Berenschot

EINDRAPPORT

Onderzoek sturen op informatie-veiligheid

Praktijklessen voor het ministerie van Binnenlandse Zaken en Koninkrijksrelaties bij het sturen op informatieveiligheid

68213 – 17 november 2022

EINDRAPPORT

Onderzoek sturen op informatieveiligheid

Praktijklessen voor het ministerie van Binnenlandse Zaken en Koninkrijksrelaties bij het sturen op informatieveiligheid

Luuk Stadhouders MSc CISM
Rianne Zivali-de Kievit MSc CISA CIPP/e

68213 – 17 november 2022

Inhoudsopgave

HOOFDSTUK 1

Inleiding

1.1 Achtergrond en vraagstelling

In de afgelopen jaren zijn vanuit het ministerie van Binnenlandse Zaken en Koninkrijksrelaties (hierna: BZK) stappen ondernomen om de informatieveiligheid bij overheden te verhogen.[1] In een interbestuurlijke actieagenda informatieveiligheid zijn overheidsbreed maatregelen getroffen, gericht op het op orde brengen en houden van de informatieveiligheid van overheidsorganisaties en het bevorderen van overheidsbrede samenwerking.

In alle bestuurslagen is het bewustzijn over informatieveiligheid en de digitale weerbaarheid de afgelopen jaren toegenomen. Initiatieven zijn genomen om informatieveiligheid een onderdeel uit te laten maken van de reguliere planning- en controlcyclus. Tussen de verschillende bestuursorganen en de bestuurslagen onderling bestaan desondanks nog verschillen in de mate waarin informatieveiligheid een integraal onderdeel uitmaakt van die planning- en controlcyclus.[2]

1.1.1 Centrale coördinatie en decentrale verantwoordelijkheid

BZK heeft de stelselverantwoordelijkheid voor informatie-veiligheid in het openbaar bestuur voor de rijkoverheid, provincies, gemeenten en waterschappen. Stelselverantwoor-delijkheid houdt in dat ieder van de betrokken overheden medeverantwoordelijkheid draagt voor het stelsel als geheel en dat elk van deze overheden daarop kan worden aangesproken. Overheidsorganisaties zijn zelf verantwoordelijk voor de wijze waarop het informatieveiligheidsbeleid in hun organisatie gestalte krijgt. Het ministerie van BZK is hierbij op dit moment kaderstellend, ondersteunend, en waar nodig aanjagend naar alle overheidslagen. Met de medeoverheden streeft BZK vooral naar uniformiteit van de aanpak binnen de overheidslaag zelf en naar optimale afstemming tussen de overheidslagen.

1.1.2 Evaluatie Baseline informatiebeveiliging Overheid (BIO)

Sinds eind 2018 geldt de Baseline informatiebeveiliging Overheid (hierna: BIO), waarin de normen voor informatiebeveiliging zijn vastgelegd waaraan alle overheden zich moeten houden. Mede gedreven door de herziening van de ISO 27001 en ISO 27002 voert BZK momenteel een evaluatie uit op de BIO, waarbij wordt gekeken op welke onderwerpen de BIO verbeterd kan worden,. Een geëvalueerde en geactualiseerde BIO krijgt een belangrijke rol op het gebied van normeren op het gebied van informatieveiligheid bij de vormgeving van de digitale transitie in Nederland. Tevens worden voorbereidingen getroffen om de BIO een wettelijke grondslag te geven in een volgende tranche van de aanstaande Wet Digitale Overheid (hierna: WDO)[3].

1.1.3 Vraagstelling

Het Directoraat-generaal Digitalisering en Overheidsorganisatie van BZK (hierna: BZK/DGDOO) heeft in het kader van de evaluatie van de BIO behoefte aan een onderzoek naar de wijze waarop in verschillende sectoren bij grote (semi-)commerciële organisaties sturing wordt gegeven aan informatieveiligheid, ofwel de wijze waarop dergelijke organisaties grip hebben op informatieveiligheid en ‘in control’ zijn. BZK kan hieruit lessen trekken, door dit bij organisaties buiten de overheid onder de loep te nemen, zodat het zijn stelselverantwoordelijkheid kan verbeteren. Meer specifiek is BZK op zoek naar best practices, inzichten of interventies om daadwerkelijk invulling te (laten) geven aan enerzijds compliance op wet- en regelgeving en anderzijds feitelijke digitale veiligheid bij medeoverheden. Hierbij is zowel aandacht voor de interne organisaties als voor de positie in het stelsel en voor de leveranciers.

1 Kamerstuk 26 643, nr. 749
2 Onderzoek toezicht en verantwoording informatieveiligheid overheid (Verdonck, Klooster & Associates, februari 2019)
3 Kamerstuk 26 643, nr. 749

De hoofdvraag luidt als volgt:

Welke lessen kan BZK trekken in de wijze waarop bij grote organisaties sturing wordt gegeven aan informatieveiligheid?

In de onderzoeksopdracht is onderscheid gemaakt tussen een drietal onderwerpen, waarbij illustratief enkele (deel)vragen zijn opgenomen:

- Governance en inrichting: op welke wijze is de centrale coördinatie van informatiebeveiliging ingericht, mede in relatie tot verantwoording, toezicht en auditing? Op welke wijze wordt 'grip' verkregen op informatieveiligheid?
- Risicomanagement: op welke wijze worden strategische tot en met operationele risico's op het gebied van informatiebeveiliging beheerst, mede in de bredere context van bedrijfsbreed risicomanagement in relatie tot de bedrijfsdoelstellingen?
- Toetsing en verantwoording: welke in- of externe prikkels dragen bij aan daadwerkelijke informatieveiligheid en/of compliance? Hoe worden organisatieonderdelen aan- of, indien nodig, bijgestuurd? Welke prikkels werken, ofwel aan welke variabele knoppen moet er gedraaid worden?

1.2 Doel van dit document

Het doel van dit eindrapport is om een antwoord te geven op de hoofdvraag die u aan Berenschot heeft gesteld. We beschrijven in het rapport nadrukkelijk de 'praktische' interventies of verbeteringen. Ook bieden wij inzicht in de wijze waarop wij tot deze antwoorden zijn gekomen. We plaatsen deze resultaten in de relevante context van de opgave voor BZK om informatieveiligheid binnen de overheid te versterken en beschrijven hierbij de noodzakelijke randvoorwaarden.

1.3 Leeswijzer

Het eindrapport is als volgt opgebouwd: In hoofdstuk 2 lichten wij onze onderzoeksopzet en aanpak toe en beschrijven wij hoe wij tot deze de resultaten zijn gekomen. In hoofdstuk 3 schetsen wij vervolgens de geanonimiseerde casussen die zijn onderzocht en geven onze inzichten in relatie tot het doel van de opdrachtgever. In hoofdstuk 4 beantwoorden we de hoofdvraag en geven wij onze conclusies en aanbevelingen weer, inclusief de 'praktische' interventies of verbeteringen die de sturing op informatieveiligheid binnen de overheid kunnen versterken.

HOOFDSTUK 2

Onderzoeksopzet

2.1 Inleiding

Om tot een volledige en adequate beantwoording van de hoofdvraag en onderliggende onderwerpen te komen, is de volgende onderzoeksopzet gehanteerd.

2.2 Aanpak van het onderzoek

Het onderzoek is gestart in juli 2022 en afgerond in oktober 2022 en werd begeleid door een medewerker van BZK/ DGDOO.

2.2.1 Fases

Het onderzoek bestond uit een drietal fases en bijhorende inspanningen en resultaten, zoals weergegeven in het volgende overzicht:

Fase	Inspanningen	Resultaat
Voorbereiding	Kick-off	Afgestemde onderzoeksopzet
		Afgestemde interviewleidraad
		Afgestemde lijst met te interviewen organisaties
	Voorbereiding onderzoek	Documentstudie
		Ingeplande interviews
Uitvoering	Interviews afnemen	Interviews
	Verdiepend onderzoek	Aanvullende documentatie verzameld en meegenomen in de documentstudie
	Uitwerken rapportage	Conceptrapportage opgesteld
	Werksessie	Inzichten gevalideerd en conceptrapportage afgestemd
	Afstemmen bevindingen	Feitelijke bevindingen per organisatie gevalideerd en afgestemd
Afronding	Afstemmen conceptrapportage	Conceptrapportage afgestemd met opdrachtgever en verbetervoorstellen verwerkt
	Afronding rapportage	Definitieve rapportage opgeleverd
	Toelichting rapportage	Presentatie resultaten

2.2.2 Onderzochte organisaties

Bij de selectie van de organisaties zijn vooraf een aantal selectiecriteria vastgesteld. Berenschot heeft op verzoek van de opdrachtgever bij het vormgeven van deze criteria, alsmede de voorgestelde keuze, een initiërende en adviserende rol gehad. De voorlopig geselecteerde organisaties werden benaderd met het verzoek deel te nemen aan dit onderzoek. Indien organisaties hiertoe bereid waren, is de betreffende organisatie vervolgens voorgelegd aan de opdrachtgever voor de definitieve opname in het onderzoek.

Hoewel de organisaties een afspiegeling zijn van de sector waarin ze werken, representeren ze deze sector niet op alle gebieden. Bij de selectie hanteerde Berenschot de volgende criteria: (i) de organisaties hebben een vergelijkbare centrale en decentrale inrichting als de overheid zelf, bijvoorbeeld in de vorm van een naamloze vennootschap (hierna: nv) met besloten vennootschappen (hierna: bv's) of geografische spreiding, (ii) de organisaties zijn 'groot' en hebben meer dan 1.000 fulltime medewerkers, (iii) de organisaties komen uit verschillende sectoren waarin verschillende type wet- en regelgeving geldt en, tot slot, (iv) de organisaties hebben, vermoedelijk, een hoge mate van professionalisering en volwassenheid op het gebied van informatieveiligheid en governance, compliance en risk (hierna: GRC) in brede zin. De onderzochte organisaties hebben toegestemd met dit onderzoek onder voorwaarde van anonimiteit.

Het gaat om de volgende geanonimiseerde organisaties:

- Organisatie 1 is één van de grootste zorgverzekeraars van Nederland.
- Organisatie 2 is een internationale beursgenoteerde onderneming.
- Organisatie 3 is één van de grootste banken van Nederland en wereldwijd actief in de financiële sector.
- Organisatie 4 is actief in Nederland en enkele omliggende landen op het gebied van vervoer.
- Organisatie 5 is één van de grootste zorgverzekeraars van Nederland.

In de interviews met de organisaties hebben we gesproken met de CISO's of diens plaatsvervanger of ondergeschikte. In een enkel geval hebben we gesproken met de verantwoordelijk directeur. Naast de onderzochte organisaties heeft Berenschot tot slot gesproken met een afvaardiging van BZK/DGDOO om de bevindingen bij de organisaties in de juiste context te kunnen beschouwen.

HOOFDSTUK 3

Beschrijving onderzochte organisaties

3.1 Organisatie 1

3.1.1 Feitelijke beschrijving

Organisatie 1 is één van de grootste zorgverzekeraars van Nederland en kent met miljoenen verzekerden een jaaromzet van miljarden. De organisatie heeft enkele duizenden medewerkers. De belangrijkste dienst is de uitvoering van de verplichte basisverzekering tegen ziektekosten. Daarnaast heeft de organisatie onder meer aanvullende ziektekostenverzekeringen. De organisatie is een rechtspersoon met een wettelijke taak en heeft geen winstoogmerk.

De organisatie werkt vanuit de aard van de organisatie zowel in de zorgsector als in de financiële dienstverlening. In de zorg(verzekerings)markt speelt de overheid een belangrijke rol en heeft de organisatie derhalve te maken met een breed spectrum aan wet- en regelgeving. Een zorgverzekeraar kent verschillende producten en diensten, die zich bovenal kenmerken door een hoge mate van vertrouwelijkheid en integriteit. Als zorgverzekeraar moet de organisatie voldoen aan financiële wetgeving, zoals de Wet op het financieel toezicht (hierna: Wft) of de Europese richtlijn Solvency II, waarin eisen worden gesteld aan onder meer risicomanagement, maar ook privacywetgeving als de Algemene Verordening Gegevensbescherming (hierna: AVG). Ook staat de organisatie onder toezicht van De Nederlandse Bank (hierna: DNB). Deze en andere wet- en regelgeving stelt op verschillende (bedrijfsvoerings-)aspecten specifieke eisen aan de organisatie.

Organisatie 1 kent een two-tier board als (dualistisch) bestuursmodel. Met een two-tier board is er een scheiding tussen directie en toezichthouders. De raad van bestuur (hierna: RvB) bestuurt de rechtspersonen, heeft de dagelijkse leiding over het bedrijf en is onder meer verantwoordelijk voor het beleid. De RvB wordt hierin ondersteund door directeuren en het management van onderliggende organisatieonderdelen De RvB is tevens verantwoordelijk voor de opzet en werking van de interne risicobeheersings- en controlesystemen. Een aparte raad van commissarissen (hierna: RvC) benoemt de RvB, houdt toezicht op het beleid van het bestuur, waarbij de RvB verantwoording aflegt over de gevoerde strategie en het risicomanagement. Naast een RvC en RvB kent de organisatie ook een Ledenraad, waarmee in spraak van verzekerende is gewaarborgd. De Ledenraad kent een onafhankelijke positie ten opzichte van de RvC en RvB en heeft vastgelegde taken en bevoegdheden.

3.1.2 Governance en inrichting

Binnen organisatie 1 is een functionaris belast met de taken zoals in algemene zin bij een CISO zijn belegd. Deze functionaris (hierna: CISO) is autonoom in het vervullen van zijn functie en beschikt over een eigen ‘CISO-team’ van tien professionals welke hij hiërarchisch aanstuurt. Ook beschikt hij over een eigen budget. De CISO rapporteert in eerste instantie aan de directeur verantwoordelijk voor ICT, maar kent tevens een directe lijn naar de RvB.

