● Whitepaper

Naar digitale weerbaarheid en compliance: Een holistische benadering voor Europese regelgeving

Themagewijs compliant – gestroomlijnd via een Integrated Control Framework.

eraneos

Inhoudsopgave

Andrea Krush
Senior Manager – Cybersecurity
Eraneos
andrea.krush@eraneos.com

Marco van Leijenhorst
Senior Consultant – Cybersecurity
Eraneos
marco.van.leijenhorst@eraneos.com

Nabeel Siddiqie
Cybersecurity Partner
Eraneos
nabeel.siddiqie@eraneos.com

Management-samenvatting

Dit whitepaper biedt een holistische benadering voor het versterken van digitale weerbaarheid en compliance binnen Europese regelgeving. De Europese Unie streeft naar een digitale samenleving die mensgericht en duurzaam is, ondersteund door robuuste digitale wetgeving zoals de NIS2-richtlijn, DORA, de AI-verordening en de Cyber Resilience-verordening.

In plaats van afzonderlijke projecten voor elke nieuwe wet, stellen we een geïntegreerde aanpak voor door thema's te identificeren die in verschillende wetten terugkomen en deze gezamenlijk aan te pakken. Een Integrated Control Framework (ICF) en een thematisch stappenplan helpen om compliance te stroomlijnen en eigenaarschap, goede besturing en het stellen van de juiste prioriteiten te bevorderen.

Compliance is essentieel voor de digitale weerbaarheid van een organisatie. Het gaat verder dan het vermijden van boetes; het vormt de basis voor een veilige en betrouwbare digitale omgeving. Door te voldoen aan eisen rondom gegevensbescherming, cybersecurity en incidentmanagement, bouwt een organisatie een sterker digitaal fundament.

Ondanks het belang van compliance, worstelen veel organisaties met de implementatie ervan. In deze whitepaper bespreken we de uitdagingen zoals gebrek aan overzicht, inefficiënties in compliance-processen, onduidelijk eigenaarschap en lage prioriteit. Het biedt oplossingen zoals standaardisatie door middel van een gestructureerd three lines-model, gecentraliseerde compliance-processen en een geïntegreerde aanpak.

Een gestructureerde aanpak met een ICF biedt een strategisch plan om de geïdentificeerde hiaten aan te pakken en naleving te bereiken. Door eigenaarschap in de eerste lijn te versterken en prioriteiten te bepalen, kunnen organisaties de transitie maken van geïsoleerde proof-of-concepts naar een volwaardige, organisatiebrede compliance-implementatie.

Het groeiende belang van digitale weerbaarheid onder EU-regelgeving

De Europese Unie heeft een ambitieuze visie voor een digitale samenleving die mensgericht en duurzaam is, waarbij burgers en bedrijven worden versterkt met robuuste digitale regelgeving.

De digitale wereld verandert razendsnel en de Europese wetgeving doet haar best om bij te blijven middels het 'Europe Fit for a Digital Age'-pakket aan wetgeving. Voor organisaties betekent dit een flink aantal nieuwe regels zoals de NIS2-richtlijn, DORA, de AI-verordening en de Cyber Resilience-verordening. En we hebben ook nog de AVG en de ePrivacy-richtlijn. Hoe blijf je als organisatie compliant zonder dat het een enorme belasting wordt?

Dit whitepaper biedt een praktische benadering. In plaats van voor elke nieuwe wet een apart project op te zetten, stellen we een slimmere aanpak voor: kijk naar thema's die in verschillende wetten terugkomen en pak die geïntegreerd aan.

We laten zien hoe een Integrated Control Framework (ICF) en een doordacht thematisch stappenplan helpen om compliance te stroomlijnen. Daarnaast belichten we het belang van eigenaarschap, goede besturing en het stellen van de juiste prioriteiten.

