijker verantwoordelijk voor de digitale weerbaarheid en cyberveiligheid van hun organisatie. Bestuurders en toezichthouders moeten toezicht houden op cybersecurityrisico's, passende maatregelen laten treffen en voldoende inzicht ontwikkelen in digitale risico's. Ook regelgeving zoals de AI Act stelt nieuwe eisen aan organisaties die AI ontwikkelen of toepassen.

Voor bestuurders en toezichthouders betekent dit dat technologie niet langer uitsluitend een onderwerp voor de ICT-afdeling is. Zij raakt aan de kern van strategie, governance, verantwoordelijkheid en zorgvuldig toezicht. De vraag is dan ook niet óf AI een rol speelt binnen organisaties, maar hoe bestuur en toezicht zich tot deze ontwikkeling verhouden.



WAT LEVERT DEZE SESSIE U OP?

Na afloop van deze masterclass:

- Heeft u inzicht in de strategische betekenis van digitalisering en AI voor organisaties en bestuur.
- Begrijpt u wat Europese regelgeving zoals de AI Act en NIS2 (Cyberbeveiligingswet) betekent voor bestuur en toezicht.
- Kunt u digitale en AI-risico's beter plaatsen binnen governance en risicobeheersing.
- Beschikt u over concrete vragen voor de bestuurskamer over digitalisering en cybersecurity.
- Krijgt u praktische handvatten om toezicht te houden op digitalisering en AI.

De bijeenkomst biedt ruimte voor uitwisseling met andere bestuurders en toezichthouders over vraagstukken die in de praktijk spelen.



Centrale vragen tijdens de sessie

Tijdens de bijeenkomst staan onder meer de volgende vragen centraal:

- Waarom zijn digitalisering en AI voor veel organisaties uitgegroeid tot kritische infrastructuur?
- Welke verantwoordelijkheden dragen bestuurders en toezichthouders bij het gebruik van digitalisering en AI?
- Wat betekent de Cyberbeveiligingswet (NIS2-richtlijn) concreet voor toezicht op digitale risico's en cybersecurity?
- Hoe heeft afhankelijkheid van buitenlandse technologiebedrijven invloed op strategie en continuïteit?
- Hoe helpen governance, ethiek en compliance om verantwoord met digitalisering en AI om te gaan?
- Welke vragen helpen in de bestuurskamer om digitalisering en AI beter te begrijpen en te bespreken?

Aan de hand van praktijkvoorbeelden vertalen we deze thema's naar situaties die bestuurders en toezichthouders in hun eigen praktijk kunnen tegenkomen.



VOOR WIE?

Deze masterclass is bedoeld voor commissarissen, toezichthouders en bestuurders die hun inzicht willen verdiepen in de rol van technologie binnen organisaties.

De bijeenkomst richt zich op professionals die beter willen begrijpen hoe AI en digitale regelgeving de bestuurlijke context veranderen en welke vragen dit oproept in de bestuurskamer.

PRAKTISCHE INFORMATIE

Datum

Woensdag 3 juni en dinsdag 16 juni 2026

Locatie

De Havixhorst
Schiphorsterweg 34-36
7966 AC De Schiphorst

Investering

€1.200,- exclusief btw

Groepsgrootte

Maximaal 12 deelnemers

Meer informatie

Voor vragen of aanvullende informatie kunt u contact opnemen met:
Jeanet Bakker: jeanet@fristoezicht.nl of 06 31 64 13 39



PROGRAMMA 3 JUNI 2026

MODERATOR: LINEKE SNELLER

13.00 - 13.30

Ontvangst en kennismaking

13.30 - 14.30

Digitalisering, AI en cybersecurity in bestuurlijk perspectief
- inzichten uit onder meer het Rapport Wennink

14.30 - 15.15

Governance en verantwoordelijkheid bij digitalisering, AI en cybersecurity
- rol van bestuur en toezicht