Enige tijd geleden is binnen organisatie 1 een ontwikkeling in gang gezet om 'security' meer naar de business te brengen en 'informatiebeveiliging daadwerkelijk onderdeel te laten zijn van het professionele handelen van elke medewerker'. De organisatie hanteert hierbij een *'Three Lines of Defense'*-model[4]. Het CISO-team functioneert, vanuit die ingezette ontwikkeling, in toenemende mate als 'tweedelijnsorganisatie', waarbij het kaderstellend, ondersteunend en monitorerend is. Het CISO-team faciliteert bijvoorbeeld pentesten onder verantwoordelijkheid van én op basis van een vraag van een organisatieonderdeel. Ook zorgt het CISO-team dat het (strategisch) informatiebeveiligingsbeleid en het tactisch en operationeel beleid volledig up-to-date is en goed vindbaar, zodat afdelingen in staat zijn autonoom te werken in lijn met de gestelde eisen en daarbij niet afhankelijk zijn van de beschikbaarheid van centrale expertise. De business is daarnaast bijvoorbeeld verantwoordelijk voor autorisatiebeheer door te zorgen voor de adequate toekenning en intrekking van toegangsrechten, en over de wijze waarop softwareontwikkeling plaatsvindt. De managers worden hierbij gefaciliteerd door periodieke inzichten, middels dashboards op specifieke KPI's[5], over de status van informatieveiligheid binnen hun afdeling en worden tevens naar alle waarschijnlijkheid in de toekomst ondersteund door zogenaamde business security-coördinatoren in de eerste lijn. De meer 'toezichthoudende' rol (conform het Three Lines of Defense-model) ligt bij een centrale GRC-/stafafdeling. Hoewel het CISO-team als 'tweedelijns' functioneert, voert het team ook nog naar eigen zeggen de nodige operationele 'eerstelijns' taken uit, waaronder centraal autorisatie beheer, functioneel beheer van informatiebeveiligingsproducten en het awareness programma.

De organisatie dient vanuit de aard van de organisatie te voldoen aan verschillende wet- en regelgeving binnen verschillende disciplines. De RvB laat zich op het gebied van informatiebeveiliging echter voornamelijk leiden door de beheersdoelstellingen die worden gehanteerd door DNB[6] aangevuld met die van Logius en andere interne doelstellingen. Middels de Good Practice Informatiebeveiliging (hierna: good practices) biedt DNB handvatten waarmee organisaties een praktische invulling kunnen geven aan die beheersingsmaatregelen. Het doel van de organisatie is hieraan geheel compliant te zijn of hoger. Hierbij is per beheersdoelstelling expliciet het eigenaarschap inclusief gerelateerde risico's benoemd én op de 'juiste plek' (en dus ook bij afdelingen) belegd. Compliant betekent daarbij, vanwege de wijze waarop DNB haar toezicht inricht, óók feitelijke informatieveiligheid. Zie verder § 3.1.4. De organisatie streeft niet alleen naar compliance omdat het moet, maar omdat de organisatie het intrinsiek ook wil.

Deze intrinsieke motivatie en de wijze waarop door organisatie 1 wordt omgegaan met informatiebeveiliging kan niet los worden gezien van de cultuur en daarbinnen de tone-at-the-top. Dit aspect wordt gezien als een cruciale randvoorwaarde en nadrukkelijke succesfactor in de wijze waarop de organisatie in staat is 'centraal te sturen' op informatieveiligheid en men 'decentraal uitvoert'. Hierbij wordt verwezen naar de aard van de organisatie en het type medische en financieel informatie dat wordt verwerkt. Door de aandacht voor privacy in de afgelopen jaren heeft men al geruime tijd oog voor dergelijke, in dit geval privacy-, risico's. Dit 'cultuuraspect' is daarbij niet slechts randvoorwaarde, maar één van de KPI's en wordt zodoende periodiek gemeten. Hierbij wordt gekeken naar aspecten zoals 'transparantie' of 'voorbeeldgedrag'.

4 Het Three Lines of Defense model wordt wereldwijd als de standaard gezien voor risicomanagement. Met dit model wordt onderscheid gemaakt in de 'business' (eerste lijn) die eindverantwoordelijk is voor de eigen processen en de risico's kent en beheerst. Daarnaast is er een functie die de eerste lijn ondersteunt, adviseert en coördineert (tweede lijn). Deze functie is verantwoordelijk voor het proces van risicomanagement en beheersing ter ondersteuning van de business. Tot slot is er een interne audit (derde lijn) die nagaat of de eerste en tweede lijn goed functioneert en hierover objectief en onafhankelijk een oordeel velt. Het model is inmiddels aangepast naar de 'Three Lines Model' (zie https://www.iia.nl/actualiteit/nieuws/belangrijke-update-three-lines-model). In deze rapportage hanteren we 'Three Lines of Defense' vanwege verwijzingen gedurende de interviews en de bredere herkenbaarheid.

5 KPI's zijn key performance indicatoren ofwel variabelen om prestaties van een organisatie, team en/of afzonderlijke medewerkers te meten, waarbij voortgang meetbaar en concreet wordt.

6 Conform art. 3.17 Wet Financieel Toezicht, juncto artikel 20 Besluit prudentiële regels en de Pensioenwet beschikken instellingen onder toezicht van DNB over adequate procedures en maatregelen ter beheersing van IT-risico's. Het gaat hierbij onder meer om het waarborgen van de integriteit, beschikbaarheid en de beveiliging van geautomatiseerde gegevens. Adequaat betekent in dit verband dat de procedures en maatregelen zijn gebaseerd op de aard, omvang en complexiteit van de risico's van de activiteiten van de instelling en de complexiteit van de organisatiestructuur. Zie ook: https://www.dnb.nl/voor-de-sector/open-boek-toezicht-fasen/lopend-toezicht/prudentieel-toezicht/governance/q-a-informatiebeveiliging/

Doordat de RvB gewend is om te gaan met strategische (en veelal financieel gedreven) risico's, en daarover op boardniveau het gesprek te voeren, en in het verleden meetbare stappen heeft gezet in de volwassenheid op het gebied van security, is hij ervaren in het werken met en centraal sturen op KPI's. Voor informatiebeveiliging zijn dan ook centraal een handvol essentiële KPI's opgesteld, die worden gekwantificeerd door feitelijke informatie uit de 'haarvaten' van de organisatie. Het gaat daarbij om KPI's als: de mate waarin autorisaties kloppen, afwijkingen op beleid, de genoemde DNB controls, risico's op phishing7, de kwaliteit van wachtwoorden of de mate waarin alle assets zijn geclassificeerd.

In lijn met de KPI's worden de inzichten en cijfers uit de organisatie daarnaast ieder kwartaal visueel inzichtelijk gemaakt in een 'klikbaar' en 'actionable' dashboard per organisatieonderdeel. Het belegde eigenaarschap wordt daarmee direct vertaald naar een concreet handelingsperspectief voor de verantwoordelijk manager of directeur. De verantwoordelijk directeur krijgt hierbij een risico met daaraan een gekoppelde actie. Deze actie vereist ook dat er vanuit het betreffend organisatieonderdeel een 'verbeterplan' komt. Indien hierop onvoldoende actie wordt ondernomen, kan een dergelijk risico geëscaleerd worden naar een volgend managementniveau en uiteindelijk bij de RvB terecht komen. Een dergelijke stap wordt nadrukkelijk als een 'tik op de vinger' ervaren.

De positie van de informatiebeveiliging, het gehanteerde en door DNB afgedwongen framework in combinatie met de daaropvolgende sturing vanuit de RvB middels KPI's, gevoed door informatie uit de gehele organisatie, stelt de organisatie in staat 'in control te zijn'. De stellingname wordt ondersteund door de in- en externe verantwoording. Zie verder § 3.1.4.

3.1.3 Risicomanagement

Risicomanagement (in brede zin) kent door de onder meer de financiële aard van de organisatie en daarmee samenhangende wettelijke eisen een lange historie. De organisatie brengt centraal gestructureerd de eigen risico's in kaart, waarbij de mogelijke gevolgen ervan worden beoordeeld en proactief maatregelen worden genomen om deze zoveel als mogelijk te beheersen. Op strategisch niveau is onder meer geëxpliciteerd dat men kiest voor een behoudende risicohouding, mede gezien de maatschappelijke rol die de organisatie vervuld,. Voor cybersecurity geldt zelf een risicomijdende risk appetite.

De rol of functie van risicomanagement is centraal georganiseerd en valt onder de GRC-/stafafdeling, waarbij risico's op het domein van informatieveiligheid één van de (strategische) onderdelen is. Vanuit de RvB is de focus van oudsher sterk gericht op zorgverzekeringsrisico's, zoals politieke ontwikkelingen, financiën of geografische ontwikkelingen. Risico's met betrekking tot cybersecurity worden de laatste jaren steeds actueler en staan hoog op de agenda. De focus van de centrale risicomanagementfunctie is met name strategisch van aard.

Risicomanagement (binnen informatiebeveiliging) is één van de belangrijkste pijlers. Binnen het CISO-team is risicomanagement een belangrijke onderdeel van het werk. Hiervoor worden twee fte ingezet. Vanuit de informatiebeveiligingsorganisatie ligt de focus daarbij voornamelijk op de operationele en tactische risico's. Deze risico's zijn zowel kwantitatief als kwalitatief van aard en worden vanuit het CISO-team aangeleverd bij GRC. Een belangrijke uitdaging daarbij is deze operationele en tactische risico's te laten aansluiten bij het (strategisch) risicomanagement van GRC. De voornaamste uitdaging, gezien de toenemende bedreigingen, is om 'cyberrisico's' te kwantificeren en de organisatie beter in staat te stellen vanuit strategisch (of 'organisatiebreed') perspectief in control te zijn. Eén van de te nemen stappen binnen de informatiebeveiligingsorganisatie is het inrichten van strakker risicomanagement bij het identificeren, classificeren en definiëren van de risico's en daaruit volgende acties. Deze uitdaging wordt breder (h)erkend en onder meer binnen het i-CERT[8] besproken.

Risicomanagement en de doorontwikkeling daarvan is daarnaast een essentieel onderdeel bij het toetsen van onder meer leveranciers vanwege de grote ketenafhankelijkheid. Organisatie 1 ziet dit als een belangrijke uitdaging voor de komende tijd en ziet hiervoor, in preventieve zin, nadrukkelijk een rol weggelegd voor 'Concern Inkoop'. Inzicht hoe leveranciers hun informatiebeveiliging op orde hebben in zowel 'opzet', 'bestaan' als 'werking', is daarvoor cruciaal. Commerciële initiatieven voor 'supplier information and risk management' zijn daarvoor veelbelovende stappen, aldus de geïnterviewde. De ketenafhankelijkheid blijft ontegenzeggelijk een groot risico. De daadwerkelijk implementatie van het concept zero trust in de gehele organisatie in onder andere architectuur en beleid en met in een ketensamenwerking de informatiebeveiliging daadwerkelijk testen zijn hierbij belangrijke vervolgstappen.

7 Medewerkers krijgen periodiek een test onder andere op phishing, maar ook andere aspecten van social engeneering

8 Zie https://www.verzekeraars.nl/publicaties/actueel/verzekeraars-verhogen-digitale-weerbaarheid-met-i-cert

3.1.4 Toetsing en verantwoording

De organisatie geeft aan een goed beeld te hebben van haar eigen volwassenheid. De doorwerking van de governance en inrichting, waarbij afwijkingen direct naar boven komen en de facto niet geaccepteerd worden, is hierbij een belangrijk pijler. Twee aspecten spelen daarbij een cruciale rol. Enerzijds heeft de organisatie een cultuur waarbij 'gebruiksvriendelijkheid niet altijd boven veiligheid gaat' en anderzijds speelt de (dreiging van) extern toetsing door en verantwoording aan DNB een belangrijke rol.

De gehele organisatie - van RvB tot elke verantwoordelijk manager en medewerker – heeft een actueel inzicht in de status van de informatieveiligheid. Doordat verantwoordelijkheden expliciet zijn belegd, op KPI's voortdurend wordt getoetst en hiërarchisch verantwoording wordt afgelegd, is de organisatie in staat een actueel getoetst inzicht te geven en dit te verantwoorden indien gewenst (in- of extern). Het CISO-team zorgt daarbij voor maandelijkse rapportages die worden aangeleverd aan de CIO over de beheersmaatregelen in relatie tot de risico's. Ook wordt gerapporteerd over de voorgang van de jaarplanning, inclusief de financiële en personele aspecten daarvan. Op hoger niveau verzorgt de GRC-afdeling de rapportages over de (kwalitatieve beschrijvingen van) strategische risico's aan de RvB, ook op het gebied van informatieveiligheid.

De (informatiebeveiligings-)organisatie laat zich sterk leiden door het versterkte toezicht van en de eisen van DNB. Hierbij ligt de focus op de operationele risico's die onder meer inzichtelijk worden gemaakt middels TIBER9. Een dergelijke aanvalssimulatie toont de daadwerkelijk weerbaarheid (en spreekt dus niet over de papieren werkelijkheid van opzet of bestaan van controls) en geeft een diep, actueel en doorwrocht inzicht in de kwetsbaarheden van de organisatie, zoals inzicht in de applicaties, hoe het netwerk eruitziet, hoe de internetbeveiliging geregeld is et cetera. Ondanks dat dergelijk 'toezicht' of 'toetsing' als een fikse inspanning wordt ervaren, blijft het bovenliggende doel van 'te leren' overeind. Dit onderschrijft de cultuur van de organisatie in het voortdurend willen leren en lessen te trekken voordat een incident plaatsvindt.

9 TIBER staat voor Threat Intelligence Based Ethical Red-teaming. Binnen dit programma testen financiële instellingen hoe weerbaar ze zijn tegen geavanceerde cyberaanvallen. Een instelling kan niet slagen of zakken voor zo'n test. Doel is om inzicht te krijgen in sterke en zwakke punten en om beter te worden. Instellingen delen hun ervaringen en verbeterplannen met elkaar. Zo profiteert de gehele sector van een test. In TIBER-NL-tests worden de tactieken, technieken en procedures van echte hackersgroepen nagebootst op basis van specifieke dreigingen voor de instelling. Er vindt een gecontroleerde aanval plaats op onder andere de kritieke functies van de instelling. Hierbij kunnen mensen, processen en IT-infrastructuur doelwit zijn. Bij de instelling zijn slechts een paar mensen op de hoogte dat er een testaanval plaatsvindt.

3.2 Organisatie 2

3.2.1 Feitelijke beschrijving

Organisatie 2 is een beursgenoteerde onderneming. Het bedrijf kent een gelaagde organisatie met verschillende besloten vennootschappen (bv's) binnen een naamloze vennootschap (nv). Het hoofdkantoor is gevestigd in Nederland. Organisatie 2 heeft een omzet van miljarden en is actief in verschillende sectoren.

Doordat de organisatie wereldwijd in verschillende jurisdicties in verschillende sectoren actief is, dient de organisatie aan een breed spectrum wet- en regelgeving te voldoen op nationaal, Europees en internationaal niveau. Deze wet- en regelgeving stelt op verschillende (bedrijfsvoerings-) aspecten specifieke eisen aan de organisatie. De internationale context zorgt ook voor extra uitdagingen op het gebied van GRC en informatieveiligheid. Organisatie 2 werkt in Nederland ook aan vitale infrastructuur, waardoor vanuit betreffende organisaties aanvullende of meer specifieke eisen worden gesteld. Voor organisatie 2 is beschikbaarheid van informatie voor de business het belangrijkste aspect. De geïnterviewde geeft aan dat downtime (of niet-beschikbaarheid) wordt gezien als groot risico voor de informatieveiligheid.

