

Provincie Noord-Holland

## **Werkbaar Weerbaar**

Weerbaarheidsbeeld provinciale organisatie en verbonden partijen

### **Colofon**

Ons kenmerk *20658*

Datum *18-4-2021*

Auteurs *John Smits  
Niko Struiksma  
Christian Boxum*

Versie *1.22a*

Status *Definitief*

[www.arenaconsulting.nl](http://www.arenaconsulting.nl)

[www.pro-facto.nl](http://www.pro-facto.nl)

# Inhoudsopgave

<b>1</b>	<b>INLEIDING .....</b>	<b>4</b>
1.1	ACHTERGROND EN DOEL .....	4
1.2	BEKNOPT BESCHRIJVING AANPAK .....	4
1.3	LEESWIJZER.....	5
<b>2</b>	<b>AFBAKENING.....</b>	<b>7</b>
2.1	DRIE RELEVANTE INVALSHOEKEN IN WEERBAARHEID TEGEN ONDERMIJNING.....	7
2.2	KWETSBARE PROCESSEN IN BEELD .....	8
2.3	WEERBAARHEIDSMATREGELEN.....	8
<b>3</b>	<b>BEWUSTZIJN .....</b>	<b>10</b>
3.1	INLEIDING .....	10
3.2	ALGEMEEN ZELFBEELD KWETSBARE PROCESSEN .....	10
3.3	BEWUSTZIJN VAN KWETSBAARHEID .....	12
3.4	RISICO'S ROND THUISWERKEN DOOR COVID-19 .....	12
<b>4</b>	<b>BESTUURLIJKE EN BELEIDSMATIGE VERANKERING.....</b>	<b>14</b>
4.1	INLEIDING .....	14
4.2	BESTUURLIJKE PRIORITEIT EN STEUN .....	14
4.3	ALGEMEEN BELEID.....	14
4.4	BIBOB-BELEID.....	16
4.5	VASTGESTELDE PROTOCOLLEN.....	16
<b>5</b>	<b>ALGEMENE ORGANISATORISCHE WAARBORGEN.....</b>	<b>17</b>
5.1	INLEIDING .....	17
5.2	ONDERMIJNING EN INTEGRITEIT .....	17
5.3	ONDERSTEUNING VANUIT HRM .....	17
5.4	INFORMATIEBEVEILIGING.....	18
5.5	INTERN TOEZICHT .....	18
<b>6</b>	<b>WEERBAARHEIDSMATREGELEN KWETSBARE PROCESSEN.....</b>	<b>20</b>
6.1	INLEIDING .....	20
6.2	WEERBAARHEIDSMATREGELEN PER SECTOR.....	20
6.3	FINANCIËLE TRANSACTIES .....	21
6.4	AANBESTEDINGEN, OFFERTES, OPDRACHTVERLENING, INKOOP .....	21
6.5	SUBSIDIES EN INVESTERINGSFONDSEN .....	22
6.6	VASTGOEDBEHEER EN GRONDEXPLOITATIE .....	22
6.7	OMGANG MET VERTROUWELIJKE INFORMATIE .....	22
6.8	VERGUNNINGVERLENING, TOEZICHT EN HANDHAVING, INCLUSIEF SANCTIONERING .....	23
6.9	CROSS-COMPLIANCE.....	23
<b>7</b>	<b>PERSOONLIJKE WEERBAARHEID.....</b>	<b>24</b>
7.1	INLEIDING .....	24
7.2	BEKENDHEID MET GELDENDE 'HUISREGELS' INTEGRITEIT .....	24
7.3	ONDERMIJNING .....	25
7.4	WEERBAAR TEGEN BEÏNVLOEDING? .....	26

