NOREA
DE BEROEPSORGANISATIE VAN IT-AUDITORS

Voorzitters politieke partijen Nederland en media

Verzonden via email.

Datum : 18 september 2025
Kenmerk : NOREA/AB-2025/1
Betreft : Aanbevelingen voor verkiezingsprogramma's 2025

Geachte leden van de verkiezingsprogrammacommissies,

De Nederlandse samenleving is in toenemende mate afhankelijk van digitale systemen. Onze economie, publieke dienstverlening en persoonlijke levens zijn verweven met IT. NOREA, de beroepsorganisatie van IT-auditors, ziet dagelijks hoe belangrijk digitale veiligheid en betrouwbaarheid zijn voor overheid, bedrijfsleven én burgers. In aanloop naar de Tweede Kamerverkiezingen van 29 oktober 2025 willen wij u daarom vier concrete voorstellen meegeven om de digitale weerbaarheid van Nederland te versterken. In deze voorstellen geven wij vorm aan de collectieve verantwoordelijkheid die we als maatschappij hebben voor digitale weerbaarheid, door:

1- de juiste aandacht binnen bedrijven en overheidsorganisaties voor de inrichting van hun digitale weerbaarheid,
2- hierover op doelmatige wijze verantwoording af te leggen,
3- meer samenwerken in het voorkomen en bestrijden van cyberincidenten,
4- het vakmanschap op IT-gebied verder te vergroten.

Deze voorstellen sluiten aan bij de huidige bredere maatschappelijke en geopolitieke uitdagingen en vereisen gezamenlijke actie van overheid en maatschappij. Zoals u zult lezen sluiten ze ook aan bij de door de overheid opgestelde Nederlandse Digitaliseringsstrategie (NDS). Door nú te investeren, met name in de invoering van de International Digital Reporting Standards (IDRS), legt Nederland de basis voor efficiënte digitale verantwoordingsstructuren. Dit is cruciaal om onze koppositie als digitaal land te behouden. We lopen voorop met digitale dienstverlening; laten we er ook voor zorgen dat we vooroplopen in slimme verantwoording hierover. Digitale samenwerking is hierbij noodzaak. Toezichthouders en regelgevers kunnen dit faciliteren en afdwingen waar nodig. Door open met elkaar te leren en te oefenen, vergroten we de weerbaarheid van de hele keten en beperken we maatschappelijke schade bij cyberincidenten. Nederland

POSTADRES
Postbus 242
2130 AE Hoofddorp

BEZOEKADRES
Frame Offices-Pharos
Mercuriusplein 3 - 1e verdieping
2132 HA Hoofddorp

E-MAIL EN WEBSITE
norea@norea.nl
www.norea.nl

OVERIG
KVK-NR:40537540
IBAN: NL02ABNA0475165403

kan hierin vooroplopen door een cultuur te stimuleren waarin veiligheid geen concurrentiegebied is maar een gedeeld belang.

Wij vragen u nadrukkelijk om de volgende 4 onderwerpen te adresseren in uw verkiezingsprogramma deze punten een plek te geven voor een veilig, innovatief en toekomstbestendig digitaal Nederland. Het gaat om de volgende 4 onderwerpen:

Vier adviezen om de digitale weerbaarheid te vergroten:

- Positioneer digitale weerbaarheid als een zaak voor iedereen in de organisatie. (Cyber) Security is geen afdeling, maar is van iedereen, van bestuurders tot operationeel medewerkers.
- Leg externe verantwoording af over de IT-beheersing binnen een organisatie en geef daarmee een impuls aan deze verantwoordelijkheid.
- Breng de digitale samenwerking binnen ketens en sectoren naar een hoger niveau. Deze samenwerking gaat over kennisuitwisseling, gezamenlijk testen, een collectief zicht op dreigingen, uitwisseling van waarschuwingen en leren van elkaars aanpak. Dit is organisatie-overstijgend en juist daarom kunnen toezichthouders en regelgevers hier het initiatief nemen.
- Breng het vakmanschap van IT-professionals omhoog. Geef het thema beheersing van IT al een plek op de basisschool en zet in op normering van opleiding, kennis en ervaring van IT-professionals. NOREA kan hierbij als een voorbeeld worden gesteld.