Ook organisatie 2 kent een dualistisch bestuursmodel, waarbij onderscheid gemaakt wordt tussen een executive board en supervisory board. Ook wordt onderscheid gemaakt in een zogenaamde Three Lines of Defense. De organisatie kent geen zogenaamde 'landenstructuur', waarbij een internationale organisatie per land (en niet bijvoorbeeld per sector) is georganiseerd. Veel bedrijfsvoeringsprocessen, waaronder GRC en informatieveiligheid, zijn centraal en daarmee wereldwijd georganiseerd.

3.2.2 Governance en inrichting

De organisatie is ingericht conform het Three Lines of Defense-model, waarbij GRC functioneert als een tweedelijns-functie. Binnen deze tweede lijn is ook de informatie-beveiligingsorganisatie georganiseerd ter ondersteuning van de eerste lijn bij het identificeren en mitigeren van risico's op organisatiebrede risico's. Deze risico's hebben onder meer betrekking op de financiële aspecten, maar focussen zich ook in toenemende mate specifiek op de risico's met betrekking tot informatiebeveiliging.

Binnen de tweede lijn en de 'informatiebeveiligingsfunctie' is een 'global information security officer' (hierna: CISO) aangesteld. De CISO ressorteert nadrukkelijk buiten de IT-afdeling vanwege de bredere scope van zijn werk. Binnen het CISO-team werken zo'n 18 fte's die zich bezighouden met onder meer security en compliance, risk management en het monitoren van de infrastructuur middels een SOC. Het team laat zich daarbij ondersteunen door verschillende externe organisaties. De CISO en het CISO-team beschikken over voldoende middelen en worden hierin gesteund door de top van de organisatie. De werking hiervan blijkt onder meer uit de directe lijnen vanuit de CISO naar het executive board én diens directie lijn naar het supervisory board, via een onderliggend committee, en de externe verantwoording die hierover wordt afgelegd in onder meer de jaarrekeningen.

Binnen de organisatie wordt voor GRC een breed geïntegreerd framework gehanteerd, waarbinnen een security control framework is uitgewerkt. Beide frameworks zijn global gedefinieerd en beschrijven het beleid, de eisen etcetera. Voor informatiebeveiliging wordt gebruikt gemaakt van een 'global Information Security Management System (hierna: ISMS)' met daarin een set controls die in lijn zijn met de ISO27001.

De recente, succesvolle implementatie van ISO27001 in Nederland heeft ertoe geleid dat wereldwijd deze standaard is of wordt geïmplementeerd. Deze implementatie wordt gezien als een belangrijke driver voor alle wereldwijde organisaties en organisatieonderdelen om actief te (gaan) voldoen aan de gestelde eisen, waarbij ook aandacht is om dit op een juiste en eenduidige werkwijze te doen. Het gaat daarbij bijvoorbeeld om de manier waarop classificaties van informatie en systemen plaatsvindt. De oorsprong van de wereldwijde implementatie van de door een overheidsorganisatie gestelde eisen bij een project ligt in Nederland. Doordat in Nederland deze eisen werden gesteld, werd de organisatie gedwongen deze gestructureerd op te pakken. Hoewel dit als een positieve motivatie werd gezien, werd tevens benadrukt dat overheden in Nederland soms verschillende eisen stellen, waarbij de ene overheidsorganisatie strikter is dan de ander: zo zou een rijksoverheidsorganisatie daadwerkelijk toetsen, terwijl een andere overheidsorganisatie slechts een vragenlijst zou hanteren. Ook de Algemene Beveiligingseisen voor Defensieopdrachten, kortweg ABDO, wordt vanwege de duidelijke structuur als een best practice genoemd.

De (huidige) wereldwijde verschillen worden ook deels verklaard doordat internationaal verschillende standaarden worden gehanteerd. Zo wordt in de Verenigde Staten (hierna: VS) veelal gebruik gemaakt van de NIST, waarbij meer aandacht is voor de technische aspecten. In het Verenigd Koninkrijk (hierna: VK) hanteert men dan weer de zogenaamde cyber essentials[10]. Doordat de organisatie globaal werkzaam is, zijn de eisen hieromtrent wel meegenomen in het ISMS.

De (sturing op de) strategische risico's wordt uitgewerkt middels KPI's (binnen het bredere GRC). Deze indicatoren variëren van (i) hoeveel mensen hebben een awarenesstraining gevolgd of (ii) hoeveel incidenten of securitymeldingen zijn er tot (iii) hoeveel van de leveranciers zijn er ISO27001 gecertificeerd. De resultaten op deze en andere KPI's worden voortdurend gemonitord en besproken met de executive board en de supervisory board. Een speciaal committee op het gebied van informatiebeveiliging onder leiding van de CEO stuurt hierbij nadrukkelijk op de vraag in hoeverre de organisatie 'in control' is en overziet daarbij de risk posture en zorgt ervoor dat die in lijn is met afgesproken risicomijdende risk appetite.

3.2.3 Risicomanagement

Risicomanagement (in brede zin) kent, evenals bij organisatie 1, door de aard, omvang en globale spreiding van de organisatie en daarmee samenhangende wettelijke eisen een lange historie. In lijn met de Three Lines of Defense is de functie van het risicomanagement centraal georganiseerd en deze valt onder de tweedelijns GRC. De organisatie brengt centraal gestructureerd de risico's van de organisatie in kaart, waarbij de mogelijke gevolgen ervan worden beoordeeld en proactief maatregelen worden genomen om de gevolgen zoveel als mogelijk te beheersen. Het belang van goed (strategisch) risicomanagement hangt nauw samen met het feit dat de organisatie beursgenoteerd is.

Op strategisch niveau is onder meer geëxpliciteerd dat informatieveiligheid een operationeel risico is. De organisatie kiest hiervoor dan ook een risicomijdende risicohouding. Voor het CISO-team is risicomanagement één van de belangrijkste pijlers en het meest cruciale onderdeel van het werk. Om dit proces te faciliteren, wordt gebruik gemaakt van een tool, waarmee met één druk op de knop een actueel overzicht is te verkrijgen van alle risico's op het gebied van informatieveiligheid. De tool wordt gevuld met onder meer incidenten, afwijkingen op beleid en koppelt dit aan de controls van de ISO27001.

10 Zie https://www.ncsc.gov.uk/cyberessentials/overview

Naast het belang van het goed onderhouden van de eigen informatieveiligheid onderschrijft de organisatie de uitdagingen op het vlak van ketenafhankelijkheid en de wijze waarop het beste met leveranciers kan of moet worden omgegaan. Eén van de KPI's is dan ook de mate waarin de leveranciers voldoen aan de ISO27001. In de praktijk betekent dit dat leveranciers moeten aantonen dat ze voldoen aan bepaalde criteria, waarbij de eisen vanuit de organisatie naar eigen zeggen alsmaar strenger worden. Dit doet de organisatie middels het eisen van een ISO-verklaring en het afnemen van een vragenlijst. Indien een leverancier hieraan niet kan voldoen, bepaalt de directie of met de betreffende leverancier in zee kan worden gegaan middels een security acception. Deze lijn trekt de organisatie ook door naar de wijze waarop ze met haar klanten omgaat en de wijze waarop de klant aan de gestelde eisen voldoet. In de praktijk betekent dit dat de organisatie bij haar klant bijvoorbeeld een applicatie heeft getest die zij geacht werd te gebruiken. De bevindingen uit dit onderzoek waren dermate ernstig dat de organisatie samen met de leverancier de kwetsbaarheden heeft verholpen. In diezelfde lijn worden klanten 'gescand' via een platform. Desondanks blijft de basis het op orde brengen van de ketenafhankelijkheid en het in gesprek blijven met de klant en de leveranciers.

3.2.4 Toetsing en verantwoording

De organisatie geeft aan een goed beeld te hebben van de volwassenheid van de organisatie: de doorwerking van de governance en inrichting, waarbij afwijkingen direct naar boven komen, is hierbij een belangrijk pijler. Een belangrijk aspect daarbij is dat organisatie 2 door een dualistisch bestuursmodel gecombineerd met de ingerichte Three Lines of Defense in staat is een adequaat en goed beeld te geven van de status van informatieveiligheid van de gehele organisatie. De organisatie steunt daarbij op een voortdurend actueel inzicht op basis van de gehanteerde frameworks en daarbinnen gehanteerde set aan controls. Ondersteunende instrumenten op het gebied van risicomanagement geven daarnaast een actueel inzicht. Binnen de organisatie wordt streng toegezien op het voldoen aan de gestelde eisen en kan, indien bijvoorbeeld een medewerker afwijkt qua eisen, er zelfs toe leiden dat disciplinaire stappen worden ondernomen of dat de medewerker bepaalde functionaliteiten wordt ontzegd. Een tweede aspect is om de intrinsieke motivatie daadwerkelijk te willen verbeteren. Deze motivatie wordt gevoed door de groeiende risk posture en ambities van de organisatie op het digitale vlak. Informatieveiligheid staat vanuit dat perspectief hoog op agenda van de supervisory board en de interne audit als derde lijn.

Doordat verantwoordelijkheden expliciet zijn belegd, op KPI's voortdurend wordt getoetst en hiërarchisch verantwoording wordt afgelegd, is de organisatie in staat een actueel getoetst inzicht op te leveren en hierover verantwoording af te leggen, indien gewenst (in- of extern). Externe toetsing of verantwoording door de Nederlandse overheid bij één specifiek project heeft door de implementatie van de ISO27001 uiteindelijk geleid tot een globale doorontwikkeling van de informatieveiligheid van de organisatie. Hoewel deze wereldwijde implementatie niet het primaire beoogde effect had, heeft het stellen van eisen (of de (dreiging van) externe toetsing of verantwoording) wel degelijk invloed gehad. Dergelijke overheidseisen moeten dan wel gestandaardiseerd worden.

3.3 Organisatie 3

3.3.1 Feitelijke beschrijving

Organisatie 3 is één van de grootste banken van Nederland en wereldwijd actief in de financiële sector. De organisatie is beursgenoteerd en kent wereldwijd duizenden fulltime medewerkers. De organisatie behaalde in de afgelopen jaren telkens een miljardenomzet en richt zich met haar producten en dienstverlening onder meer op vermogen, corporate en private banking.

Zowel op nationaal als Europees niveau is de bankensector sterk gereguleerd, waardoor de organisatie hoge eisen moet stellen aan de eigen organisatie. Vanuit de type producten en dienstverlening moet de organisatie voldoen aan uiteenlopende wet- en regelgeving, zoals de Wft, Wet ter voorkoming van witwassen en financieren van terrorisme (hierna: Wwft) of de Europese richtlijn Solvency II. Ook staat de organisatie onder toezicht van DNB en de Autoriteit Financiële Markten (hierna: AFM). Met onder meer de verwachte introductie van de Digital Operational Resilience Act (hierna: DORA), ontwikkeld om het (cyber)risicomanagement en operationele weerbaarheid te versterken, zullen deze eisen alsmaar verzwaren.

Informatie is één van de meest waardevolle middelen van de organisatie, waarbij de processen onderdeel zijn van de vitale infrastructuur van Nederland. Klanten vertrouwen in toenemende mate op diensten als online bankieren. Het juist functioneren van de IT-systemen is dan ook cruciaal. De systemen van de bank zijn onderdeel van complexe infrastructuren, waarbij de bank verbonden is met allerlei andere (publieke) netwerken. Dit heeft tot gevolg dat de processen en onderliggende systemen van de bank inherent interessant zijn voor cyberaanvallen. De bank ziet het dan ook als belangrijke verantwoordelijkheid om de informatie, privacy en geld van haar klanten adequaat te beschermen.

Evenals organisatie 1 en 2 kent organisatie 3 een dualistisch bestuursmodel, dat bestaat uit een raad van bestuur en raad van commissarissen. De organisatie kent ook het onderscheid in de Three Lines of Defense, waarbij het omgaan met risico's binnen het gematigde risicoprofiel van de bank in de eerste lijn is belegd, de tweede lijn de risicomanagementfunctie invult en de eerste lijn ondersteunt en uitdaagt om daadwerkelijk het eigenschap en de verantwoordelijkheid van het risico te nemen. De tweede lijn toetst op het beleid en de richtlijnen, zoals de wijze waarop met autorisaties wordt omgegaan. De derde lijn vormt de 'interne audit' en is verantwoordelijk voor het evalueren van dit proces en het hierover intern verantwoording afleggen. Naast de interne audit legt de bank ook jaarlijks verantwoording af aan de externe auditor die, naast de financiële aspecten, ook kijkt naar security. De organisatie kent geen zogenaamde landenstructuur. De bedrijfsvoeringsprocessen, waaronder risicomanagement en informatieveiligheid, zijn dan ook centraal en daarmee wereldwijd, georganiseerd.

3.3.2 Governance en inrichting

Binnen de organisatie zijn veel processen, services en capabilities centraal georganiseerd, waarbij een aparte informatiebeveiligingsorganisatie is ingericht. Aan het hoofd van deze informatiebeveiligingsorganisatie, dan wel CISO-office, staat een CISO. Deze CISO-office valt onder de eerste lijn en heeft een wereldwijd mandaat. De CISO-organisatie zet de security strategie uit en ondersteunt met honderden fulltime medewerkers de business in alle landen en continenten. Daarbij wordt opgemerkt dat ten opzichte van andere grootbanken de CISO-organisatie relatief groot is, omdat ook andere taken en werkzaamheden worden verricht (zoals fraude in de betaalketen en andere vormen van financieel economische criminaliteit) dan taken strikt op het gebied van informatieveiligheid.

De CISO-office bestaat uit verschillende afdeling, zoals een Security Operations Center (SOC), Identity & Access Management en een afdeling gericht op awareness en communicatie, waar opleidingsprogramma's worden ontwikkeld voor medewerkers. Ook kent de CISO-office een afdeling specifiek gericht op de governance en organisatie, waarbij onder meer gekeken wordt naar de eisen vanuit DNB.

Om de verantwoordelijkheid van de bank aan klanten waar te kunnen maken, hanteert de organisatie een zogenaamd information security risk framework, waarmee wordt gezorgd dat de beschikbaarheid, integriteit en vertrouwelijkheid te allen tijde wordt gewaarborgd. In dit framework worden onder meer rollen en verantwoordelijkheden geëxpliciteerd, de organisatorische structuren beschreven en richtlijnen uitgewerkt die van toepassing zijn op de bank, leveranciers en andere partijen waarmee informatie wordt uitgewisseld. Het beleid en de richtlijnen zijn wereldwijd en organisatiebreed van toepassing en worden jaarlijks gereviewed en, indien nodig, geactualiseerd. Het framework hanteert de vijf stappen van het NIST Cybersecurity Framework[11]. De organisatie heeft op basis van dit framework per fase zogenaamde capabilities uitgewerkt, waaraan weer maatregelen zijn gekoppeld. Bij 'access control' gaat het dan bijvoorbeeld om de periodieke controles op toegangsrechten, bij 'awareness' om micro learnings of de inzet van een cybersecuritygame en bij 'network protection' om allerlei veelal technische maatregelen zoals (web application) firewalls of IDS. De bank ziet binnen het framework en externe dreigingen een belangrijke uitdaging op het gebied van 'recovery'.