<b>8</b>	<b>ORGANISATIECULTUUR EN FEITELIJK HANDELEN .....</b>	<b>27</b>
8.1	INLEIDING .....	27
8.2	UITDRAGEN NORMEN EN WAARDEN DOOR DE LEIDING .....	27
8.3	NORMEN EN WAARDEN: INTEGRITEIT CENTRAAL.....	28
8.4	OPENHEID CULTUUR.....	29
8.5	WELKE ONDERSTEUNING MISSEN MEDEWERKERS? .....	31
<b>9</b>	<b>PROVINCIALE WEERBAARHEID EN VERBONDEN PARTIJEN .....</b>	<b>32</b>
9.1	INLEIDING .....	32
9.2	AANPAK .....	32
9.3	OMGEVINGSDIENSTEN .....	33
9.4	RECREATIESCHAPPEN.....	34
9.5	NUTSBEDRIJVEN.....	35
9.6	ONTWIKKELINGSMAAATSCHAPPIJEN.....	36
9.7	STIMULERINGSFONDSEN .....	37
<b>10</b>	<b>SAMENVATTENDE CONCLUSIES .....</b>	<b>39</b>
10.1	ALGEMEEN BEELD: BASIS OP ORDE, WEL TIJD VOOR ENIG ONDERHOUD .....	39
10.2	CONCLUSIE 1: BEWUSTZIJN WISSELEND EN WAARSCHIJNLIJK KENNISACHTERSTAND .....	40
10.3	CONCLUSIE 2: INTEGRITEIT BESTUURLIJK VERANKERD, NIET SPECIFIEK WEERBAARHEID.....	41
10.4	CONCLUSIE 3: GOEDE BASIS ORGANISATORISCHE VERANKERING; HRM NOG WITTE VLEK.....	41
10.5	CONCLUSIE 4: GOEDE BASIS VAN MAATREGELEN; ENIG ONDERHOUD NODIG.....	43
10.6	CONCLUSIE 5: PERSOONLIJKE WEERBAARHEID HEEFT ONDERSTEUNING NODIG .....	43
10.7	CONCLUSIE 6: INTEGRITEIT DE NORM; GEEN ALGEHELE CULTUUR VAN AANSPREKEN.....	44
10.8	CONCLUSIE 7: DE ORGANISATIE HANDELT, MAAR GEVOELDE STEUN WISSELT .....	44
10.9	CONCLUSIE 8: WEDERZIJDSE AFHANKELIJKHEID IN WEERBAARHEID .....	45
<b>11</b>	<b>AANBEVELINGEN.....</b>	<b>47</b>
11.1	AANBEVELING 1: VERGROOT KENNIS EN HET BEWUSTZIJN VAN MEDEWERKERS .....	47
11.2	AANBEVELING 2: ORGANISEER HET VERWERKEN VAN SIGNALLEN .....	47
11.3	AANBEVELING 3: VERSTERK DE FUNCTIE VAN HRM .....	48
11.4	AANBEVELING 4: VOER EEN APK-CONTROLE MEEST KWETSBAAR PROCESSEN UIT.....	48
11.5	AANBEVELING 5: HAAK DE WEERBAARHEID VAN VERBONDEN PARTIJEN AAN .....	48

## BIJLAGEN

- Bijlage 1: Analyse kader weerbaarheidsonderzoek

# 1 Inleiding

## 1.1 Achtergrond en doel

De provincie Noord-Holland heeft zich via het project 'Versterking kwaliteit en integriteit lokaal bestuur' ingezet voor het versterken van de weerbaarheid van (gemeenten in) Noord-Holland tegen ondermijnende criminaliteit. In het collegeakkoord 'Duurzaam doorpakken!' is de aandacht voor de aanpak van ondermijning en de provinciale rol daarin bevestigd. Een van de aandachtspunten daarin is de weerbaarheid van de eigen organisatie, inclusief verbonden partijen. Om daar zicht op te krijgen is in de periode augustus-december 2020 een onderzoek uitgevoerd met als belangrijkste doelstellingen:

1. Het in beeld brengen welke (werk)processen en functies binnen de (ambtelijke) organisatie en (publieke) verbonden partijen kwetsbaar (kunnen) zijn voor ondermijning en integriteitsschendingen.
2. Het inzichtelijk maken in hoeverre de provincie mogelijke ondermijningsrisico's loopt in deze kwetsbare processen en functies.
3. Het komen tot concrete en werkbare verbeterpunten wat betreft de weerbaarheid in deze kwetsbare processen en functies.

Deze doelstelling is vertaald naar de volgende centrale onderzoeksvragen:

1. Welke (werk)processen en functies van de provincie Noord-Holland kunnen als 'kwetsbaar' worden gekwalificeerd?
2. Welke waarborgen zijn aangebracht om deze processen en functies te beschermen tegen ondermijningspogingen en integriteitsschendingen?
3. Hoe weerbaar is de provinciale organisatie op basis van het voorgaande dan wel waar loopt de provincie potentiële ondermijningsrisico's?
4. Wat kan de provincie doen om de weerbaarheid van de organisatie te vergroten?
5. Hoe kan de provincie zicht houden op de weerbaarheid en potentiële ondermijningsrisico's bij verbonden partijen en daar waar nodig op bijsturen?

## 1.2 Beknopte beschrijving aanpak

Het onderzoek is uitgevoerd aan de hand van een eerder ontwikkeld analysekader en onderzoeksmethodiek (zie bijlage 1). In de kern is gekeken naar vijf aandachtsgebieden wat betreft de weerbaarheid van de organisatie:

1. Het risicobewustzijn.
2. De bestuurlijke en beleidsmatige borging.
3. Organisatorische borging ('hard- en soft-controls').
4. De organisatiecultuur.
5. Het feitelijk handelen.

In hoofdstuk 2 worden deze begrippen en de begrippen 'kwetsbare processen' en 'weerbaarheid' nader toegelicht.