Waarom compliance belangrijk is voor de digitale weerbaarheid van een organisatie

Compliance met digitale wet- en regelgeving is fundamenteel voor de digitale weerbaarheid van een organisatie. Het gaat verder dan het vermijden van boetes; het vormt de basis voor een veilige en betrouwbare digitale omgeving. Door te voldoen aan eisen rondom gegevensbescherming, cybersecurity en incidentmanagement, bouwt een organisatie een sterker digitaal fundament. Dit resulteert in beter beschermde bedrijfsprocessen, een hogere mate van data-integriteit en een verhoogd vermogen om cyberdreigingen en operationele verstoringen te voorkomen en te mitigeren. Compliance is daarmee niet slechts een verplichting, maar biedt ook toegevoegde waarde voor de organisatie door de kwaliteit, integriteit en beveiliging van haar data te waarborgen.

Uitdagingen bij het voldoen aan digitale regelgeving

Ondanks het belang van compliance worstelen veel organisaties met de implementatie ervan. Verschillende uitdagingen zitten de implementatie bij menige organisatie in de weg.

Gebrek aan overzicht

Veel organisaties missen een gecentraliseerde compliance-structuur, wat leidt tot inconsistent beleid en versnipperde implementatie. Dit probleem wordt verergerd door de complexiteit van meerdere, overlappende regelgevingen.

In plaats van de traditionele aanpak waarbij voor elke regelgeving afzonderlijk wordt gekeken naar compliance, is het effectiever om te kijken naar de overkoepelende thema's die in verschillende wetgevingen terugkomen. Een Integrated Control Framework (ICF) kan helpen bij een gestructureerde aanpak bij het in kaart brengen van de eisen om aan de regelgeving te voldoen. In het volgende stuk gaan we hier dieper op in.

Inefficiënties in compliance-processen

Dubbele processen, overlap tussen adviserende functies en versnippering in de organisatie kosten organisaties onnodig veel tijd en geld, met wisselvallige resultaten als gevolg.

In plaats van aparte processen op te tuigen voor elke nieuwe regelgeving - denk aan gescheiden incidentmanagementprocessen voor de AVG en DORA - kunnen organisaties efficiënter werken door slim te consolideren.

Organisaties kunnen de efficiëntie op dit vlak op de volgende manieren verbeteren.

- Standaardisatie door middel van een gestructureerd three lines-model
- Gecentraliseerde compliance-processen om efficiëntie en schaalbaarheid te waarborgen
- Geïntegreerde aanpak die domeinoverstijgend werkt

Onduidelijk eigenaarschap

Veel bedrijfsonderdelen missen de kennis of capaciteit voor eigenaarschap in de 'eerste lijn'. Dit leidt tot een te grote afhankelijkheid van tweede-lijn-adviseurs en gebrekkige implementatie. Als het eigenaarschap niet duidelijk is vastgelegd, weet niemand wie verantwoordelijk is voor de oplevering voor een document of als een bepaald proces niet werkt.

Lage prioriteit

De verantwoordelijken stellen vaak niet de juiste prioriteiten bij digitale weerbaarheid, wat resulteert in onvoldoende investeringen en verspilde middelen. Met name commerciële organisaties geven vaak pas prioriteit aan compliance als er boetes aan vasthangen, terwijl een meer overkoepelende blik op thema's effectiever zou zijn.

Compliance structureren met het Integrated Control Framework

Vanuit een thematische aanpak biedt een Integrated Control Framework (ICF) een gestructureerde aanpak voor het in kaart brengen van regelgevingsvereisten door:

- Beleid en beoordeling van risico's uniform af te stemmen
- GRC-tools (Governance, Risk & Compliance) te benutten om het bijhouden en rapporteren van compliance-voortgang te automatiseren
- Overlap tussen regelgeving te verminderen

Een ICF is een universeel middel dat alle organisaties kunnen inzetten, maar de invulling moet wel organisatie-specifiek zijn. Wanneer je een control-framework opstelt, zet je wettelijke vereisten om in controls die aangeven hoe je in de organisatie kunt voldoen aan de vereisten. Als je dat goed doet, doe je het zo specifiek dat het echt is toegespitst op de eigen organisatie: wie, wat, waar, wanneer, hoe, waarom.

Als je bijvoorbeeld ‚wie' niet vastlegt, heb je geen eigenaarschap. De verschillende wetgevingen zijn qua eisen vaak niet zo specifiek. Er staat bijvoorbeeld dat ‚vulnerability management' noodzakelijk is, maar niet wie er verantwoordelijk is of hoe het proces moet verlopen, of op welke systemen. Als je alleen vulnerability management afvinkt omdat je organisatie een vulnerability management tool heeft, is het de vraag of je aantoonbaar compliant bent.