De organisatie hanteert verschillende KPI's, waarbij de deze wereldwijd vergeleken kunnen worden, zodat inzichtelijk is waar het goed en minder goed gaat. Op basis van het beleid worden standaarden en eventuele werkinstructies uitgewerkt. Een belangrijke (set aan) KPI's is Entity Levels Controls and Assessments (hierna: ELCA), waarbij onder meer aandacht is voor hardening. In die context zijn eerder maatregelen genomen op het gebied van SSO en het dichtzetten van USB-poorten. Deze ELCA's worden opgesteld door de tweede lijn, waarbij de eerste lijn moet aantonen hieraan te voldoen.

11 De vijf stappen zijn 'Identify', 'Protect', 'Detect', 'Respond' en 'Recover'. Zie https://www.nist.gov/cyberframework

De RvB krijgt ieder kwartaal een update vanuit een dashboard, waar op basis van TLP een overzicht wordt gegeven van de stand van zaken per gestelde KPI. De RvB wordt hierin ondersteund door verschillende risk committees. Zie ook § 3.3.3. De inzichten vormen de basis om op specifieke onderdelen nader in te zoomen. IAM en incident response zijn onderwerpen die bijvoorbeeld blijvend om aandacht vragen.

Om daadwerkelijk goed inzicht te krijgen in de haarvaten van de organisatie zijn binnen de organisatieonderdelen functionarissen aangesteld om zowel strategisch als operationeel invulling te geven aan informatieveiligheid binnen dat onderdeel van de business. Hiërarchisch vallen deze functionarissen onder de CISO met een functionele lijn naar de business. In hun taakuitvoering zijn zij feitelijk een liason voor de CISO. Deze security officers functioneren in deze constructie in een matrix.

Buiten de organisatie deelt de bank veel ervaringen met andere banken, zoals best practices en operationele informatie met betrekking tot dreigingen en kwetsbaarheden. Het uitgangspunt daarbij is dat banken in dergelijke samenwerkingsverbanden, en dat geldt ook voor andere sectoren, niet concurreren op het gebied van cybersecurity. Dergelijke samenwerkingen gaan ook verder en richten zich bijvoorbeeld op innovaties om cybersecurity te verbeteren. Dit doen de banken met verschillende kennispartners, zoals binnen het PCSI-programma[12]. Tevens werken ze samen op het gebied van Threat Intelligence en security met andere banken en grote bedrijven in Nederland. Bij dergelijke innovaties wordt bijvoorbeeld gekeken naar strategische (technologische) ontwikkelingen, maar ook naar aspecten op het gebied van de human factor en hoe zaken structureel verbeterd kunnen worden.

3.3.3 Risicomanagement

Risicomanagement is één van de belangrijkste pijlers voor de bank, waarbij één lid van de RvB expliciet de verantwoordelijkheid draagt. De risico's waar de organisatie (mogelijk) aan bloot wordt gesteld, zijn ingedeeld in de verschillende hoofdcategorieën. De bank maakt hierbij onderscheid in financiële risico's en niet-financiële risico's. Onder de niet-financiële risico's vallen onder meer datalekken en cyberrisico's. Om dergelijke risico's adequaat te kunnen beheersen, is in lijn met de Three Lines of Defense een organisatiebrede risk governance ingericht, waarin de RvB en RvC op het allerhoogste niveau een belangrijke rol spelen.

Om risico's beheersbaar te houden, wordt een organisatiebreed framework gehanteerd. De bank hanteert een gematigd risicoprofiel en zet bij haar medewerkers middels communicatie, training en toetsing bij beoordelingen voortdurend in op risicobewustzijn als integraal onderdeel van de organisatiebrede risicocultuur.

Om de operationele risico's, zoals op het gebied van informatieveiligheid, te kunnen beheersen, hanteert de bank een apart framework, waarbij onder meer specifieke aandacht is voor compliance, informatieveiligheid en bedrijfscontinuïteit. Managers in de eerste lijn dragen zorg voor het identificeren en mitigeren van de risico's en controleren periodiek de effectiviteit van de maatregelen binnen hun verantwoordelijkheid. Bij een dergelijke verantwoordelijkheid behoort ook een duidelijk handelingsperspectief. Weet de business wat ze behoren te doen, ook als het bijvoorbeeld gaat om incident respons of recovery? Vanuit de gehele organisatie komen dergelijke risico's bij elkaar, worden periodiek besproken en uiteindelijk geaggregeerd en op strategisch niveau gerapporteerd aan een vertegenwoordiging van de RvB in een 'Group Risk Committee'. Een enkel risico, zoals het gebruik van verschillende softwarepakketten voor videoconferenties tijdens corona, zorgde uiteindelijk voor een overzicht van de gebruikte pakketten en vormde een belangrijke basis om shadow IT verder op te pakken.

De bank zet zich actief in om voortdurende de meest actuele 'informatie van buiten de organisatie' te hebben. Zo is er een threat intelligence team en wordt gekeken naar welke (type) aanvallen in de markt, bij andere banken of bij leveranciers plaatsvinden, welke toekomstige ontwikkelingen er spelen (zoals wet- en regelgeving) of welke ontwikkelingen of dreigingen op de middellange termijn een risico gaan vormen. Op basis van deze inzichten worden risicoanalyses gemaakt en in zogenaamde risk quadrants geplaatst. Afhankelijk van het type risico en indeling wordt vervolgens gekeken welke maatregelen noodzakelijk zijn.

12 Zie https://pcsi.nl/

Ketenafhankelijkheid en leveranciers vormen in toenemende mate een specifiek aandachtsgebied, waarbij supply chain attacks - een type aanval waarbij de organisatie aangevallen wordt via een zwakke schakel in de logistieke keten van de organisatie - bijzondere aandacht krijgt. De grootste opgave zit daarbij in de wijze waarop je als organisatie in staat bent informatieveiligheid in de keten te garanderen. Ketenveiligheid vereist, mede vanwege de verantwoordelijkheid als vitaal proces, dat je eisen stelt aan je keten en leveranciers. De bank hanteert dan ook het uitgangspunt dat je je leveranciers en partners voortdurend mee moet nemen en beschouwt dat zelfs als vierde pijler binnen people, process, technology en, aanvullend, partners. Om dit risico te ondervangen, zet de bank nadrukkelijk in op Vendor Security Management, waarbij er specifiek aandacht is voor (het mitigeren van) risico's in relatie tot leveranciers. In het verleden werd hierbij voornamelijk gekeken naar IT-leveranciers, maar de inspanningen zijn inmiddels verbreed tot alle leveranciers. De bank vraagt in dit kader onder meer alle (beoogde) leveranciers om vragenlijsten in te vullen, brengt on premise-bezoeken, gebruikt commerciële tools en platforms en doet soms pentesten. Indien een organisatie hieraan niet kan of wil voldoen, dan stopt de samenwerking. De bank ervaart anderzijds dat grote klanten vergelijkbare eisen aan haar stellen, zoals certificering op ISO27001 of ISAE 3402.

3.3.4 Toetsing en verantwoording

De bank geeft aan een goed beeld te hebben van de volwassenheid van de organisatie. In lijn met andere sterk gereguleerde organisaties in dit onderzoek is een belangrijke rol weggelegd voor de interne governance en inrichting (waarbij een belangrijke rol is weggelegd voor de Three Lines of Defense). De wijze waarop met risico's wordt omgegaan en de (dreiging van) extern toetsing door en verantwoording aan DNB is ook belangrijk. Niet voldoen kan immers grote consequenties hebben.

In de wijze waarop wordt omgegaan met risico's worden twee aspecten uitgelicht. Enerzijds is de bank goed in staat te reageren op interne afwijkingen. Dergelijke afwijkingen worden snel geconstateerd door de aan de business gekoppelde information security officer. Bij afwijkingen van de risk appetite wordt een issue aangemaakt en is het aan de business om dat op te lossen. Indien een risico niet adequaat wordt opgepakt, dient de verantwoordelijk manager uiteindelijk 'op het matje te komen' bij een risk committee, waarbij hij of zij een deadline krijgt opgelegd om het issue op te lossen middels een verbeterplan. Indien een dergelijke escalatie onvoldoende blijkt, is een 'onprettige' escalatie naar het Group Risk Committee de finale stap. Anderzijds is de wijze waarop de bank omgaat met externe afwijkingen (bij leveranciers) een essentieel aspect. Aangezien de bank een grote naam heeft, zijn leveranciers vrijwel altijd bereid om binnen een besproken termijn te voldoen aan de gestelde eisen. Als dat in een enkele keer niet het geval blijkt of als er sprake is van onwil dan wordt simpelweg afscheid genomen van die leverancier.

Tot slot is de sterke regulering van de sector net als bij organisatie 1 een nadrukkelijke aansporing om de werking van alle controls op orde te hebben. Op de momenten dat bijvoorbeeld de Europese Centrale Bank (hierna: ECB) langskomt, verlangt ze telkens bewijs en worden steekproeven gedaan. Dergelijke trajecten, evenals het eerder genoemde TIBER, zijn voor de bank intensief. Een onafhankelijke, goed functionerende, interne derde lijn zorgt er echter voor dat dergelijke trajecten (redelijk) positief worden afgerond.

3.4 Organisatie 4

3.4.1 Feitelijke beschrijving

Organisatie 4 is actief in Nederland en enkele omliggende landen op het gebied van vervoer. Het bedrijf is een naamloze vennootschap. De organisatie heeft ook enkele bv's. Het hoofdkantoor is gevestigd in Nederland. In Nederland zijn enkele tienduizenden fulltime medewerkers werkzaam en behaalde de organisatie een omzet van enkele miljarden.

De organisatie verleent diensten in het hart van de Nederlandse samenleving en heeft in de dagelijkse operatie te maken met informatietechnologie (IT), operational technology (OT) en ketenafhankelijkheden en beschikt dan ook over veel data en (persoons)gegevens. De dienstverlening is een vitaal proces en als organisatie een Aanbieder Essentiele Dienst (AED). Een verstoring, aantasting of uitval van een dergelijk proces heeft grote gevolgen voor Nederland. De organisatie dient zich aan verschillende wet- en regelgeving te houden op nationaal en Europees niveau, waaronder de Wet Beveiliging Netwerk- en Informatiesystemen (hierna: Wbni). Deze en andere wet- en regelgeving stelt op verschillende (bedrijfsvoerings)aspecten specifieke eisen aan de organisatie, zoals, in het geval van de Wbni, een meldplicht van incidenten en een zorgplicht voor het treffen van adequate beveiligingsmaatregelen. Continuïteit van de dienstverlening én veilige dienstverlening is daarbij een belangrijke opgave.

Ook organisatie 4 kent een dualistisch bestuursmodel, waarbij onderscheid gemaakt wordt tussen een RvB en RvC. Binnen de organisatie wordt gewerkt volgens het Three Lines of Defense model. De lijnorganisatie (eerste lijn) is verantwoordelijk is voor het uitvoeren van risicomanagement. De tweede lijn draagt zorg voor het beleid, ondersteuning en bewaakt of de lijnorganisatie de verantwoordelijkheid neemt voor het risico-management. Cybersecurity valt binnen dit risicomanagement-proces, waarbij de CISO zich richt op de onderwerpen informatiebeveiliging en cybersecurity. De derde lijn toetst, zoals ook bij de andere organisaties, of de eerste en tweede lijn adequaat functioneren. De bedrijfsvoeringsprocessen, waaronder GRC en informatieveiligheid, zijn centraal georganiseerd.

3.4.2 Governance en inrichting

Binnen organisatie 4 is een CISO belast met de taken en verantwoordelijkheden op dit gebied. De CISO is een onafhankelijke tweedelijnsfunctie en geeft onder meer vorm aan de strategie van de organisatie op het werkveld van informatiebeveiliging en cybersecurity en bereidt de organisatie voor op (aangescherpte of nieuwe) wet- en regelgeving. De CISO is verantwoordelijk voor het centrale en organisatiebreed toegepaste informatiebeveiligingsbeleid en het toezicht daarop vanuit de tweede lijn.

De CISO valt binnen de tweede lijn en stuurt security-collega's in de eerste lijn functioneel aan. De CISO werkt daarnaast nauw samen met collega's uit de bredere risk-functie. De CISO beschikt daarnaast over een 'eigen' CISO-team met tien voltijds medewerkers en flexibele inhuur en heeft een eigen budget. De CISO rapporteert aan de directeur Risk en Compliance, die op zijn beurt rechtstreeks rapporteert aan de president directeur.

Aan de hand van een roadmap wordt de informatieveiligheid en cybersecurity voortdurend versterkt. Deze versterking is deels procesmatig op het gebied van governance en beleid en deels inhoudelijk op het gebied van IT en OT. Organisatie 4 steunt daarbij op grote externe leveranciers en heeft hiervoor een duidelijke governance afgesproken, waaronder een stuurgroep mét die leveranciers.

Enige tijd geleden is binnen de organisatie een ontwikkeling in gang gezet om IT en daarmee cybersecurity meer naar de business te brengen. In de uitvoering van de tweedelijnsfunctie is de verantwoordelijkheid uitgewerkt in een zogenaamd CyberSecurity Management Systeem (hierna: CSMS), vergelijkbaar met een ISMS. In dit systeem wordt beleid uitgewerkt in onder meer centrale standaarden en richtlijnen. Op verschillende vlakken, zoals IT of bijvoorbeeld incident response, is in toenemende mate een verschuiving te zien naar de business. Bij de business liggen, in lijn met de Three Lines of Defense, immers de verantwoordelijkheden én specifieke kennis. Op het gebied van OT is die heel anders dan op het gebied van IT.

Door de uitlopende bedrijfsmiddelen van de organisatie worden verschillende frameworks, normenkaders en (sectorspecifieke) standaarden gehanteerd binnen het CSMS. Verschillende (type) systemen vragen om verschillende eisen, die mede worden bepaald door wet- en regelgeving. Hoewel de organisatie een publieke taak heeft, is zij niet gebonden aan de BIO. Het voldoen aan de juiste wet- en regelgeving is echter wel een belangrijk aspect. Zo is een certificering op ISO27001 bij de beoogde leveranciers een 'knock-out-criterium'. In het verleden werd het NIST-framework gehanteerd, maar inmiddels vormt het risicomanagement de kern. Middels dreigingen en kwetsbaarheden volgens het proces van BIA's worden risico's inzichtelijk gemaakt, geduid in heat maps, opgevolgd in een roadmap en nadrukkelijk gevolgd door de RvB. De uitdaging daarbij is risico's steeds meer te kwantificeren.