Het interne onderzoek is uitgevoerd aan de hand van:

- Een intake lijst op organisatieniveau om in beeld te brengen welke maatregelen (beleid, organisatie, protocollen etc.) er op concernniveau zijn genomen met het oog op mogelijke integriteitsrisico's en/of criminele beïnvloeding.
- Een scan van de documenten waarin dit is vastgelegd.
- Een intake lijst die is uitgezet bij alle sectoren teneinde de kwetsbare processen en getroffen maatregelen in beeld te brengen.
- Vertrouwelijke verdiepende gesprekken met management en/of medewerkers van 16 sectoren<sup>1</sup>.
- Bilaterale gesprekken met de Commissaris van de Koning, met de algemeen directeur en met de griffier.
- Een groepsgesprek met de directie.
- Een digitale anonieme vragenlijst die is uitgezet onder alle medewerkers (zowel medewerkers in eigen dienst als externe inhuur) teneinde een beeld te krijgen van het risicobewustzijn van de eigen weerbaarheid en van hoe de organisatie met ondermijningsrisico's omgaat. De respons hierop bedroeg ruim 30% (n=609)<sup>2</sup>.

Het onderzoek naar de verbonden partijen was niet gericht op het vellen van een oordeel over de weerbaarheid van deze organisaties. De focus lag op het inzichtelijk maken van de aard van de mogelijke kwetsbaarheden van verschillende typen verbonden partijen en de mogelijke afhankelijkheden in relatie tot de provinciale weerbaarheid. Meer specifiek is gekeken naar de volgende typen verbonden partijen:

1. Omgevingsdiensten
2. Recreatieschappen
3. Nutsbedrijven
4. Ontwikkelingsmaatschappijen
5. Stimuleringsfondsen

Het onderzoek is uitgevoerd aan de hand van een intake lijst op organisatieniveau (wat zijn de kwetsbare processen en getroffen maatregelen?) en per verbonden partij één of meerdere verdiepende gesprekken.

### 1.3 Leeswijzer

Het voorliggende onderzoeksrapport is opgebouwd aan de hand van het analysekader. Hoofdstuk 2 start met een schets van het referentiekader: de invalshoek van het onderzoek en de centrale begrippen als ondermijning, kwetsbare processen en

---

<sup>1</sup> Directie beleid: ruimtelijke ontwikkeling, bestuur en strategie, grond, omgevingsbeleid, onderzoek en informatie. Concernzaken: Concern Service Centrum, Financiën, HRM, Facility Management, Subsidies en Inkoop, CIO office/informatievoorziening en ICT. Beheer en Uitvoering: Bodem en Groen, Realisatie Infrastructuur. Overige: concern-control, Staf AD (chauffeurs).

<sup>2</sup> Dat is hoog in vergelijking met de responspercentages van voorgaande weerbaarheidsaudits die Arena Consulting en Pro Facto hebben uitgevoerd onder drie Noord-Hollandse gemeenten, maar lager dan bij een andere provincie waarvoor Pro Facto en Arena een weerbaarheidsaudit hebben uitgevoerd (43%).

weerbaarheid(smaatregelen). De inhoudelijke bevindingen van het onderzoek beginnen in hoofdstuk 3 met het risicobewustzijn van management en medewerkers. Daarbij is ook gekeken naar de informatiepositie ("is er zicht op risico's?"). Hoofdstuk 4 gaat in op de bestuurlijk en beleidsmatige borging: wat is het vastgestelde beleid, is weerbaarheid verankerd in de portefeuilles van het bestuur, zijn en middelen beschikbaar? In de hoofdstukken 5, 6 en 7 wordt ingegaan op de organisatorische waarborgen: de algemene voorzieningen en ondersteuning (hoofdstuk 5), de procesmatige waarborgen (hoofdstuk 6) en de persoonlijke weerbaarheid (hoofdstuk 7). Aansluitend gaat hoofdstuk 8 in op de organisatiecultuur en het feitelijk handelen in de organisatie: wat is het gedrag in de praktijk? Hoofdstuk 9 schetst de bevindingen uit het deelonderzoek 'verbonden partijen'. In de hoofdstukken 10 en 11 worden respectievelijk de belangrijkste bevindingen samengevat en voorzien van conclusies en aanbevelingen.

## 2 Afbakening

Georganiseerde criminaliteit kan alleen bestaan bij de gratie van diensten van de 'bovenwereld'. Dat kan gaan om vergunningen, toegang tot regulier bankverkeer en het beschikken over legale 'productiemiddelen' (panden, transportmiddelen, grondstoffen, facilitators). Het kan ook gaan om het kweken van 'goodwill' om geaccepteerd te worden in de samenleving waardoor het moeilijker wordt om gunsten te weigeren. Die verwevenheid van onderwereld en bovenwereld wordt aangeduid als *ondermijning*.