15.15 - 15.30

Pauze

15.30 - 16.30

De 7 vragen die je miniaal moet stellen

16.30 - 17.00

Boardroomgesprek en reflectie



PROGRAMMA 16 JUNI 2026

MODERATOR: ERIK RUTKENS

13.00 - 13.30

Ontvangst en kennismaking

13.30 - 14.30

Cybersecurity

14.30 - 15.15

Soevereine cloud / quantum computing

15.15 - 15.30

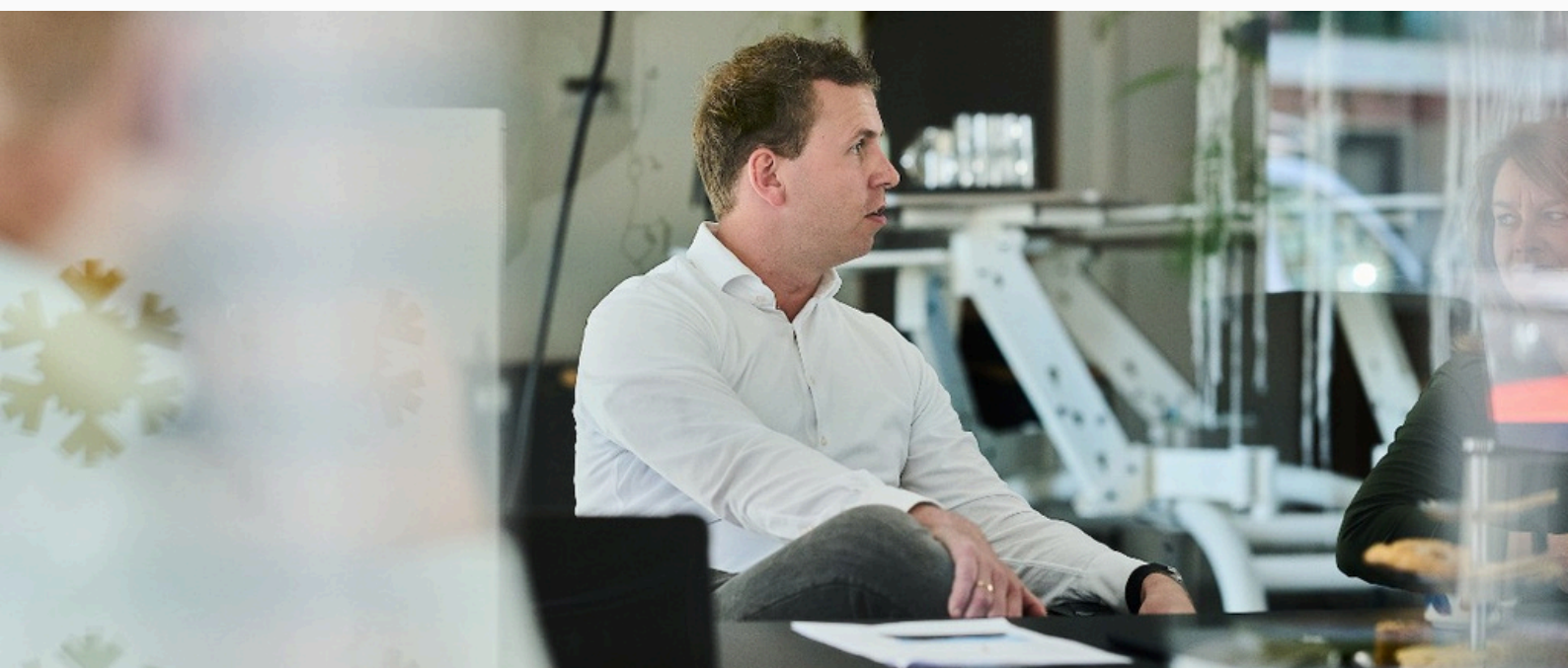
Pauze

15.30 - 16.30

Digitale risico's en Europese regelgeving
- AI Act en Cyberbeveiligingswet (NIS2) in de praktijk

16.30 - 17.00

Boardroomgesprek en reflectie



MODERATOREN

ERIK RUTKENS

LINEKE SNELLER



Erik Rutkens is deeltijd practoor digitaal veilige hard- en software aan Noorderpoort. Daarnaast is hij directeur-eigenaar van Dayzero, een netwerkorganisatie die schaalbare cybersecurity-ideeën ondersteunt met advies, netwerk, diensten, faciliteiten of zelfs met kapitaal. Ook richtte Erik Qbit Cyber Security op, waar hij meer dan 10 jaar directeur was. Verder is Erik één van de initiatiefnemers voor publiek-private samenwerkingen voor het vergroten van de cybersecurity van het MKB in Noord-Nederland.

Met meer dan 20 jaar ervaring in cybersecurity weet Erik als geen ander welke nieuwe bedreigingen zich voordoen en wat organisaties kunnen doen om hun digitale weerbaarheid te vergroten. Hij spreekt en schrijft regelmatig over nieuwe ontwikkelingen op het gebied van cybersecurity. Erik studeerde bedrijfskunde aan de Rijksuniversiteit Groningen.

Prof. dr. Lineke Sneller is hoogleraar Digitalisering & AI in Accounting, Control, Governance en Auditing aan de Rijksuniversiteit Groningen. In haar werk verbindt zij technologie, bestuur en toezicht.

Naast haar academische rol is zij actief als toezichthouder bij verschillende organisaties. Eerder werkte zij jarenlang in internationale technologie- en telecombedrijven, onder meer als CIO.

Door haar brede ervaring in zowel praktijk als wetenschap kijkt Lineke scherp naar de invloed van digitalisering en AI op organisaties, bestuur en toezicht. Daarbij gaat het haar niet alleen om technologie, maar vooral om de vragen die bestuurders en toezichthouders zich daarbij moeten stellen.