Vanuit de organisatie vind jaarlijks een classificatie van de informatie en informatiesystemen plaats. Op basis van de BIV wordt bezien in hoeverre een bedrijfsmiddel een zogenaamd kroonjuweel is. Bij de score van drie op één van de aspecten is het een kroonjuweel en dienen onder meer vijftien basismaatregelen genomen te worden. Deze kroonjuwelen krijgen de meeste aandacht in de organisatie en op deze controls moet dan ook 100% gescoord worden. Op dit moment kent de organisatie zo'n 200 kroonjuwelen.

In lijn met de andere organisaties worden risico's ook expliciet belegd bij de eerste lijn. Als het om grote risico's gaat en de risicobereidheid niet wordt overschreden, dient de betreffende manager het op te lossen. Risico's buiten de risicobereidheid worden direct gerapporteerd en indien nodig geëscaleerd.

Naast de governance en inrichting wordt cultuur gezien als een cruciale randvoorwaarde en een nadrukkelijke succesfactor in de wijze waarop de organisatie in staat is 'centraal te sturen' op informatieveiligheid en men 'decentraal uitvoert'. Hierbij wordt verwezen naar de aard van de organisatie, de dienstverlening en een risicobewuste cultuur op andere veiligheidsdomeinen. Voor dat laatste aspect wordt onder meer gebruik gemaakt van een QHSE-framework (Quality, Health, Safety and Environment). Dit aspect krijgt dan ook nadrukkelijke aandacht in de (executie van de) strategie (zoals roadshow, micro learnings, phishingcampagnes etc.). Awareness is daarbij een 'persoonlijke' KPI van de CISO, waarbij hij dit onderwerp meeneemt in iedere meeting met de RvB of RvC.

3.4.3 Risicomanagement

Risicomanagement is integraal onderdeel van de organisatie en vormt de kern van de Three Lines of Defense. De organisatie hanteert verschillende risicothema's en daaraan gekoppelde risicobereidheid. Risico's worden ingedeeld naar de mate van kans van optreden en de mate van impact op de strategische doelstellingen. Aan alle risicothema's zijn concrete KPI's gekoppeld. De risicobereidheid wordt jaarlijks per thema door de RvB geëvalueerd en indien nodig aangepast.

Geïdentificeerde risico's zijn met de risico-eigenaar in risicoregisters vastgelegd en worden gescoord met behulp van één uniforme risicomatrix. Per kwartaal worden de voornaamste risico's per bedrijfsonderdeel gerapporteerd en besproken in de RvB als onderdeel van de planning- en controlcyclus. De RvB rapporteert en legt verantwoording af over het risicomanagement en de interne controle aan de RvC. De organisatie gebruikt hiervoor onder meer een GRC-tool en ICF-tool.

De CISO vervult vanuit diens rol in de tweede lijn een belangrijke rol in het bijhouden van risico's en dreigingen binnen het onderdeel. Een toename aan zero days of een verhoogd dreigingslandschap leidt daarbij tot eerder patchmanagement en/of incidentmanagement.

Ketenafhankelijkheden en de wijze waarop met leveranciers wordt omgegaan, vraagt om blijvende aandacht. De organisatie heeft bijvoorbeeld een gedeelde van de infrastructuur on premise, maar ook op onderdelen – waaronder appliances waarbij hoge beschikbaarheid cruciaal is – extern belegd. Ook securitydiensten, zoals SOC/SIEM, zijn veelal hybride. Op deze onderwerpen zijn de verantwoordelijkheden al snel verspreid belegd bij meerdere partijen. In het geval van een incident of calamiteit vraagt dit om een integrale afhandeling. Op dit moment is dit aspect vooral belegd bij de inkoop van goederen of diensten en uitgewerkt in standaard verwerkingsovereenkomsten of standaard requirements en gericht op compliance. De doorontwikkeling naar feitelijke informatieveiligheid en doorwerking van het concept 'zero trust' is in de komende jaren een belangrijk gespreksonderwerp met de leveranciers, onder meer op het gebied van IAM. Op dat gebied ligt, aldus de organisatie, ook een belangrijke rol voor de overheid. Immers, veel organisaties doen zaken met veelal dezelfde publieke en private organisaties en er zijn dezelfde dreigingen van toepassing.

3.4.4 Toetsing en verantwoording

De organisatie is in staat een adequaat en goed beeld te geven van de status van informatieveiligheid van de gehele organisatie en het niveau van volwassenheid aan te duiden. De organisatie ziet dat de nodige maatregelen zijn getroffen, maar ziet ondertussen de bedreigingen, cyberrisico's en de attack surface door toenemende digitalisering toenemen. Ook nemen de eisen vanuit wet- en regelgeving (compliance) toe.

Om de toenemende bedreigingen op de groeiende attack surface te ondervangen, benoemt de organisatie dat het scannen van 'de buitenkant' van organisaties op specifieke parameters kan helpen. Een dergelijke taak wordt nu opgepakt door bijvoorbeeld een partij als DIVD[13], maar zou als standaard dienst door de overheid kunnen worden aangeboden. Een dergelijke scan biedt bovendien snel inzicht in een risicoprofiel per organisatie.

Met de huidige governance en inrichting en de aandacht voor risicomanagement komen afwijkingen, zeker op de kroonjuwelen, adequaat 'naar boven'. Belangrijke succesfactoren zijn daarbij de werking van het dualistisch bestuursmodel, de ingerichte Three Lines of Defense en ingebedde risicocultuur. De organisatie steunt daarbij op de gehanteerde frameworks en daarbinnen gehanteerde set aan controls. Ondersteunende softwarepakketten op het gebied van risicomanagement geven daarnaast een actueel inzicht. Compliance op wet- en regelgeving op het gebied van cybersecurity en informatiebeveiliging staat bovendien hoog op agenda van het RvB en de RvC, waarbij in publieke statements hierover nadrukkelijk verantwoording wordt afgelegd.

De toetsing en verantwoording van leveranciers vindt voornamelijk plaats langs de lijn van compliance en het afleggen van verklaringen. Feitelijke informatieveiligheid krijgt daarbij in toenemende mate een belangrijke rol. Wat daarin voor de organisatie, en daarmee ook voor de overheid, helpt is een set afdwingbare controls als dwingende baseline. Zeker in de vitale sector kan je op basis van verplichte wetgeving niets aan het toeval overlaten. Dergelijke eisen verplichten organisaties, en in die lijn dus ook medeoverheden, in het doen van investeringen op het gebied van informatieveiligheid en cybersecurity.

De geïnterviewde stelt dat ook vanuit de duidelijke taken, bevoegdheden en verantwoordelijkheden, geprojecteerd op bijvoorbeeld een gemeentelijke overheid, de eind-verantwoordelijkheid expliciet belegd zou moeten worden bij het college van Burgemeester en Wethouders. Deze verantwoordelijkheid is immers voor de RvB en RvC bij de nieuwe NIS2-richtlijn-organisatie meer dan een paragraaf in het jaarverslag, maar leidt tot administratieve boetes voor de organisatie of mogelijk zelfs tot gevolgen voor het hoger management.

3.5 Organisatie 5

3.5.1 Feitelijke beschrijving

Evenals organisatie 1 is organisatie 5 één van de grootste zorgverzekeraars van Nederland. De zorgverzekeraar kent miljoenen verzekerden en een jaaromzet van miljarden. Er werken op dit moment enkele duizenden voltijds medewerkers. Ook voor deze zorgverzekeraar is het belangrijkste product het uitvoeren van de verplichte basisverzekering tegen ziektekosten, naast onder meer aanvullende ziektekostenverzekeringen. De organisatie is een private organisatie met een publieke taak en heeft geen winstoogmerk.

De organisatie werkt vanuit de aard van de organisatie zowel in de zorgsector als in de financiële dienstverlening. In de zorg(verzekerings)markt speelt de overheid een belangrijke rol en heeft de organisatie derhalve te maken met een breed spectrum aan wet- en regelgeving. Een zorgverzekeraar kent verschillende producten en diensten, die zich bovenal kenmerken door een hoge mate van vertrouwelijkheid en integriteit. De impact van een cyberaanval is als hoog ingeschat vanwege de grote afhankelijkheid van geautomatiseerde informatieverwerking, digitale dienstverlening en toepassingen. Om deze klantgegevens te beschermen, en reputatie-, data- of financiële schade te voorkomen, treft de organisatie veel beheersmaatregelen. Als zorgverzekeraar moet de organisatie bovendien voldoen aan uiteenlopende wet- en regelgeving en staat onder toezicht van DNB. Deze wet- en regelgeving stelt op verschillende (bedrijfsvoerings)aspecten specifieke eisen aan de organisatie.

13 Zie https://www.divd.nl/

De zorgverzekeraar kent een dualistisch bestuursmodel, waarbij er een scheiding is tussen directie en toezichthouders. De RvB bestuurt de rechtspersonen, heeft de dagelijkse leiding over het bedrijf en is onder meer verantwoordelijk voor het beleid en de opzet en werking van de interne risicobeheersings- en controlesystemen. De RvB verantwoordt over de gevoerde strategie en het risicomanagement aan een RvC. Daarbij gaat het onder meer over risico's op het gebied van informatiebeveiliging en cybersecurity. Een RvC houdt daarop toezicht. De RvC laat zich bij de uitoefening van zijn toezicht op het door de RvB gevoerde risicobeleid adviseren door onder meer een risico-commissie.

Naast een RvC en RvB kent de organisatie ook een Ledenraad, om het belang van de verzekerden te waarborgen. De Ledenraad kent een onafhankelijke positie ten opzichte van de RvC en RvB, heeft vastgelegde taken en bevoegdheden en is medebepalend voor de toekomstige koers van de organisatie.

3.5.2 Governance en inrichting

De organisatie vindt een integere bedrijfsvoering belangrijk, hetgeen onder meer betekent dat de organisatie wet- en regelgeving naleeft en een goed risicomanagementsysteem hanteert, verantwoord omgaat met risico's en het vertrouwen van de stakeholders behoudt en vergroot en zorgt voor de realisatie van de strategische doelstellingen. In lijn met deze overtuiging is de organisatie opgezet volgens het Three Lines of Defense-model. Met het inbedden van de juiste check and balances en verplichte functies en functionarissen versterkt de organisatie het risicomanagement en de risicocultuur van de organisatie.

De GRC-functie is georganiseerd als tweede lijn, waaronder de CISO ook ressorteert. De CISO opereert alleen en rapporteert direct aan de verantwoordelijk directeur. De CISO maakt het strategisch informatiebeveiligingsbeleid en maakt op basis daarvan onder meer baselines. In de eerste lijn en vanuit de verantwoordelijkheden binnen die bedrijfsonderdelen is daarnaast een Cyber Security Center met zo'n vijftien medewerkers belast met het ontwikkelen van het beleid (in afstemming met en binnen de kaders en het risicoprofiel vanuit de tweede lijn) en met het implementeren van dit beleid met baselines. Dit team is niet ondergebracht bij één bedrijfsonderdeel maar vanuit de eerste lijn werkzaam binnen de gehele organisatie. Belangrijke afweging daarbij is dat een organisatiemodel met security officers in ieder bedrijfsonderdeel qua juiste capaciteit niet realistisch is. Binnen dit organisatiebrede onderdeel is ook een SOC ingericht op de monitoring van de infrastructuur en incident response. Conform de Three Lines of Defense ziet de derde lijn toe op het gebruik van de baselines.

Als organisatie in een sterk gereguleerde sector dient de organisatie onder meer te voldoen aan DNB good practices. Dit model gaat uit van 'pas toe of leg uit' en wordt op dit moment geïmplementeerd. De zorgverzekeraar gaat voor een zo breed mogelijke toepassing, ondanks dat de gestelde eisen soms lastig zijn en vanuit de verschillende lijnen verschillend worden beoordeeld. Op basis van deze good practices zijn ook KPI's vastgesteld, waarbij aanvullend ook wordt gekeken naar allerhande incidenten, waaronder ook datalekken. Belangrijke reden om naar dit aspect te kijken, was een teruglopend aantal meldingen, waarbij onduidelijk was wat hiervoor de reden was. Was de daling van het aantal meldingen een positieve ontwikkeling of werd er feitelijke informatie uit de organisatie gemist?

De organisatie hanteert een kader met normen en baselines, maar benadrukt dat het moet gaan om de daadwerkelijke veiligheid. Het voldoen aan een normenkader betekent niet dat de feitelijke digitale veiligheid van de organisatie op orde is. Meer bepalend is het individuele gedrag en lerend vermogen van de organisatie. Daarbij is het omgaan met risico's een cruciaal onderwerp. De wijze waarop de organisatie op dit moment omgaat (of om moet gaan) met DNB good practices staat hier dan ook enigszins haaks op. Idealiter werkt de organisatie aan de risico's die de organisatie daadwerkelijk loopt en die moeten worden beheerst. In dat opzicht is de geïnterviewde blij met de komst van DORA, waarmee het (cyber)risicomanagement en de operationele weerbaarheid versterkt moet worden, ook in samenspraak en samenwerking met leveranciers. Cybersecurity in brede zin of digitale weerbaarheid is een onderwerp waarop in de komende jaren fiks geïnvesteerd moet worden.

De zorgverzekeraar heeft verschillende waarborgen en processen georganiseerd om informatie over informatieveiligheid uit de organisatie 'op te halen'. Deze waarborgen zijn georganiseerd rondom de ITIL-processen, waarbij procesmanagers verantwoordelijk zijn. Bij een incident worden problems gedefinieerd, evaluaties gedaan en mogelijk nieuwe risicoinschattingen gemaakt. Daarnaast is security onderdeel van de DevOps-teams, waarbij eventuele risico's worden geïnventariseerd en beheerst. Een product owner is, samen met het eerstelijns cybersecurity team, dan ook zelf verantwoordelijk om bijvoorbeeld een pentest te doen bij de ontwikkeling van een web-applicatie.

Het beleggen van deze verantwoordelijkheid op dit niveau benadrukt wel het belang van gedegen beleid, goede baselines en awareness bij iedere medewerker. De combinatie van awareness aan de voorkant, een slot op de deur middels de processen en het doorlopen van de PDCA-cyclus zijn cruciale succesfactoren.