### 2.1 Drie relevante invalshoeken in weerbaarheid tegen ondermijning

Ondermijning kan zich op verschillende manieren manifesteren binnen een overheidsorganisatie als de provincie. In dit onderzoek maken we het onderscheid in drie invalshoeken:

1. Het door medewerkers oppikken van signalen die kunnen duiden op ondermijning van de samenleving (of andere overheden). Bijvoorbeeld door buitendienstmedewerkers op bedrijfsterreinen of in het buitengebied (signalen die kunnen duiden op drugscriminaliteit). Het onderzoek richt zich op de vraag of medewerkers in staat zijn dergelijke signalen te herkennen. Het kunnen herkennen en verwerken van dergelijke signalen kan de informatiepositie van de overheid (bestuur, strafrecht, belastingdienst etc.) versterken. Maar het kunnen herkennen van signalen is ook van belang voor de weerbaarheid: een medewerker die zich (onbewust) begeeft in een omgeving waar criminelen actief zijn, kan immers ook risico's lopen.
2. Ten tweede richt het onderzoek zich op de weerbaarheid tegen mogelijke onbewuste facilitering van criminele ondermijning door de provincie. Ondermijnende criminaliteit kan immers niet zonder facilitators in de 'bovenwereld'. Onbewust kunnen overheidsorganisaties, zoals de provincie, ondermijnende criminaliteit faciliteren door middel van het verlenen van vergunningen, subsidies, opdrachten etc. Omdat ondermijning een vorm van criminaliteit is die zich veelal aan het zicht onttrekt kunnen overheden hieraan onbewust bijdragen. We kijken naar kwetsbare processen en functies binnen de provincie Noord-Holland die mogelijk onbewust bijdragen aan het faciliteren van criminele activiteiten en de mate van bewustzijn binnen de organisatie over de mogelijke aanwezigheid en gevaren van ondermijning. Vervolgens wordt gezien welke maatregelen getroffen worden om het faciliteren van ondermijning tegen te gaan en hoe daarmee in de praktijk wordt omgegaan.
3. Ten derde kunnen criminelen door middel van beïnvloeding van bestuurders of ambtenaren proberen hun doelen te verwezenlijken. Daarbij kan gedacht worden aan bedreiging, intimidatie, omkoping of infiltratie. De provincie staat verschillende instrumenten ter beschikking om zich hiertegen te wapenen. Dan kan bijvoorbeeld gedacht worden aan het stellen van integriteitsregels, procedures om incidenten op veilige en vertrouwelijke wijze te melden en klokkenluidersregelingen. In dit onderzoek kijken we hoe deze procedures zijn vormgegeven, hoe hieraan in de praktijk invulling wordt gegeven en wat de bekendheid is van ambtenaren en bestuurders met deze regelingen.

## 2.2 Kwetsbare processen in beeld

In het onderzoek is met name gekeken naar de zogenaamde 'kwetsbare processen': dit zijn processen, handelingen of functies waar een crimineel mogelijk toegang kan krijgen tot financiële middelen, vertrouwelijke informatie, rechten (zoals vergunningen), vastgoed en documenten (zoals reisdocumenten) of waar er een belang ligt voor een crimineel dat een medewerker even 'wegkijkt', bijvoorbeeld bij het toezicht. Samengevat gaat het om:

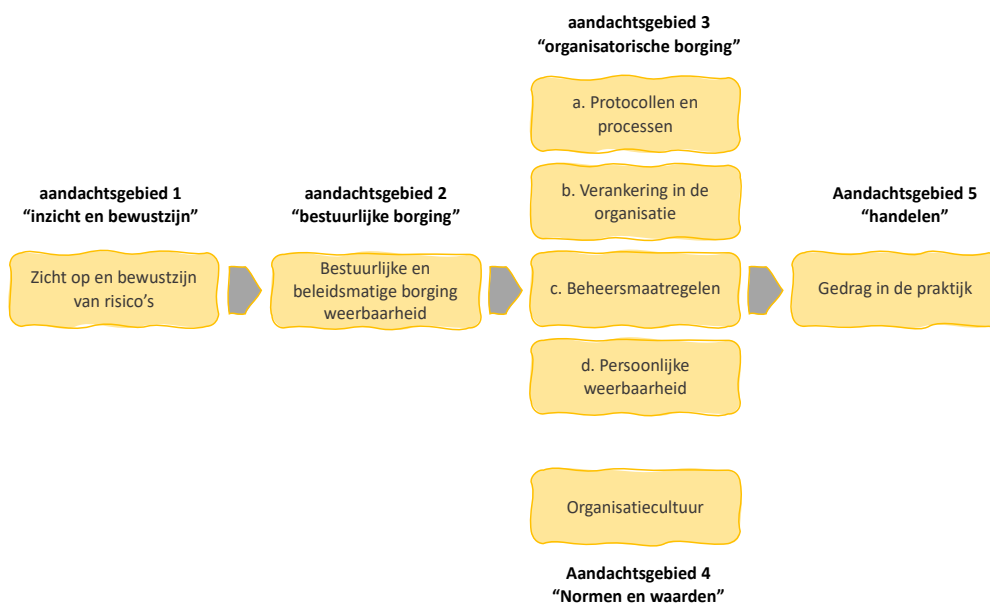
- financiële transacties (betalingen, facturering, innen boetes etc)
- aanbestedingen, inkoop, inhuur (offertes, beoordeling, opdrachtverlening)
- subsidieverlening
- vastgoedbeheer, grondexploitatie
- vergunningverlening en ontheffingsverzoeken
- toezicht en handhaving
- boetes opleggen (of kwijtschelden)
- omgaan met vertrouwelijke informatie (strategisch, financieel, persoonsgegevens)
- omgaan met waardedocumenten (zoals reisdocumenten)
- aangaan deelnemingen of samenwerking met private partijen

In het onderzoek is voor de hele organisatie in beeld gebracht welke kwetsbare processen waar in de organisatie in welke mate voorkomen. Bij het treffen van weerbaarheidsmaatregelen moet hier de prioriteit liggen.