Eigenaarschap bereiken door de eerste lijn te versterken

Effectieve compliance vereist een samenhang tussen governance, risicobeheer en interne controle. Het Three Lines Model biedt hierbij een structuur waarin operationeel management, risicofuncties en interne audit samenwerken om risico's te beheersen en naleving te waarborgen. Dit gaat verder dan regelgeving en vraagt om een cultuur van ethiek en verantwoordelijkheid. Bij veel organisaties ontbreekt het organisatieonderdelen aan kennis of capaciteit voor eigenaarschap in de eerste lijn. Dit leidt tot een gebrekkige implementatie en een te grote afhankelijkheid van tweedelijns adviseurs die optreden als poortwachters

Eigenaarschap begint met aan de voorkant benoemen welke manager erover gaat. Wie krijgt een probleem op het moment dat het niet goed gaat? Dit moet zo dicht tegen de operatie aan zitten dat je deze persoon ook kunt benoemen. "Namen en rugnummers" zorgen ervoor dat je als organisatie weet waar het fout gaat, maar belangrijker, dat je als organisatie de verantwoordelijken kan ondersteunen op een gepaste manier om het juist goed te laten gaan.

Eigenaarschap is op de volgende manieren te bereiken:

- Coaching en gestructureerde training van de 1e lijn via de „I do – We do – You do"-aanpak, waarbij uiteindelijk de verantwoordelijken in de organisatie zelf maatregelen initiëren en implementeren
- Het sturen en structuren van de 2e lijn als verkeersmonitor in plaats van gatekeeper
- Het inbedden van compliance binnen operationele IT-administratie en governance-structuren

Risk management cultuur: De rol van risk en compliance moet veranderen

Prioriteiten bepalen

Verantwoordelijken stellen vaak niet de juiste prioriteiten bij digitale weerbaarheid, wat resulteert in:

- Onvoldoende investeringen in noodzakelijke beveiligingsmaatregelen
- Implementatie-inspanningen zonder gerichte prioriteiten, wat resulteert in verspilde middelen
- Geïsoleerde projecten die blijven steken in de proof of concept-fase

We zien vaak dat organisaties pas prioriteit geven aan compliance als er boetes aan vasthangen. Het is effectiever om te kijken naar overkoepelende thema's en fijnmaziger te bepalen waar de risico's liggen. Thema's zoals waar en hoe je afhankelijk bent van derde partijen. Als je bijvoorbeeld alles in de cloud hebt en in één regio, kun je veel last hebben van uitval van het energienetwerk in die regio.

Een kritiek aspect van effectieve compliance is het inbedden van digitale weerbaarheid binnen bedrijfsactiviteiten, in plaats van het te behandelen als een geïsoleerde functie. Daarbij is compliance een gedeelde verantwoordelijkheid in de hele organisatie. De organisatie vermijdt bovendien een silomentaliteit, waarbij security en compliance gescheiden zijn van de business.

Zo stem je de verwachtingen af op de uitvoering:

01.

Implementeer een duidelijke roadmap en backlog-aanpak om compliance-stappen efficiënt op elkaar te laten volgen;