3.5.3 Risicomanagement

Het risicomanagementsysteem van de organisatie is erop gericht om risico's op zowel operationeel, tactisch als strategisch niveau te identificeren en te beheersen en is een integraal onderdeel van de lijnorganisatie op al deze niveaus. De tweede lijn zorgt voor de kaders bij het uitvoeren van risicoanalyses. In de tactische risicoanalyse wordt vervolgens op basis van de operationele analyse per organisatieonderdeel gekeken naar de (samenhang van de) beheersmaatregelen. De strategische risico's zijn direct gerelateerd aan de bedrijfsdoelstellingen. De eindverantwoordelijk managers en directeuren geven een interne In Control Statement (hierna: ICS) af, waarbij ze verantwoording afleggen aan onder meer de RvB over de effectiviteit van de interne risicobeheersing.

Om de strategische doelstellingen van de organisatie te behalen, worden logischerwijs activiteiten ontplooid waaraan inherent risico's gekoppeld zijn. De mate waarin echter risico's worden genomen bij de operatie is afhankelijk van de risicobereidheid. Op het gebied van cybersecurity is de risicobereidheid laag, onder meer omdat de organisatie te maken heeft met gerichte en ongerichte cyberaanvallen waaruit schade kan ontstaan. Als de risicobereidheid wordt overschreven wordt gesproken over een 'risicobereidheidsoverschrijding' en worden aanvullende beheersmaatregelen getroffen.

De tweede lijn maakt een kwartaalrapportage van de risico's, zoals ze werkelijk zijn waargenomen op basis van Key Risk Indicators en rapporteert aan het verantwoordelijk lid van de RvB. Gedurende het kwartaal wordt hierover wekelijks overlegd met de CISO. In deze rapportage staan, naast andersoortige risico's, onderwerpen als (i) kwetsbaarheden op internet facing applicaties, (ii) zogenaamde 'prio 1 incidenten', (iii) de tijdigheid van het toepassen van kritieke patches, (iv) het percentage medewerkers dat het awareness programma heeft gevolgd en (v) de top 10 van cyberrisico's. Een kleine afwijking zorgt dat een indicator op 'rood' komt en het risico op het allerhoogste niveau wordt besproken.

In een complexe sector ben je onlosmakelijk met elkaar, publieke netwerken en leveranciers verbonden. Dit zorgt voor ketenafhankelijkheden en brengt risico's met zich mee. Een onderwerp als 'privileged accountmanagement' is bij dergelijke afhankelijkheden een uitdaging. Immers, beheerders werken voor meerdere klanten en zij moeten wel hun werk kunnen blijven doen. Hierbij dient de juiste balans te worden gevonden tussen informatiebeveiliging versus werkbaarheid. Ook de wijze waarop leveranciers verschillend omgaan met problemen staat soms in contrast met (de aantoonbaarheid van) het beleid. Dergelijke gesprekken worden tot op het allerhoogste niveau gevoerd met leveranciers. In uitzonderlijke gevallen kan een factuur later betaald worden of kan zelfs afscheid worden genomen van leveranciers. Leveranciers laten het echter zelden zo ver komen.

3.5.4 Toetsing en verantwoording

Doordat de sector sterk gereguleerd is en de interne beheersing op orde is, stelt de organisatie een goed inzicht te hebben in de volwassenheid van de eigen organisatie. De organisatie vervult daarbij ook een voorbeeldfunctie naar bijvoorbeeld ziekenhuizen en stellen ook eisen aan die organisaties. Compliance (bijvoorbeeld als in het halen van 'vinkjes') of daadwerkelijke veiligheid (bijvoorbeeld op basis van onafhankelijke tests) is daarbij een terugkerend thema. De wijze waarop naar specifieke controls wordt gekeken verschilt daarbij soms per eerste, tweede of derde lijn.

Belangrijke aanjager voor het verbeteren van de cybersecurity posture is de toezichthouder DNB die verschillende instrumenten kan inzetten, zoals een aanwijzing, om de organisatie aan de gestelde eisen te laten voldoen. De focus ligt vooralsnog op individuele toetsing binnen de organisatie of op de externe toetsing van een organisatie. Het doel zou meer gericht moeten zijn op het veiliger of tenminste meer risicobewuster maken van het gehele stelsel of de gehele keten. De opgave is dan ook niet zozeer meer toetsing of verantwoording, maar meer in dialoog te gaan met elkaar om de reële (in plaats van 'theoretische') risico's, te faciliteren en concrete handvatten te bieden. De good practices van DNB bieden hiervoor goede voorbeelden, hoewel die ook weer absoluut zijn.

HOOFDSTUK 4

Conclusies en aanbevelingen

In dit hoofdstuk combineren we de feitelijke bevindingen met de opgedane inzichten uit de verschillende gesprekken met de organisaties uit de verschillende sectoren. We beschrijven allereerst de conclusies uit de gesprekken met de organisaties (§ 4.1) en ‘vertalen’ dit vervolgens naar welke lessen BZK kan trekken in de wijze waarop bij grote organisaties sturing wordt gegeven aan informatieveiligheid, met welke aspecten de (rijks)overheid de digitale veiligheid en weerbaarheid kan versterken en BZK zijn stelselverantwoordelijkheid kan inrichten (§ 4.2).

We beantwoorden de hoofdvraag **'Welke lessen kan BZK trekken in de wijze waarop bij grote organisaties sturing wordt gegeven aan informatieveiligheid?'** langs de onderwerpen governance en inrichting, risicomanagement en toetsing en verantwoording.

4.1 Conclusies

4.1.1 Governance en inrichting

Op basis van de interviews en aanvullende documentstudie stellen we onder 'governance en inrichting' verschillende rode draden vast die te clusteren zijn rondom de onderwerpen 'interne governance en inrichting', 'externe governance' en 'randvoorwaarden'.

Interne governance en inrichting

Eén van de belangrijkste aspecten van een organisatie die goed wordt bestuurd en 'in control' is, is het dualistische bestuursmodel met een raad van bestuur en raad van commissarissen. Deze verdeling zorgt voor een heldere interne structuur, waardoor er duidelijke afbakeningen zijn in taken, bevoegdheden en verantwoordelijkheden op het gebied van uitvoering en toezicht. Een dergelijke structuur heeft als voordeel dat de RvB betrokken is bij de dagelijkse gang van zaken en de RvC als apart orgaan met eigen verantwoordelijkheden toezicht houdt op het bestuur. RvB en RvC vinden zonder uitzondering cybersecurity, als strategisch risico voor de continuïteit van de organisatie, belangrijk en cruciaal voor het voortbestaan van de organisatie. Ze hebben een voorbeeldfunctie en dragen dit daadwerkelijk uit. Dit heeft effectieve doorwerking in de mate waarin de rest van de organisatie omgaat met security.

Naast het dualistisch bestuursmodel wordt binnen iedere organisatie expliciet onderscheid gemaakt in de Three Lines of Defense. Hoewel er nuances zijn in de wijze waarop de Three Lines of Defense is ingericht en wordt gehanteerd, is er telkens een centrale 'tweedelijns' informatiebeveiligingsfunctie ingericht, veelal binnen een generieke risicomanagementfunctie ofwel enterprise risk management. De eerste lijn (ofwel de business) draagt, binnen de door de top van de organisatie gestelde (strategische) risicobereidheid, de verantwoordelijkheid om risico's te beheersen. De tweedelijnsfunctie is verantwoordelijk voor kaders, beleid en de doorvertaling naar (meer) operationele procedures en processen. Deze tweede lijn ziet toe op naleving van dit beleid bij de eerste lijn.

De nuances op dit punt zitten onder meer in het feit dat sommige organisaties bepaalde 'ondersteuning' hebben ingericht binnen de eerste lijn (bijvoorbeeld organisatie 5), zodat de business de verantwoordelijkheid voor het eigenaarschap kan nemen. Dergelijke ondersteuning bestaat onder meer uit kennis, expertise en capaciteit in mens en (financiële) middelen.

Ter ondersteuning van de uitvoering van de tweedelijnsfunctie, gekoppeld aan het dualistisch bestuursmodel en gericht op organisatiebreed enterprise risk management, is bij iedere organisatie een centraal security risico framework ingericht. Afhankelijk van de organisatie is dat framework onderdeel van een breder raamwerk of bestaat het naast andere raamwerken. Hierbij zijn de te behalen bedrijfsdoelstellingen van strategie tot uitvoering uitgelijnd met de te nemen risico's. Een dergelijk security risk framework omvat een verplichte set controls vanwaar door zowel de eerste als de tweede lijn gestuurd kan worden op informatieveiligheid. Een (al dan niet verplichte) combinatie van frameworks zorgt bovendien voor een juiste mix van controls, waarbij bijvoorbeeld ook technische of sectorspecifieke eisen zijn opgenomen. Zicht en grip op strategische risico's en de operationele uit- en doorwerking resulteert in passende beheersmaatregelen. Aan deze controls zijn vervolgens meetbare KPI's, zoals de mate waarin autorisaties kloppen of hoeveel incidenten of securitymeldingen er zijn, gekoppeld, zodat er te allen tijde inzicht is en er gelegenheid is tot (bij)sturen voor de eerste en tweede lijn. Het sturen op percentages en meetbare KPI's brengt daarentegen wel het risico met zich mee dat dit wordt gehanteerd als een 'afvinklijst', waardoor het middel kan verworden tot een doel op zich.

De organisaties maken onderscheid in compliance en daadwerkelijke informatieveiligheid of cybersecurity. Het adagium is daarbij dat hoewel compliance aan wet- en regelgeving belangrijk is het achterliggend doel, daadwerkelijke informatieveiligheid, nog belangrijker is. Er kunnen derhalve risico's zijn op aspecten van compliance (zoals het niet voldoen aan een eis) én risico's betreffende de daadwerkelijke informatieveiligheid (zoals een kwetsbaarheid). Deze 'duale' denkwijze heeft doorwerking in de wijze waarop wordt omgegaan met risico's in relatie tot de strategische risk appetite en welke maatregelen derhalve genomen (moeten) worden of welke inspanningen of activiteiten worden ontplooid. De organisaties gebruiken compliance, hoewel vanuit strategisch risicomanagement belangrijk, als middel om daadwerkelijke informatieveiligheid te realiseren; oftewel compliance draagt bij aan de feitelijke informatieveiligheid, zo blijkt uit de interviews.

Externe governance

Een adequate interne governance en inrichting is met name gericht op het behalen van de strategische doelstellingen van een organisatie. Dergelijke bedrijfsdoelstellingen zijn veelal financieel gedreven, al dan niet door de aandeelhouders. Een ander belangrijk aspect is echter een sterke externe motivatie vanuit het toezicht ofwel externe governance vanwege de in enkele gevallen vitale functie die de organisaties hebben in Nederland.

Een sterk gereguleerde sector, zoals de financiële sector of de zorgsector, met eisen van en toezicht door bijvoorbeeld DNB zorgt voor een stevige verankering van risicomanagement (in brede zin) binnen de organisaties en daardoor ook op het gebied van informatieveiligheid. Eigenaarschap van de risico's is belegd 'waar het hoort'. Dit ziet niet alleen toe op 'opzet' en 'bestaan', maar ook in toenemende mate op de 'werking'. Een dergelijke sterke (toezichts)rol, met het stellen van eisen, inclusief de werking, zorgt voor strategische agendering op het hoogste niveau binnen een organisatie en werkt door in de gehele operatie. Zie ook § 4.1.3.

Randvoorwaarden

Een ander belangrijk aspect is dat door de omvang van de verschillende organisaties ze in staat zijn nadrukkelijk taken, bevoegdheden en verantwoordelijkheden te kunnen scheiden. Ze hebben simpelweg de capaciteit in mens en middelen om de juiste investeringen te doen en activiteiten te ontplooien om volwassen en adequate informatiebeveiliging(sorganisatie) in te richten.

De organisaties uit dit onderzoek hebben daarnaast vanuit verschillende perspectieven een langere historie op het gebied van compliance. Zo dient de financiële sector zich al lange tijd aan verschillende (internationale) wet- en regelgeving te houden en is van oudsher in de zorgsector aandacht voor verschillende 'vormen' van veiligheid. Aandacht voor privacy van (medische) gegevens en aanpalend informatiebeveiliging is met de komst van de AVG versterkt. Deze historie zorgt voor een zeker fundament aan 'risicocultuur', waarop ontwikkelingen op het gebied van informatiebeveiliging en cybersecurity kunnen voortbouwen. Een sterke risicocultuur is randvoorwaardelijk en een succesfactor voor 'centraal sturen en coördineren' en 'decentraal - in de haarvaten van een organisatie - uitvoeren'.

Autonomie en verantwoordelijkheid beleggen 'waar het hoort' staat bij alle organisaties centraal. De interne governance vanuit de Three Lines of Defense biedt daarbij een organisatorisch kapstok. Een ondersteunend aspect hierin is een duidelijke procesmatige inrichting en werkende 'ITIL-processen', zoals changemanagement, waarbij centraal kaders en eisen worden gesteld en in de business tot uitvoering kan worden gebracht. De strategische risicobereidheid, toepassing op informatieveiligheid en doorwerking in de uitvoering is daarmee volledig uitgelijnd. Een tweede lijn kan dan toezien op naleving al dan niet met sancties of escalaties naar hogere gremia. Daarbij is een goede informatievoorziening in het geval er afwijkingen zijn vanuit de haarvaten van de organisatie naar de RvB en RvC cruciaal. De tweede lijn vervult hierin een belangrijke signalerende en coördinerende rol.

4.1.2 Risicomanagement

De (interne) governance van de organisaties is gestructureerd langs de lijnen van organisatiebreed risicomanagement. Voor iedere (commerciële) organisatie zijn continuïteit, financiële baten en behoud van imago in meer of mindere mate de belangrijkste motieven. Dreigingen of risico's op deze aspecten dienen dan ook vroegtijdig geïdentificeerd en beheerst te worden. Risicomanagement vormt daarmee de kern van de organisaties. De organisaties hebben - organisatiebreed - strategisch tot operationeel risicomanagement 'werkend', waarbij cybersecurity of informatieveiligheid veelal wordt gezien als strategisch risico voor de continuïteit van de organisatie. De organisaties dragen dan ook voortdurend uit dat informatieveiligheid onderdeel is van de strategische afwegingen en keuzes van de organisatie.

Organisatiebreed (strategisch) risicomanagement vormt de kern van risicomanagement. Op strategisch niveau worden dreigingen en risico's in beeld gebracht en bepaald op welke wijze een organisatie daarmee om wenst te gaan. Hierbij wordt onderscheid gemaakt in strategisch, tactische en operationele risico's, waarbij vanuit de generieke risicomanagementfunctie voornamelijk wordt gekeken naar strategische risico's (vanuit GRC). De focus bij de 'informatiebeveiligingsfunctie of -organisatie' ligt met name op de tactisch operationele risico's. Keuze hoe wordt omgegaan met specifieke (strategische) risico's worden vastgelegd in de risicobereidheid van de organisatie. Verschillende type risico's kunnen daarbij verschillende 'risk appetites' hebben. Voor informatieveiligheid - als één van die risico' - geldt dat organisaties zonder uitzondering risicomijdend zijn.