## 2.3 Weerbaarheidsmaatregelen

De weerbaarheid van de organisatie wordt bepaald door een combinatie van factoren die in onderstaande figuur zijn samengevat.

Figuur 2.1: Aandachtsgebieden weerbaarheidsscan





Weerbaarheid begint bij het zich bewust zijn van risico's en het kunnen herkennen van signalen die kunnen duiden op ondermijning. Dat betekent dat medewerkers ook kennis moeten hebben van wat kwetsbare processen zijn en met welke vormen van ondermijning zij in hun specifieke werk het meest waarschijnlijk te maken zouden kunnen krijgen. Dat is voor handhavers anders dan voor subsidie-adviseurs of projectleiders in infrastructurele projecten.

Belangrijk is voldoende bestuurlijke steun en een beleidsmatige borging: draagt het bestuur integriteit en zich bewustzijn van ondermijningsrisico's uit? Is er beleid (met middelen) vastgesteld waar het gaat om integriteit, aanpak ondermijning en weerbaarheid?

In de organisatie kunnen verschillende soorten waarborgen tegen ondermijning worden aangebracht. In het onderzoek wordt vooral naar drie elementen gekeken:

- De *procesmatige (instrumentele) waarborgen*: is er – waar van toepassing - bijvoorbeeld sprake van functiescheiding, toepassen van het vier-ogen-principe, functieroulatie, technische beveiligingen, screenings etc.
- De *organisatorische voorzieningen*: in hoeverre wordt de weerbaarheid ondersteund vanuit ICT (informatieveiligheid), HRM (persoonlijke weerbaarheid), concerncontrol (intern toezicht) en veiligheid (zoals inzet Bibob).
- De *persoonlijke weerbaarheid* van medewerkers: in hoeverre zijn medewerkers in staat signalen die kunnen duiden op ondermijning en beïnvloedingspogingen te herkennen en zijn ze zich voldoende bewust van kwetsbaarheden.

Naast de structuur zijn ook de organisatiecultuur, met integriteit en een veilige omgeving als norm, en (daarvan afgeleid) het feitelijke handelen van de organisatie van belang: is er een sfeer waarin open kan worden gesproken over integriteit? Spreekt men elkaar aan op gedrag, ook van medewerkers richting leiding? Wordt er altijd opgetreden bij een vermoeden van integriteitsschending of poging tot beïnvloeding? En voelen medewerkers zich voldoende gesteund als zich iets voordoet?

### 3 Bewustzijn

#### 3.1 Inleiding

Weerbaarheid begint bij het bewustzijn van de mogelijke aanwezigheid van ondermijnende criminaliteit, de risico's daarvan en het kunnen herkennen van signalen die kunnen duiden op criminele intenties of activiteiten. Inzicht, bewustzijn en competentie zijn belangrijk voor de weerbaarheid van de organisatie en voor de (provinciale) informatiepositie bij de aanpak van georganiseerde criminaliteit. Signalen over ondermijning die medewerkers oppikken, moeten op een centraal punt in de organisatie bijeengebracht worden om er adequaat op te kunnen reageren. Dit levert samengevat een volgend beeld op.

#### 3.2 Algemeen zelfbeeld kwetsbare processen

Ondermijningspogingen richten zich vooral op de 'kwetsbare processen'. Aan de sectormanagers is gevraagd welke kwetsbare processen in hun sector voorkomen.

Figuur 3.1: Mate waarin er volgens de sectormanagers kwetsbare processen voorkomen in hun sector

	Financiële handelingen	Aanbestedingen	Subsidies	Vastgoed en grondexploitatie	Aanvragen en beoordelen offertes	Opdrachtverlening	Inkoop	Omgang met vertrouwelijke informatie	Vergunningen en ontheffingen	Toezicht en handhaving	Boetes opleggen of kwijtschelden	Aangaan deelnemingen of samenwerking private partijen
<b>Algemeen</b>												
Staf algemeen directeur												
Concerncontrol												
Statengriffie												
<b>Beleid</b>												
Grond												
Bestuur en strategie												
Ruimtelijke ontwikkeling												
Integrale opgaven en transities												
Groen												
Onderzoek en informatie												
Regionale economie en erfgoed												
Secretariaat en beleidsondersteuning												
Mobiliteit												
Omgevingsbeleid												
<b>Concernzaken</b>												
Facility management												
Financiën												
Concern service centrum												
HRM												
Subsidies en inkoop												
Informatievoorziening en ICT												
CIO-office												
Juridische zaken												
<b>Beheer en uitvoering</b>												
Netwerkmanagement												
Realisatie infrastructuur												
Beheerstrategie / programmering infra												
Kwaliteit, beheersing, informatie												
Bodem en groen												
Ingenieursdiensten												
Smart mobility												