Hiernavolgend zijn deze onderwerpen nader uitgewerkt

Met vriendelijke groet,

Marc Welters
Voorzitter NOREA

Jacques van den Broek
Voorzitter Raad van Advies NOREA
(voormalig CEO Randstad Holding)

Voor meer informatie kunt u contact opnemen met Marc Welters (voorzitter +31621252223) of Jacco Jacobs (vice-voozitter +31631028370).

Positioneer digitale weerbaarheid als verantwoordelijkheid van de hele maatschappij

Digitale veiligheid is niet langer een zaak van alleen de IT-afdeling – het is een uitdaging voor de hele samenleving. Dit betekent dat iedereen een rol heeft: van bestuurders die het onderwerp tot prioriteit maken tot burgers die zich bewust zijn van online risico's. Cybersecurity is een **collectieve verantwoordelijkheid**. Bestuurders in zowel de publieke als private sector moeten digitale weerbaarheid behandelen als "*chef-sache*" – een topprioriteit die zij actief uitdragen. De Cyber Security Raad benadrukt in zijn recente handreiking voor bestuurders en bedrijfseigenaren dat de eindverantwoordelijkheid voor cyberrisico's niet kan worden weggedelegeerd naar IT-specialisten; het voltallige bestuur blijft verantwoordelijk en potentieel aansprakelijk voor digitale veiligheid. Met andere woorden: cyberveiligheid is geen IT-trucje, maar een bestuurs- en maatschappelijke plicht.

Deze brede benadering houdt in dat overheid, bedrijfsleven en burgers gezamenlijk optreden tegen digitale dreigingen. De Nationale Coördinator Terrorismebestrijding en Veiligheid (NCTV) riep onlangs op tot een "Whole of Society""-aanpak: nationale veiligheid is persoonlijke en organisatorische veiligheid en iedereen moet een rol opnemen in het beschermen van onze digitale samenleving. Concrete invulling hiervan begint bij bewustwording op elk niveau. Campagnes voor digitale hygiëne, duidelijke richtlijnen en toegankelijke hulpmiddelen kunnen burgers en MKB helpen om basismaatregelen te treffen. Tegelijk moeten sectorleiders en politici het goede voorbeeld geven en laten zien dat digitale weerbaarheid net zo essentieel is als fysieke veiligheid.

Door digitale veiligheid als een maatschappelijke verantwoordelijkheid te positioneren, doorbreken we het idee dat "IT het wel oplost". Pas als iedere schakel meedoet, creëren we een echt weerbare keten en een cyberveilig Nederland. Dit vergt bestuurlijk eigenaarschap van de overheid, investeringen in mensen (bewustzijn en training) en nauwe samenwerking over sectoren heen. *Ons voorstel is om binnen het kabinet één minister aan te stellen die beleidsmatig kan optreden en regie en coördinatie voert over deze digitale veiligheid*. Alleen zo doen we recht aan de grote maatschappelijke uitdaging van digitalisering en houden we het vertrouwen van burgers in een veilig digitaal Nederland hoog.