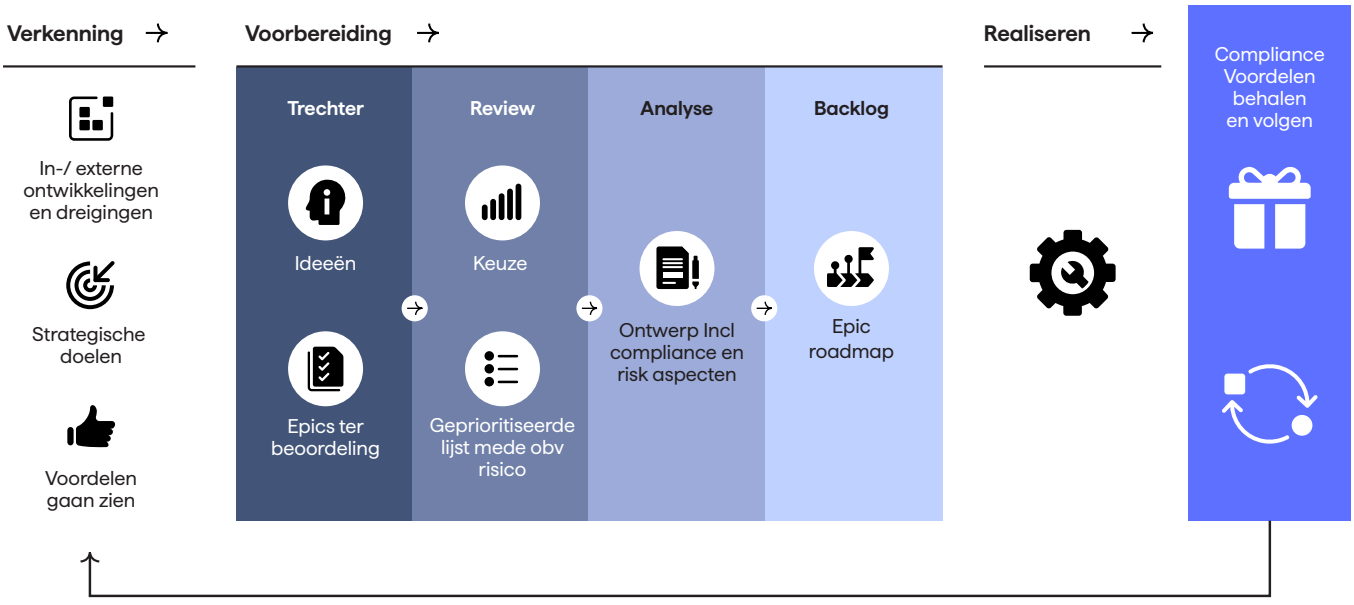
02.

Maak een risico-gebaseerde prioritering om verwachtingen van het management af te stemmen op cybersecurity-investeringen; en

03.

Toon de waarde van compliance-investeringen aan door de impact op de hele waardeketen te benadrukken.

De werkelijke waarde van digitale weerbaarheid zit in oplossingen die de gehele organisatie ten goede komen, niet alleen afzonderlijke afdelingen. Door deze uitdagingen systematisch aan te pakken, kunnen organisaties compliance én weerbaarheid bereiken.



Met een praktische aanpak naar weerbaarheid én compliance

Om de complexiteit van EU-regelgeving effectief aan te pakken, is een gestructureerd compliance-implementatiemodel nodig. Dit model, gebaseerd op bewezen benaderingen voor de NIS2 richtlijn, DORA, de AVG en andere regelgevingen, biedt een praktisch kader voor het bereiken van compliance.

In de praktijk is het vaak niet zo dat je elk onderdeel van een wet moet afvinken. Met een gestructureerde aanpak kun je veel risicogestuurder naar de wetgeving kijken.

Je begint vanuit je eigen basissystematiek. De meeste organisaties hebben een basisraamwerk dat ze kunnen uitbreiden om vervolgens risicogebaseerd aan het werk te gaan. Als je als organisatie ziet dat er bijvoorbeeld risico's zijn op het gebied van governance, begin je daarmee. Je prioriteert en maakt het klein. Daarna werk je aan continue verbetering en laat het groeien. Dat is de beste manier om gestructureerd naar compliance te werken.

Stap 1: Scope

De eerste stap is het afbakenen van de reikwijdte van de compliance-inspanningen:

- Het identificeren van relevante wettelijke vereisten voor de organisatie
- Het bepalen van het risicobeeld van de organisatie met betrekking tot deze vereisten

Stap 2: Startpunt

De tweede stap richt zich op de huidige status van de organisatie:

- Het evalueren van de huidige capaciteiten van de organisatie om aan de vereisten te voldoen en het identificeren van de restrisico's
- Het ontwikkelen van het gewenste resultaat (SOLL) als referentiepunt voor compliance

Stap 3: Gap assessment

De derde stap is het analyseren van de verschillen:

- Het identificeren van de hiaten tussen de huidige mogelijkheden en de vereiste normen

Stap 4: Roadmap

Op basis van de gap-analyse wordt een strategisch plan ontwikkeld:

- Het ontwikkelen van een strategisch plan om de geïdentificeerde hiaten aan te pakken en naleving te bereiken
- Het prioriteren van maatregelen op basis van risicoanalyse en het definiëren van verantwoordelijkheden

Stap 5: Implementatie

De vijfde stap omvat de uitvoering van het plan:

- Het uitvoeren van de roadmap en het implementeren van de wijzigingen om naleving te garanderen
- Het volgen van de implementatie en het continu verbeteren van de getroffen maatregelen

Stap 6: Integrated Control Framework

De laatste fase richt zich op het borgen van compliance door middel van een Integrated Control Framework:

- Het inrichten van een control framework om de effectiviteit van de geïmplementeerde maatregelen te toetsen
- Het monitoren van de naleving van de regelgevingsvereisten binnen het control framework
- Het waarborgen van continue controle en aanpassing waar nodig

De praktische waarde van de gestructureerde aanpak

Als je een gestandaardiseerd proces gebruikt, heb je een toekomstgerichte aanpak. Bij nieuwe wetten of aanpassingen kun je inhaken op bepaalde punten van het stappenplan. Je hoeft niet steeds opnieuw te beginnen, maar je kunt gebruiken wat er al ligt, of het nu bij de IT-afdeling of bij de compliance-afdeling is ondergebracht.

Deze gestructureerde aanpak biedt een aantal voordelen:

- **Efficiëntie:** door overlappende vereisten te identificeren, vermindert het dubbel werk
- **Schaalbaarheid:** het raamwerk kan worden aangepast naarmate nieuwe regelgeving ontstaat
- **Duurzaamheid:** door eigenaarschap in de eerste lijn te bevorderen, wordt compliance een integraal onderdeel van bedrijfsprocessen

Door deze gestructureerde aanpak te volgen, kunnen organisaties de transitie maken van geïsoleerde proof-of-concepts naar volwaardige, organisatiebrede compliance-implementatie.

Andrea Krush
Senior Manager – Cybersecurity
Eraneos
andrea.krush@eraneos.com

Marco van Leijenhorst
Senior Consultant – Cybersecurity
Eraneos
marco.van.leijenhorst@eraneos.com