■ belangrijk deel van het werk   
 ■ Komt voor (niet hoofdmoot)   
 ■ Komt (bijna) niet voor

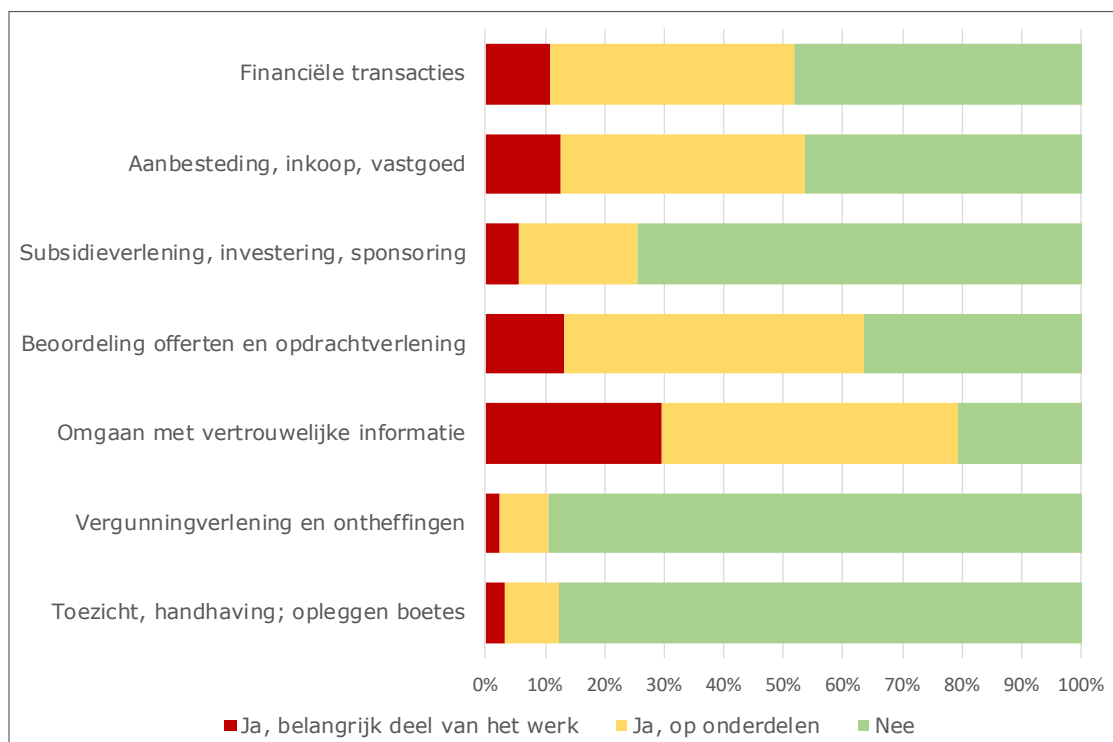
Het algemene beeld is dat elke sector in meerdere of mindere mate met kwetsbare processen te maken heeft en potentieel vatbaar kan zijn voor ondermijning. Er zijn enkele sectoren waar meerdere kwetsbare processen tot de kernactiviteiten behoren:

- Grond
- Subsidies en Inkoop
- Informatie en ICT
- Realisatie Infrastructuur
- Kwaliteit, Beheersing en Informatie
- Bodem en Groen

In de kern gaat het daarbij vooral om processen waarin financiële middelen of vertrouwelijke informatie omgaan. Vastgoedbeheer/grondexploitatie, het geven van toestemmingen (vergunningverlening), toezicht en handhaving en het aangaan van private deelnemingen komen beperkt voor. Dit met de aantekening dat vergunningverlening, toezicht en handhaving (VTH) in het fysieke domein in mandaat is belegd bij de omgevingsdiensten en dat verbonden partijen mogelijk wel private deelnemingen aangaan.

Ook aan de medewerkers is gevraagd met welke kwetsbare processen zij te maken hebben. Bijna 80% geeft aan met vertrouwelijke informatie om te gaan, daarvan 30% als hoofdactiviteit. 50-60% geeft aan te maken te hebben met financiële transacties, aanbesteding, offertes en opdrachtverlening.