NOREA
DE BEROEPSORGANISATIE VAN IT-AUDITORS

Introduceer één standaard digitale verantwoordingsrapportage om regeldruk te verlagen en veiligheid te verhogen

Maak verantwoording over IT en cybersecurity eenvoudiger én effectiever met een cyberjaarverslag volgens de International Digital Reporting Standards (IDRS). Grote organisaties moeten nu voor tientallen eisen en toezichthouders apart rapporteren over digitale veiligheid – een administratieve nachtmerrie die tot hoge lasten en versnipperde inzichten leidt. *Door één geïntegreerd **cyberjaarverslag** in te voeren, kunnen we deze dubbelingen schrappen en tegelijkertijd bestuurders meer inzicht geven in de stand van digitale veiligheid.* De businesscase is duidelijk: één standaard verslag vervangt vele losse audits en checks, waardoor dubbel werk verdwijnt en auditkosten dalen. Zo'n **IDRS-cyberjaarverslag** maakt digitale veiligheid bovendien een vast onderdeel van de managementcyclus, wat een continue verbetercultuur stimuleert. De door de overheid uitgebrachte Nederlandse Digitaliseringsstrategie (NDS) onderstreept het belang van publiek-private samenwerking, standaarden en gezamenlijke bouwstenen in de digitale overheid, wat nauw aansluit bij het advies om verantwoording over IT-beheersing te standaardiseren en digitalisering ketenvast te organiseren

De Tweede Kamer heeft het belang hiervan onderstreept in de motie Kathmann **(3 juni 2025)**. Daarin wordt geconstateerd dat financiële en maatschappelijke jaarverslagen gangbaar zijn, maar vergelijkbaar inzicht in cyberveiligheid ontbreekt. De Kamer verzocht de regering om, samen met overheid en bedrijfsleven, te verkennen hoe een cyberjaarverslag op basis van IDRS als brede standaard kan worden ingevoerd, op een manier die **lastenverlichting én verbeterde veiligheid** oplevert. Het IDRS-concept – vergelijkbaar met een financieel jaarverslag, maar dan voor IT-beheersing – is door NOREA uitgewerkt en in praktijk getoetst bij o.a. een zorgverzekeraar en beursgenoteerd fonds. De eerste resultaten laten zien dat zo'n standaard haalbaar is en werkt.

Voordelen van een IDRS-cyberjaarverslag in één oogopslag:

- **Lagere regeldruk:** Eén rapportage vervangt vele afzonderlijke IT-rapportages, waardoor overlap verdwijnt en administratieve lasten sterk verminderen.
- **Meer grip op veiligheid:** Bestuurders moeten het cyberjaarverslag goedkeuren, waardoor digitale risico's structureel op de bestuurstafel komen en continu verbeterd worden. En dit cyberjaarverslag kijkt niet alleen naar het verleden, maar juist ook naar de getroffen maatregelen om nu en in de toekomst weerbaar te zijn en blijven.
- **Toekomstbestendigheid:** Organisaties bereiden zich proactief voor op nieuwe wetgeving – zoals de EU-richtlijnen **NIS2** (cybersecurity) en **DORA**

(operationele veerkracht financiële sector) – zonder telkens nieuwe verantwoordingslijnen op te tuigen.
- **Transparantie en vertrouwen:** Een gestandaardiseerd publiek verslag vergroot het vertrouwen bij burgers, klanten en ketenpartners, en maakt het mogelijk prestaties op het gebied van digitale veiligheid te vergelijken.

Door nú te investeren in de invoering van IDRS legt Nederland de basis voor efficiënte digitale verantwoordingsstructuren. Dit is cruciaal om onze koppositie als digitaal land te behouden. We lopen voorop met digitale dienstverlening; laten we er ook voor zorgen dat we voorop open in **slimme verantwoording** hierover. Zo voorkomen we dat groeiende eisen uit o.a. NIS2 en DORA onze organisaties verlammen met rapportagedruk. Integendeel – met IDRS versterken we tegelijkertijd de veiligheid én verminderen we onnodige bureaucratie. Die win-win past bij een innovatief Nederland dat digitalisering omarmt.