Deze strategische keuzes hebben doorwerking in de wijze waarop de gehele organisatie met informatiebeveiligingsrisico's omgaat. Dit geldt ook in de wijze waarop met leveranciers wordt omgegaan. Organisaties hebben immers maar tot op zekere hoogte 'grip' op de wijze waarop leveranciers of partners omgaan met informatie. Met name deze koppelvlakken met andere organisaties (of ketenafhankelijkheden) vormen in toenemende mate een uitdaging voor de organisaties. Organisaties zetten actief in op supplier information and risk management. Het bewustzijn van deze ketenafhankelijkheid en leveranciers draagt bij aan inzicht in risico's. Het adagium 'controle op' gaat daarbij boven 'vertrouwen in', waarbij de organisaties het uitgangspunt van het streven naar feitelijke informatieveiligheid hanteren. Organisaties richten zich bovendien meer op informatieveiligheid in het stelsel als geheel, onder meer door intensievere samenwerkingen.

Externe dreigingsinformatie blijft tot slot cruciaal en wordt soms zelf actief in kaart gebracht en gedeeld in samenwerking met andere (vergelijkbare) organisaties of sectoren onder meer via ISAC's of CERTS.

4.1.3 Toetsing en verantwoording

Controle en toetsing

Zoals eerder benoemd, speelt een dualistisch bestuursmodel gecombineerd met een goede inrichting van de Three Lines of Defense een belangrijke rol bij de onderzochte organisaties om grip te hebben op informatieveiligheid. Hieruit volgt dat een zekere mate van controle en toetsing 'tussen de lijnen' belangrijk is. Dergelijke controle en het toezicht vindt getrapt plaats. Deze gelaagdheid is van belang, omdat de focus van elke lijn net anders is. Het geheel zorgt daarmee voor een sterke beheersing van informatieveiligheid. De controle kent de volgende elementen:

- De tweede lijn controleert of de eerste lijn binnen de gestelde kaders werkt. Met andere woorden: worden de afspraken binnen de organisatie nageleefd? Een dergelijke controle gebeurt naast het faciliteren en adviseren.
- De derde lijn kijkt naar het samenspel van de eerste en tweede lijn en beoordeelt of dit samenspel inhoudelijke en procesmatig goed verloopt.
- De 'vierde lijn', de externe toezichthouder, toetst vervolgens het geheel.

Bij een adequaat samenspel wordt door de organisaties de controle van tweede en derde lijn vooral gezien als een hulpmiddel om de organisatie als geheel scherp te houden en de verbeteringen door te voeren die het geheel nog sterker maken. De externe toezichthouder doet vervolgens een formele toetsing. Alleen al de 'dreiging' van externe toetsing is een belangrijke aanjager voor verbeteringen. Zeker in de financiële sector, waar DNB als een sterke externe toezichthouder aanwezig is en door middel van de *Good Practice Informatiebeveiliging* beheersingsmaatregelen beschrijft om informatiebeveiliging te borgen, wordt gestreefd naar het volledig voldoen aan de eisen van de externe toezichthouder. Dit is niet alleen vanwege de eisen die gesteld worden, maar ook vanwege het feit dat in de ogen van de toezichthouder het onvoldoende beheersen van risico's betekent dat er sancties worden opgelegd door DNB.

Interne verantwoording

Buiten de eventuele verantwoording aan een externe toezichthouder, is verantwoording intern een essentieel onderdeel van het geheel. In een volwassen organisatie is verantwoording een continu proces, gekoppeld aan risicomanagement en periodieke managementrapportages. Op elk willekeurig moment is een organisatie in staat om te laten zien hoe de organisatie ervoor staat op het gebied van in control zijn, waar de grootste risico's liggen op compliance én daadwerkelijke informatieveiligheid en hoe hiermee wordt omgegaan. Het management kent zijn verantwoordelijkheden en is aanspreekbaar op afwijkingen van het beleid en geconstateerde risico's. Ook worden duidelijke afspraken gemaakt voor verbeteringen en hierop wordt gestuurd.

Testen en weerbaarheid

Waar toetsing vaak meer gericht is op compliance, is testen gericht op feitelijke informatieveiligheid. Voor het in control hebben van informatieveiligheid wordt testen dan ook als noodzakelijk gezien. Ondanks dat beheersmaatregelen op orde kunnen zijn, geeft het testen van organisaties inzicht in waar de benodigde digitale weerbaarheid vergroot moet worden. In een wereld waarin dreigingen continu veranderen en snel toenemen, onder meer door wijzigingen in aanvalsmethoden, is testen onontbeerlijk om zicht te hebben op de mate waarin men weerbaar is tegen die dreigingen. Het programma TIBER-NL is hier een prachtig voorbeeld van. In deze Threat Intelligence Based Ethical Red-Teaming wordt de weerbaarheid van financiële instellingen tegen geavanceerde cyberaanvallen getest, gebaseerd op realistische dreigingen.

4.1.4 Cultuur

Voor alle genoemde aspecten is een functionele risico- of veiligheidscultuur randvoorwaardelijk. In een cultuur waarin (informatie)veiligheid gezien wordt als de verantwoordelijkheid van iedere medewerker is het gemakkelijker om organisatiebreed te sturen op risico's. Die cultuur moet in alle lagen van de organisatie aanwezig zijn. Hierbij geldt in elk geval dat het uitdragen van het belang door het hoogste management bijdraagt aan de wijze waarop individuele medewerkers hiermee vervolgens omgaan. Wanneer er een risico- of veiligheidscultuur aanwezig is binnen de organisatie is het vaak gemakkelijker om wijzigingen vanwege informatieveiligheid door te voeren, zeker wanneer deze invloed hebben op de gebruiksvriendelijkheid of toegankelijkheid van systemen.

4.2 Aanbevelingen

Voornoemde (praktische) inzichten en conclusies hebben we afgezet tegen de achtergrond van de focus van BZK op het verhogen van informatieveiligheid bij overheden en de ambities om de informatieveiligheid op orde te brengen en te houden. Dit vanuit de stelselverantwoordelijkheid voor informatieveiligheid bij de rijkoverheid, provincies, gemeenten en waterschappen. Daarbij wordt ook gestreefd naar uniformiteit binnen en naar optimale afstemming tussen de overheidslagen.

Daar waar mogelijk wordt bij de aanbevelingen een dergelijke verbetermogelijkheid voor BZK in meer algemene zin of specifiek ten aanzien van de BIO expliciet benoemd.

4.2.1 Algemeen

Overheidsorganisaties zijn zelf verantwoordelijk voor de wijze waarop het informatieveiligheidsbeleid in hun organisatie gestalte krijgt. BZK treedt hierbij kaderstellend, ondersteunend, en waar nodig aanjagend op naar alle overheidslagen. Het is noodzakelijk de ambities op informatieveiligheidsgebied te verwezenlijken, mede in de context van de vormgeving van de digitale transitie in Nederland. De evaluatie van de BIO biedt, mede door de herziening van de ISO 27002, de gelegenheid om binnen een BIO 2.0 op onderwerpen verbeteringen door te voeren of aanvullingen te doen of in de bredere context van dit instrument de aanbevelingen door te voeren.

Aanbeveling: Versterk de rol van BZK om juiste en eenduidige kaders te stellen. Zorg voor voldoende capaciteit en middelen bij BZK om deze uitvoering aan te jagen en te coördineren en de overheidslagen hierbij te (laten) ondersteunen. Blijf bovenal de overheidslagen aansporen de ambities in de gestelde kaders te realiseren.

Aanbeveling: Continueer de rol van BZK in het actief normeren en het bepalen van die ambities. Hanteer hiervoor de BIO, zorg voor een wettelijke grondslag in de WDO en draag op deze wijze bij aan het behalen van de doelen voor de digitale transitie.

4.2.2 Governance en inrichting

Dualistisch bestuursmodel

Een dualistisch bestuursmodel draagt bij aan een versterking van informatieveiligheid door een scheiding van uitvoering en controle en toezicht en zorgt hiermee voor checks and balances op het allerhoogste niveau. Dit is van groot belang voor zowel de compliance als daadwerkelijke informatieveiligheid. Een dualistisch model is voor de overheid een bekend model en wordt reeds toegepast. Bij veel publieke organisaties is een scheiding tussen de gekozen volksvertegenwoordiging en het bestuur. Een dergelijk model biedt dan ook mogelijkheden voor de verbetering van de inrichting van individuele overheidsorganisaties. Dit geldt echter in algemene zin, want er is niet sprake van één overheid met één volksvertegenwoordiging. Er zijn immers centrale en decentrale overheden met ieder hun eigen volksvertegenwoordiging. De autonomie van bijvoorbeeld de gemeenten maakt dat op rijksniveau slechts beperkt invloed is op de lagere overheid.

Aanbeveling: Onderzoek voor overheidsorganisaties die een dergelijk model niet kennen, zoals agentschappen, of de eigenaar van het ministerie waarvan het agentschap onderdeel is voldoende in staat is om toezicht te houden op het beleid van het agentschap. Bezie daarbij of het sturingsmodel afdoende werkt en of aanvullende voorschriften, structuren of waarborgen (zoals bij de onderzochte organisaties) noodzakelijk zijn.

Aanbeveling: Onderzoek voor zbo's of sturing en toezicht door de minister afdoende is op het aspect van informatieveiligheid en of aanvullende voorschriften, structuren of waarborgen noodzakelijk zijn. Bezie daarbij of het sturingsmodel afdoende werkt en of aanvullende voorschriften, structuren of waarborgen noodzakelijk zijn.

De verschillende lagen binnen het openbaar bestuur hebben ieder een eigen dualistisch model. Dit betekent dat sturing vanuit een stelselverantwoordelijkheid (overheidsbreed) op dit punt lastig is vanwege de afhankelijkheid van de bereidheid van het lokale bestuur om hieraan mee te werken. Realistisch gezien is de invloed van de coördinerende - en verticale interbestuurlijke sturingsrol van BZK beperkt.

Aanbeveling: Continueer de kaderstellende, ondersteunende en aansporende rol van BZK om (de werking van) controle en toezicht bij de overheidslagen te blijven versterken.

Om de werking van dit dualistisch bestuursmodel binnen overheidsorganisaties te versterken voor informatiebeveiliging, is het van belang dat het toezicht - in casu de volksvertegenwoordiging - voldoende geëquipeerd is om de toezichtrol goed in te vullen.

Aanbeveling: Zorg voor een basisopleiding voor iedere volksvertegenwoordiger binnen alle lagen van het openbaar bestuur op het gebied van informatieveiligheid en risicomanagement. Dit kan bijdragen aan een (kwalitatieve) versterking van de horizontale sturing op informatieveiligheid vanuit de gedachte van het dualistisch bestuursmodel. Het belang van informatieveiligheid kan hierbij nadrukkelijk worden gestimuleerd, waardoor we verwachten dat hiervan enige doorwerking naar de organisaties zal plaatsvinden, doordat de juiste vragen worden gesteld.

Three Lines of Defense met een sterke vierde lijn

De waarde van het Three Lines of Defense-model wordt breed gedeeld. Ook binnen de overheid is dit een bekend model.

Aanbeveling: Draag nadrukkelijk het nut en de noodzaak van het Three Lines of Defense-model uit. Richt de inspanningen hierbij op expliciete implementatie bij onder meer medeoverheden als kwalitatieve versterking van de interne governance. Dit zal dan ook bijdragen aan de (beleids)doelen van BZK. Verantwoording wordt hiermee een continu proces, gekoppeld aan risicomanagement en periodieke managementrapportages. Een organisatie is dan op ieder moment in staat om te laten zien hoe ze ervoor staat op het gebied van in control zijn, waar de grootste risico's liggen op het gebied van compliance én de daadwerkelijke informatieveiligheid, en hoe hiermee wordt omgegaan. Het management kent zijn verantwoordelijkheden en is aanspreekbaar op afwijkingen van het beleid en de geconstateerde risico's.

Aanbeveling: Vervul hierin in elk geval de rol van aanjager en laat medeoverheden ondersteunen met best practices. Verken de mogelijkheid om vertegenwoordigende organisaties als de VNG zichzelf dergelijke organisatieprincipes op te laten leggen ('verplichtende zelfregulering'), vergelijkbaar met de huidige BIO. Een ander alternatief zou zijn om rule-based een voorschrift op te nemen in de BIO, waarbij bijvoorbeeld de doelstelling van hoofdstuk 5 wordt uitgebreid met de vereisten om 'de informatiebeveiligingsfunctie in overeenstemming te laten zijn met organisatiebreed risicomanagement en inrichtingsprincipes' en daarbij verwijzen naar een best practice. Hierbij kan dan tevens een link worden gelegd met control 18.2.2.1 in hoofdstuk 18 'Naleving', waarbij de informatiebeveiligingsfunctie nadrukkelijker wordt ingebed in de governance van de organisaties.

Aanbeveling: Versterk binnen de overheid de 'vierde lijn' als externe toezichthouder gericht op horizontaal toezicht. Bij de rijksoverheid zit de vierde lijn vooral bij de Algemene Rekenkamer[14]. Bij de lokale overheid dienen lokale Rekenkamers dan een dergelijke rol te vervullen. We adviseren op dit aspect ook een aanjagende rol van BZK om hierin enige uniformiteit en een kwalitatieve verbetering te bewerkstelligen. Voor deze toezichthouders geldt in meer of mindere mate dat op dit moment (i) niet gewerkt wordt met een duidelijk kader, zoals DNB met de Good Practice Informatiebeveiliging doet, (ii) er geen handhavingsmodel aanwezig is en (iii) informatiebeveiliging onderbelicht is in het geheel aan onderwerpen waar zij toezicht op houden.

Aanbeveling: Zorg voor een basisopleiding voor externe toezichthouders binnen alle lagen van het openbaar bestuur op het gebied van informatieveiligheid en risicomanagement. Dit kan bijdragen aan een (kwalitatieve) versterking van het toezicht op informatieveiligheid vanuit de gedachte van de Three Lines of Defense.

Daarnaast zijn er stelselhouders, zoals DigiD en SUWI, die ook een vorm van vierdelijns controle doen. De hoeveelheid stelsels die alle hun eigen regels stellen, dragen echter niet bij aan een eenduidig sterk vierdelijns toezicht, zowel in de kaders die gesteld worden, als in de wijze waarop gehandhaafd wordt. Zo zien we bij DigiD een strenge handhaving, waarbij uiteindelijk afsluiting als consequentie geldt bij het niet voldoen. Bij andere stelsels wordt daarentegen weer nauwelijks gehandhaafd.