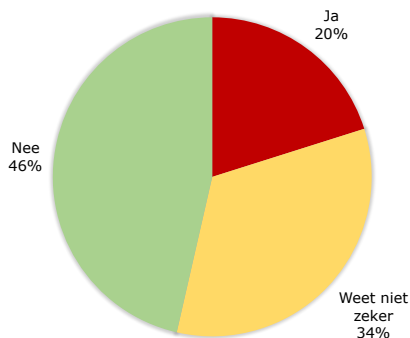
Figuur 3.2: Percentage medewerkers dat aangeeft met kwetsbare processen te werken (n=592)



### 3.3 Bewustzijn van kwetsbaarheid

Weerbaarheid begint bij voldoende bewustzijn van de mogelijke risico's, dat wil zeggen de mogelijkheid dat criminelen kunnen proberen invloed uit te oefenen. In het onderzoek is aan medewerkers gevraagd in hoeverre ze denken dat hun werk interessant is voor criminelen.

Figuur 3.3: Verwachting medewerkers over ondermijningsrisico's  
(n= 601)



Ruim 20% van de respondenten verwacht dat dat het geval is, bijvoorbeeld vanwege toegang tot informatie of middelen. Bijna de helft verwacht dat dat niet zo is. Ruim 30% geeft aan dat niet (zeker) te weten. Dat is een indicatie dat er mogelijk onvoldoende kennis is van kwetsbaarheden en risico's.

Wat opvalt is dat de meeste gesprekspartners positief zijn over het feit dat dit onderzoek wordt uitgevoerd en dat er (weer) aandacht wordt besteed aan dit thema. Uit de gesprekken komt echter een wisselend beeld naar voren daar waar het gaat om de inschatting van risico's. Bij sommige sectoren is er een sterk risicobewustzijn aanwezig, bij andere sectoren worden de risico's minder groot ingeschat. Met name in de sectoren waar men te maken heeft met financiële processen, zoals inkoop en (met name onderhandse) aanbesteding en waar men langjarige relaties onderhoudt met partijen in de buitenwereld is men zich bewust van de risico's. De sectoren waar de risico's laag worden ingeschat (door de medewerkers zelf) hebben veelal niet met (meerdere) kwetsbare processen te maken.

*Uit interviews blijkt dat er binnen de sector Grond in de afgelopen twintig jaar een grote cultuuromslag heeft plaatsgevonden. De vastgoedwereld is in deze periode enorm veranderd en er heersen een andere cultuur en mores als het gaat om integriteit. Waar het twintig jaar geleden bijvoorbeeld nog heel gebruikelijk was dat overheidsambtenaren een informele relatie onderhielden met de vastgoedwereld en zich lieten uitnodigen voor o.a. etentjes en feestelijkheden en geschenken aannamen, is dat tegenwoordig ondenkbaar. Binnen de sector Grond wordt hier tegenwoordig streng op toegezien en zit goed tussen de oren bij medewerkers van de sector wat wel en niet kan.*

### 3.4 Risico's rond thuiswerken door Covid-19

Na de uitbraak van Covid-19 werkt Nederland zoveel mogelijk thuis. Dat is ook het uitgangspunt bij de provincie Noord-Holland. Dit kan in relatie tot ondermijning bepaalde risico's met zich meebrengen. Criminelen hebben belang bij 'isolatie' van een 'slachtoffer'.

Dat is precies die situatie die het structurele thuiswerken door de COVID-19 maatregelen wordt bewerkstelligd. Er is minder (sociale) controle van collega's en leidinggevenden. Bovendien kan de (langdurige) werksituatie in combinatie met (overige)privé-omstandigheden (verlies werk partner, permanent kinderen in huis, schulden, verslavingen) iemand kwetsbaarder maken. Andere risico's die een rol kunnen spelen zijn:

- Ziekteverzuim onder medewerkers die verantwoordelijk zijn voor het beheer en de beveiliging van de hardware, besturingssystemen en hardware.
- De mogelijke kwetsbaarheid van de netwerkfaciliteiten op de thuiswerkplek en het werken met schaduwapplicaties (eigen applicaties waarop wordt gewerkt bij slechte netwerkverbindingen).
- Vertrouwelijkheid van (video)gesprekken en informatie (meekijken, meeluisteren; 'inbreken' in overleg).
- Toename van 'phishing-campagnes' van criminelen.

In alle interviews met de verschillende sectoren is gevraagd naar de potentiële risico's van thuiswerken door corona en hoe groot deze risico's worden ingeschat. Daaruit komt een wisselend beeld naar voren. Bij veel sectoren worden de risico's niet groot geacht, thuiswerken gebeurt immers altijd al wel en de technische faciliteiten zijn daarvoor aanwezig. De risico's die hierboven staan beschreven worden niet in alle gesprekken als zodanig herkend.

## 4 Bestuurlijke en beleidsmatige verankering

### 4.1 Inleiding

Voor een weerbare ambtelijke organisatie zijn bestuurlijke en beleidsmatige steun onontbeerlijk om prioriteiten te stellen, richting te geven en de benodigde middelen veilig te stellen. Bestuurlijke en beleidsmatige verankering kan door:

- ondermijning en weerbaarheid onderdeel te laten zijn van het collegeprogramma;
- specifiek toegewezen portefeuilles in het college;
- een vastgesteld beleid tegen ondermijning (zoals Bibob-beleid);
- beschikbaarheid van middelen om de organisatie weerbaar te maken.