Versterk digitale samenwerking in ketens en sectoren

Cyberdreigingen stoppen niet bij de grenzen van één organisatie – daarom moeten organisaties binnen ketens en sectoren veel hechter samenwerken. Een keten is immers zo sterk als de zwakste schakel. Banken, ziekenhuizen, energieleveranciers, toeleveranciers – ze zijn digitaal met elkaar verbonden en afhankelijk. Alleen door **collectieve actie** kunnen zij een krachtige vuist maken tegen cyberaanvallen. Dit vraagt om het voortbouwen op bestaande initiatieven en deze op te schalen.

In de praktijk betekent dit verplichte kennisuitwisseling, gezamenlijke oefeningen en gecoördineerde respons. Nu gebeurt dit vaak nog op vrijwillige basis, maar die vrijblijvendheid moet eruit. **Proactieve ketensamenwerking** zou de norm moeten zijn, geen hobby van enkel voorhoedespelers. Goede voorbeelden zijn er al: in de financiële sector worden onder regie van De Nederlandsche Bank TIBER-tests uitgevoerd, waarbij in een gesimuleerde hack de gehele keten – inclusief leveranciers – wordt doorgelicht. Deze aanpak, een soort "ecosysteem-audit", toont aan dat samenwerking loont: organisaties leren niet alleen of hun eigen verdediging op orde is, maar ook waar zwakke plekken bij partners zitten die hun veiligheid beïnvloeden. Ook het Nationaal Cyber Security Centrum (NCSC) heeft de afgelopen jaren sectorale informatieknooppunten en vertrouwelijke samenwerkingsverbanden (zoals ISACs) uitgebreid, zodat honderden partijen actuele dreigingsinformatie kunnen delen. Toch is er **nog een wereld te winnen** – zeker ook buiten de vitale sectoren door (a) informatie-uitwisseling (b) samen oefenen in crisissen (c) cyberweerbaarheidstesten. Publiek-private initiatieven als de Cybersecurity Alliantie van ECP en het nieuwe Cyber Chain Resilience Consortium (CCRC) laten zien hoe het kan: bedrijven, overheden en hun leveranciers werken crosssectoraal samen om

zich te wapenen tegen supply-chain aanvallen. Dergelijke samenwerkingen moeten niet incidenteel zijn, maar structureel. De NCTV heeft in 2024 terecht opgeroepen tot meer civiele weerbaarheid, waarbij publieke en private organisaties gezamenlijk optrekken tegen dreigingen. Dat betekent ook dat toezichthouders en overheid waar nodig een handje helpen om sectoren te organiseren. *Wij pleiten ervoor dat in elke vitale keten – van zorg tot transport – periodieke cyberoefeningen en informatie-uitwisseling verplicht onderdeel worden van de crisisvoorbereiding. En dat hierover een centrale regie wordt gevoerd die vanuit één ministerie wordt geborgd.* En waar de *lessons learned* over incidenten worden verzameld en gedeeld (vergelijk de open meldcultuur in de luchtvaart) om herhaling te voorkomen.

Kortom, digitale samenwerking is noodzaak. Toezichthouders en regelgevers kunnen dit faciliteren en afdwingen waar nodig. Door open met elkaar te leren en te oefenen, vergroten we de weerbaarheid van de hele keten en beperken we maatschappelijke schade bij cyberincidenten. Nederland kan hierin vooroplopen door een cultuur te stimuleren waarin veiligheid geen concurrentiegebied is maar een gedeeld belang.

Verhoog het vakmanschap in IT en versterk de Nederlandse techsector

Digitale weerbaarheid begint en eindigt bij mensen. Zonder voldoende deskundige IT-professionals en cybersecurity-experts komen al onze ambities in gevaar. Helaas kampt Nederland – net als de rest van de wereld – met een groeiend tekort aan digitale vakmensen. De vraag naar cybersecurityspecialisten zal de komende jaren alleen maar toenemen, onder andere door nieuwe Europese regels die extra expertise vereisen. Onderzoek van het kabinet bevestigt dat er aanzienlijke tekorten zijn en dat de instroom van talent achterblijft. We moeten daarom vol inzetten op het vergroten van het **IT-vakmanschap** en het stimuleren van onze eigen techsector, zodat Nederland niet afhankelijk wordt van schaarse kennis uit het buitenland.