14 De Audit Dienst Rijk scharen we onder de derde lijn voor de Rijksoverheid als interne auditdienst voor alle departementen.

Aanbeveling: Versterk het vierdelijns toezicht op informatiebeveiliging en standaardiseer bovenal langs de lijn van uniforme kwaliteit. Onderzoeken van lokale rekenkamers[15] gericht op de informatieveiligheid tonen aan dat een dergelijke 'vierde lijn' daadwerkelijk tot verbeteringen kan leiden.
Een dergelijke versterking en standaardisatie dient plaats te vinden middels het vergroten van de juiste kennis bij deze toezichthouders, alsook door het zich meer eenduidig te richten op normen waarop het horizontaal en verticaal toezicht plaatsvindt. De BIO zou hierbij als het (enige) fundament moeten gelden, waarbij slechts bij expliciete risico's vanuit andere stelsels aanvullende overheidsmaatregelen mogen worden genomen. Vanuit die gedachte onderschrijven we dan ook de voorgenomen wettelijke verankering van de BIO in de Wet Digitale Overheid. We verwachten dat dit zal bijdragen aan een eenduidiger toezicht vanuit de diverse stelsels door meer uniformiteit van regels.

Aanbeveling: Zorg in deze context en voor een sluitend stelsel voor meer eenduidigheid in de handhaving ('sanctiebeleid') waar mogelijk. Een verkenning naar het huidige sanctiebeleid en de toepassing daarvan binnen verschillende stelsels kan hierbij inzicht verschaffen in wat het meest passend is en 'wat werkt'.

4.2.3 Risicomanagement

Voor een betere inbedding van (strategisch) risicomanagement op het gebied van informatiebeveiliging is het van belang dat dit binnen organisaties goed ingericht is. Binnen het openbaar bestuur vindt risicomanagement ook op strategisch niveau plaats binnen de individuele organisaties. In hoeverre een organisatie in staat is hieraan adequaat invulling te geven, hangt van vele factoren af. Een belangrijk aspect is de omvang van de organisatie, met bijhorende capaciteiten en middelen. Tegelijkertijd is er ongeacht de omvang binnen een organisatie altijd veel informatie in omloop. De rijksoverheid geeft een grote variëteit aan sturingslijnen aan andere overheidslagen op een breed palet aan onderwerpen, zoals financieel.

Een verondersteld, integrale strategische risico framework, waarbinnen een bestuursorgaan moet opereren, is daarmee groot en zeer divers en daardoor complex en weerbarstig. Dit wordt ook versterkt door het ontbreken van een duidelijke sturingslijn vanuit het kabinet, door het grote palet aan onderwerpen en initiatieven dat richting overheidsorganisaties gaat.

Ook hierin ontbreekt het aan een duidelijke integrale strategische sturing en (complementaire) samenhang binnen organisaties en in het stelsel. In dit complexe verband moet elke overheidsorganisatie bovendien zelf bepalen welke (strategische) risk appetite men hanteert. Dat is op z'n minst beperkend in het kader van beoogde eenduidigheid en professionaliteit, aangezien het vaak om dezelfde (soort) informatie gaat die beschermd wordt en de burger daarin meer eenduidigheid mag verwachten van 'de overheid'.
Een eenduidige doorvertaling in KPI's, mede in relatie tot horizontale of zelfs verticale sturing, kan hierdoor onvoldoende worden vormgegeven.

Aanbeveling: Hanteer een bestaand (of te ontwikkelen) risicomanagementfunctie (in de context van een dualistisch bestuursmodel en de Three Lines of Defense) om de ambities op het vlak van informatieveiligheid daadwerkelijk te verwezenlijken. Draag dit nadrukkelijk uit. Vanuit de financiële stromen is risicomanagement reeds veel meer ingebed. De Comptabiliteitswet[16] vormt hierin een belangrijke (wettelijke) basis. Door informatiebeveiliging hier nadrukkelijk aan te koppelen, kan strategisch risicomanagement versterkt worden. Onderzoek op welke wijze hier een nadrukkelijkere verbinding gemaakt kan worden met informatiebeveiliging en maak daarbij gebruik van de ervaringen die de afgelopen jaren hiermee opgedaan zijn.

Aanbeveling: Verken of 'de implementatie van organisatie-breed strategisch risicomanagement' - in lijn met de aanbevelingen op het vlak van de Three Lines of Defense - mogelijk kunnen worden opgepakt door de medeoverheden door middel van bijvoorbeeld 'verplichtende zelfregulering' of een voorschrift op te nemen in de BIO (zie ook § 4.2.1). Het uitdragen van toepassingen van 'strategisch risicomanagement' in de vorm van best practices kan hierbij inspireren en stimuleren. Dergelijke best practices laten zien hoe organisaties een security risk framework met een verplichte set controls hebben, waardoor zowel de eerste als de tweede lijn kunnen sturen op informatieveiligheid. Een (al dan niet verplichte) combinatie van frameworks zorgt daarbij voor een juiste mix van controls, waarbij bijvoorbeeld ook technische of sectorspecifieke eisen zijn opgenomen.

15 Bijvoorbeeld gemeente Rotterdam (https://rekenkamer.rotterdam.nl/onderzoeken/in-onveilige-handen/) of gemeente Eindhoven (https://www.nvrr.nl/wp-content/uploads/2021/12/Rekenkamerrapport-Informatieveiligheid-smartsafe.pdf)

16 Zie https://wetten.overheid.nl/BWBR0039429/2022-08-01

Aanbeveling: Maak bovenal veel meer gebruik van het instrument communicatie vanuit BZK. Daar waar invloed op strategische, verticale, sturing vanuit het kabinet zeer beperkt is, is de invloed op de eigen communicatie ontzettend groot. Door meer aandacht te geven aan de verwachtingen die overheidsbreed gesteld worden op het gebied van informatieveiligheid kan meer invulling gegeven worden aan de delta die er nu is op het gebied van strategisch - organisatiebreed - risicomanagement. De versterking van tactisch/operationeel risicomanagement op het gebied van informatiebeveiliging zal veelal binnen de individuele organisaties moeten plaatsvinden. Vanuit de stelselverantwoordelijkheid van BZK kan hierbij vooral gedacht worden aan de verwachtingen richting medeoverheden op dit gebied te expliciteren en meer duiding te geven, bijvoorbeeld in de vorm van handreikingen, over hoe dit vorm gegeven kan worden.

Aanbeveling: Blijf actief communiceren over de goede initiatieven op het gebied van leveranciersmanagement en inkoop, zoals de ICO-Wizard. Draag de nut en noodzaak hiervan uit, al dan niet via vertegenwoordigende organisaties. Het belang van dergelijke activiteiten is groot. Op dit gebied zien we vooral mogelijkheden om actiever in te zetten op het toetsen én testen van leveranciers op compliance en feitelijke informatieveiligheid. We zien dat dit nu vaak niet verder gaat dan het verifiëren van een ISO 27001-certificering ('administratieve informatieveiligheid'). De gesproken commerciële organisaties zijn veel actiever op het toetsen van de feitelijke informatieveiligheid, bijvoorbeeld door middel van commerciële tools die hiervoor ingezet kunnen worden. Grijp deze mogelijke verbeteringen aan door het bundelen van de krachten op dit gebied en bovenal de kennis omtrent leveranciers actief te delen. Zo kunnen de kleinere organisaties hier ook invulling aan geven, kan efficiënt gebruik worden gemaakt van overheidsmiddelen en worden leveranciers ontlast doordat zij minder vaak hoeven aan te tonen te voldoen aan de gestelde eisen.

4.2.4 Toetsing en verantwoording

De interne governance en inrichting van de organisaties met een dualistisch bestuursmodel en Three Lines of Defense is onlosmakelijk gekoppeld aan controle en toetsing, interne verantwoording en daadwerkelijk testen. Deze aspecten van toetsing en verantwoording worden aangejaagd door, of zijn eisen van, een vorm van externe governance. De in- en externe governance zijn dan ook niet los van elkaar te zien en dienen als één mechanisme te worden bezien. We zien dat binnen de overheid de elementen op zichzelf in 'opzet' (deels) bestaan, maar nog onvoldoende in de praktijk en in samenhang werken.

Aanbeveling: Neem de aanbevelingen ter hand en vervolmaak het stelsel met onder meer de 'vierdelijns' controle, waarin (in- en externe) toetsing en verantwoording worden meegenomen. Belangrijk aandachtspunt daarbij is dat er gekeken wordt naar de feitelijke informatieveiligheid, om te voorkomen dat het 'slechts' een compliance-gedreven verandering betreft en bestaande kritiek op 'afvinklijstjes' versterkt wordt.

Aanbeveling: Zet in toenemende mate in op daadwerkelijk testen en daarover organisaties te (laten) verantwoorden. TIBER kan hiervoor als voorbeeld dienen. Op deze wijze gaat het toetsen en verantwoorden niet slechts over 'administratieve informatieveiligheid', maar om de feitelijke informatieveiligheid.

4.2.5 Cultuur

Voor alle bovengenoemde aspecten geldt dat die slechts bijdragen aan informatieveiligheid mits er een functionele veiligheids- of risicocultuur is. Een functionele en gezonde risicocultuur is daarbij een randvoorwaarde (voor een volwassen en weerbare organisatie op informatieveiligheid), een gevolg (van het zetten van stappen in volwassenheid en weerbaarheid) en een doel (om na te streven). Immers een functionele risicocultuur draagt op zijn beurt weer bij aan een weerbare organisatie.

Bij de onderzochte organisaties is dit cultuuraspect integraal onderdeel van de organisatie en krijgt voortdurend aandacht. De sleutel om dit ook binnen overheidsorganisaties voor elkaar te krijgen, ligt nadrukkelijk en uitsluitend bij de (ambtelijke en bestuurlijke top van de) individuele organisaties. Het succes van risicomanagement en in het verlengde informatieveiligheid valt of staat met de houding en het gedrag van de organisatie en de individuen daarbinnen. De 'zachte' aspecten zoals een risico- of veiligheidscultuur, die cruciaal zijn voor (sturing op) informatieveiligheid, werken onvoldoende door tot in de haarvaten van de overheidsorganisaties.

Aanbeveling: Zorg voor een wettelijke verplichting van de BIO. Onze verwachting is dat een wettelijke verplichting van de BIO deze cultuur zal versnellen, inclusief (kwaliteits-) eisen gericht op 'wat' er moet gebeuren (en niet 'hoe') aan de inrichting en governance van (risicomanagement binnen) publieke organisaties (zoals beschreven in § 4.2.1 en 4.2.2).

Een gezonde risicocultuur is daarbij niet hetzelfde als een risicomijdende cultuur. Ook het slechts focussen op risicobeheersing en controle van systemen (een zogenaamde 'harde' benadering) is onvoldoende. Er dient dan ook een passende combinatie gevonden te worden tussen hard en soft controls. Het gaat dan enerzijds om het verbeteren van de hard controls, zoals eerder genoemde inrichting en heldere governance binnen de organisaties, en anderzijds om het ontwikkelen van duidelijk beleid en processen voor risicobeheersing en het formuleren van de risicobereidheid van de organisatie, inclusief het vaststellen ervan door de ambtelijke top en het bestuur.

Aanbeveling: Stel kwaliteitsaspecten van een gezonde risicocultuur, zoals duidelijk beleid en het formuleren van de risicobereidheid, vast. Zoals eerder gesteld kan BZK hierin richting geven middels het stellen van kwaliteitsaspecten (de 'wat') aan organisaties en direct of via vertegenwoordigende organisaties of gremia als VNG, IPO of UvW actief stimuleren. Ook hierin kan een zekere verplichting over 'wat' er geregeld moet zijn een waarborg zijn vanuit de stelselverantwoordelijkheid van BZK, zonder het over te nemen.

In deze lijn is bovenal het (eigen) voorbeeldgedrag van de ambtelijke en bestuurlijke leiding cruciaal. Hoewel de tone at the top veelal ongrijpbaar is, vormt een helder gestandaardiseerd beeld van de gewenste risicocultuur en hiernaar handelen het fundament. Dit gedrag in woord en daad zet de toon en kan, middels (gekwantificeerd) onderzoek, inzichtelijk gemaakt worden. Gedrag dat niet passend is, moet duidelijke consequenties hebben, bijvoorbeeld door het inperken van functionaliteit.

Aanbeveling: Geef het goede voorbeeld en draag dergelijk voorbeeldgedrag actief uit. BZK en de rijksoverheid hebben die toonzettende rol en dienen dit gedrag dan ook te laten zien: practice what you preach.

Tegelijkertijd merken we hier op dat cultuur binnen een overheidsorganisatie niet gemakkelijk te sturen is vanuit de stelselverantwoordelijkheid van BZK. De diversiteit onder overheidsorganisaties is groot en de belangen en prioriteiten die spelen binnen die organisaties zijn zo mogelijk nog diverser. We zien de grootste kans van slagen op het zorgen voor een cultuurverandering door organisaties zoveel mogelijk te ondersteunen bij het verhogen van hun volwassenheid.

Aanbeveling: Streef naar het verhogen van de algehele volwassenheid van organisaties op het gebied van informatiebeveiliging. Een hogere volwassenheid leidt tot een risicocultuur waarin informatiebeveiliging vanzelfsprekender onderdeel wordt van alle aspecten binnen de organisatie en dat leidt weer tot een hogere volwassenheid. Sturen op volwassenheid zien we als een belangrijke enabler van de gewenste risicocultuur.

Berenschot

‘WIJ ZIJN BERENSCHOT, GRONDLEGGER VAN VOORUITGANG’

Nederland is continu in ontwikkeling. Maatschappelijk, economisch en organisatorisch verandert er veel. Al meer dan tachtig jaar volgen wij als adviesbureau deze ontwikkelingen op de voet en werken we aan een vooruitstrevende samenleving. De behoefte om iets fundamenteels te betekenen voor mens en maatschappij zit in onze genen. Met onze adviezen en oplossingen hebben we dan ook actief meegebouwd aan het Nederland van vandaag. Altijd op zoek naar duurzame vooruitgang.

Alles wat we doen is onderzocht, onderbouwd en vanuit meerdere invalshoeken bekeken. Zo komen we tot gefundeerde adviezen en slimme oplossingen. Die zijn op het eerste gezicht misschien niet altijd de meest voor de hand liggende. Juist deze eigenzinnigheid maakt ons uniek. Daarbij zijn we niet van symptoombestrijding. En gaan pas naar huis als het is opgelost.

Berenschot Groep B.V.

Van Deventerlaan 31-51, 3528 AG Utrecht

Postbus 8039, 3503 RA Utrecht

030 2 916 916

www.berenschot.nl