Nabeel Siddiqie
Cybersecurity Partner
Eraneos
nabeel.siddiqie@eraneos.com

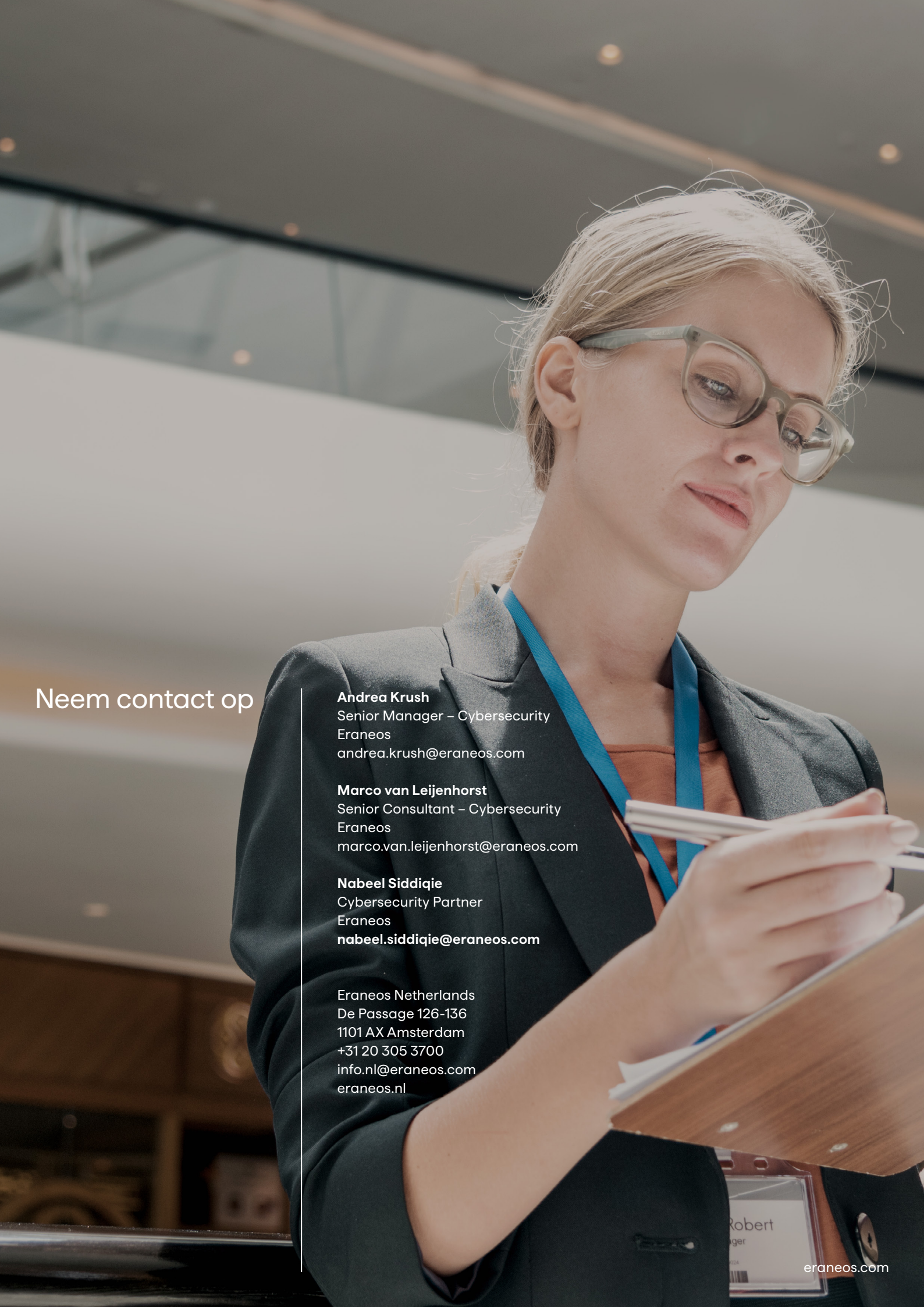
Conclusie

Een gestandaardiseerde compliance-aanpak voorkomt dubbel werk, is schaalbaar en zorgt voor duurzame digitale weerbaarheid. Door compliance structureel te benaderen, wordt het een integraal onderdeel van de organisatie en niet slechts een verplichting. Structuur kan aangebracht worden met het gebruik van een ICF en om de compliance-aanpak efficiënter te maken.

Het menselijke aspect van compliance is niet te onderschatten. Uiteindelijk zijn het de mensen binnen de organisatie die beleid uitvoeren en naleving waarborgen. Dit vraagt niet alleen om duidelijke richtlijnen, maar ook om draagvlak en eigenaarschap, vooral in de eerste lijn. Een helder gedefinieerde rolverdeling en aanspreekbaarheid zijn essentieel: als verantwoordelijkheden niet duidelijk zijn, blijft implementatie steken.

In plaats van enkel beleid op te leggen, is het van belang om de dialoog aan te gaan en te zorgen voor betrokkenheid. Pas dan ontstaat de brug tussen beleid en praktische uitvoering. Governance speelt hierin een sleutelrol: als een schakel hapert, moet duidelijk zijn waar en hoe wordt ingegrepen. Dat inzicht ontbreekt regelmatig, mede omdat mensen van nature terughoudend zijn om op hun verantwoordelijkheden te worden aangesproken. Juist daarom is het belangrijk om compliance stevig in de eerste lijn te verankeren, zodat verantwoordelijkheden helder zijn en naleving geen papieren werkelijkheid blijft.

Heb je hulp nodig bij je digitale compliance? Neem dan gerust contact met ons op.



Neem contact op

Andrea Krush
Senior Manager – Cybersecurity
Eraneos
andrea.krush@eraneos.com

Marco van Leijenhorst
Senior Consultant – Cybersecurity
Eraneos
marco.van.leijenhorst@eraneos.com

Nabeel Siddiqie
Cybersecurity Partner
Eraneos
nabeel.siddiqie@eraneos.com

Eraneos Netherlands
De Passage 126-136
1101 AX Amsterdam
+31 20 305 3700
info.nl@eraneos.com
eraneos.nl