Ten eerste is **onderwijs** de sleutel. *Digitale basisvaardigheden én cybersecurity moeten een vaste plek krijgen in de curricula, van basisschool tot en met universiteit.* Kinderen maken steeds vroeger gebruik van digitale middelen; zij moeten leren hoe ze dit veilig doen en interesse ontwikkelen in techniek. We pleiten voor **structurele aandacht voor digitale weerbaarheid in het onderwijs**: denk aan programmeerlessen, cyberhygiëne, maar ook aantrekkelijk beroepsonderwijs dat jongeren enthousiast maakt voor IT. Daarnaast moeten we omscholing en bijscholing faciliteren. De technologische ontwikkelingen gaan razendsnel, dus ook de huidige beroepsbevolking moet zich continu kunnen ontwikkelen. Het goede nieuws is dat de overheid dit begint in te zien: er is bijvoorbeeld een **Human Capital Agenda ICT** opgezet met een programmalijn cybersecurity om de samenwerking

tussen onderwijs en bedrijfsleven te verbeteren en meer IT'ers op te leiden. Zulke initiatieven verdienen uitbreiding en lange termijn commitment. Een van de zes prioriteiten in de Nederlandse Digitaliseringsstrategie is 'Digitaal vakmanschap en een moderne werkomgeving', waarmee het kabinet erkent dat investeren in mensen en vaardigheden cruciaal is voor de weerbaarheid én concurrentiekracht van Nederland.

Ten tweede moeten we de **Nederlandse techsector** als geheel versterken. Een sterke eigen techindustrie, van cybersecurity startups tot AI-ontwikkelaars, draagt niet alleen bij aan economische groei en strategische autonomie, maar ook direct aan onze digitale weerbaarheid. Innovatie en veiligheid gaan hand in hand: nieuwe oplossingen op het gebied van bijvoorbeeld kunstmatige intelligentie, cloud en quantum bieden kansen, maar stellen ook eisen aan veiligheid. Nederland heeft de kans om zich te profileren als Europees koploper in digitale innovatie en vakmanschap. De overheid kan dit beter faciliteren dan ze nu doet. Want we staan nu al hoog in ranglijsten als de DESI-index en gelden als een van de meest gedigitaliseerde landen. Die voorsprong moeten we benutten door tegelijkertijd voorop te lopen in cybersecurity-expertise. *Dat betekent onder meer: concrete initiatieven voor intensieve publiek-private samenwerking in onderzoek en ontwikkeling, doorvoeren van een pakket aantrekkelijke vestigingsvoorwaarden voor techbedrijven, en het wegnemen van knelpunten (bijv. door meer investeringen in techno-startups en het moderniseren van ICT-onderwijs)*.

Investeren in digitaal vakmanschap levert dubbel rendement op: we krijgen beter beveiligde organisaties én een bloeiende digitale economie. Elke euro die we nu steken in IT-kennis en skills, betaalt zich snel en meervoudig terug in de vorm van innovatiekracht, nieuwe banen en minder schade door cybercrime. Laten we van Nederland niet alleen een proeftuin voor nieuwe technologie maken, maar ook een bolwerk van digitaal vakmanschap. Zo verhogen we onze weerbaarheid en versterken we tegelijk onze positie als toonaangevende tech-natie in Europa.

Met bovenstaande vier punten vragen wij aandacht voor een weerbaar digitaal Nederland. Door digitale veiligheid als een gedeeld maatschappelijk belang te zien, slim om te gaan met verantwoording, intensief samen te werken in ketens en te investeren in mensen en kennis, kunnen we de uitdagingen van de digitale toekomst aan. In dit geopolitieke klimaat zijn deze onderwerpen evident om politiek te adresseren en richting te geven in partijprogramma's.