### 4.2 Bestuurlijke prioriteit en steun

In de gesprekken duikt 'de geest van Hooijmaijers' nog diverse keren op. De gedeputeerde die in 2009 is afgetreden naar aanleiding van de bankencrisis waarbij de provincie € 78 mln dreigde te verliezen. Hooijmaijers is strafrechtelijk vervolgd en in 2013 veroordeeld voor omkoping, witwassen en valsheid in geschrifte rond bouwprojecten<sup>3</sup>. Naar aanleiding van het onderzoek van de commissie 'Schoon Schip' (2011) heeft de provincie maatregelen getroffen om de integriteit van het bestuurlijk (en ambtelijk) handelen beter te borgen. Dat werkt ook nu nog door, zo blijkt uit diverse gesprekken, in de zin dat een herhaling voorkomen moet worden en er scherper wordt gelet op integriteit.

Van de respondenten die daarover hun mening hebben gegeven (n=605), vindt 84% dat de leiding van de organisatie uitdraagt integriteit belangrijk te vinden. Van alle ondervraagde medewerkers (n=605) geeft 60% aan dat het college van Gedeputeerde Staten het belang van integriteit actief uitdraagt. In vergelijking met de voorgaande weerbaarheidsaudits scoort de provincie Noord-Holland op dit punt relatief hoog.

### 4.3 Algemeen beleid

In het Coalitieakkoord 2019 – 2023 is een passage gewijd aan de gevaren van ondermijning. Hierin is opgenomen dat 'ondermijning van het openbaar bestuur door georganiseerde criminaliteit het fundament van de democratische rechtsorde raakt. Wij blijven strijden tegen alle vormen van ondermijning en stellen hiervoor middelen beschikbaar'.

De provincie heeft nog geen (apart) beleid geformuleerd wat betreft de aanpak van de weerbaarheid van de eigen organisatie tegen ondermijning. Dat is wel in voorbereiding. De belangrijkste sporen nu zijn de Agenda 'Weerbaar Noord-Holland' gericht op het versterken

---

<sup>3</sup> Dit Dit speelde nadat de gedeputeerde was afgereden toen tijdens de bankencrisis in 2008 bleek dat de provincie veel geld had uitstaat bij onder andere de IJslandse Landsbanki en daarmee €78 mln dreigde te verliezen. Hij kwam in 2009 weer in het nieuws vanwege de zogenaamde 'bonnetjesaffaire' waarbij hoge declaraties waren gedaan zonder dat bonnetjes konden worden overleg. De toenmalige Commissaris van de Koningin, Harry Borghouts, die de declaraties had goedgekeurd, trad daarop ook af.

van de bestuurlijke weerbaarheid tegen ondermijnende criminaliteit en dat als kapstok dient voor het in voorbereiding zijnde beleid rond weerbaarheid.

*De drie pijlers van de Agenda Weerbaar Noord-Holland zijn:*

- 1. Vergroten Interne Weerbaarheid*
- 2. Eigen beleidskracht*
- 3. Lokale Weerbaarheid.*

*Het hoofddoel van de Agenda is om binnen de geografische grenzen van Noord-Holland de weerbaarheid te vergroten. Hierbij trekt de provincie gezamenlijk op met de 47 Noord-Hollandse gemeenten, de drie RIEC's in de provincie en andere partners.*

*Voorbeelden van (voltooide) projecten binnen de Agenda zijn: de uitrol van de Quickscan gemeentelijke weerbaarheid, de ontwikkeling van een methodiek ter verbetering van de informatiepositie ten aanzien van vakantieparken, de aansluiting van de Noord-Hollandse gemeenten op het netwerk van Meld Misdaad Anoniem en het opdrachtgeverschap van dit provinciaal weerbaarheidsbeeld.*

Daarnaast beschikt de provincie over staand Bibob-beleid (bestuurlijk vastgesteld in 2008 en daarna steeds geactualiseerd). Het Bibob-beleid is gespecificeerd voor:

- vastgoed- en grondtransacties
- subsidie-aanvragen
- aanvragen vergunningen
- overheidsopdrachten m.b.t bouw, milieu of ICT.

Binnen het college heeft de Commissaris van de Koning de portefeuille ondermijning en integriteit/weerbaarheid.

*Ten aanzien van ondermijningsrisico's in de 'buitenwereld' heeft de provincie geen eigen ondermijningsbeeld laten opstellen. Er is op basis van de gemeentelijke ondermijningsbeelden in 2018 een regionaal ondermijningsbeeld opgesteld. Daarbij is de notie – vanuit de eerder uitgevoerde pilots – dat de lokale ondermijningsbeelden niet per se actueel en accuraat zijn. Het opgestelde beeld wordt ook niet actueel gehouden.*

Wat betreft het bestuur is er een bestuurlijke gedragscode (voor GS en PS) en vastgesteld integriteitsbeleid voor de organisatie als geheel. Voor het versterken van de weerbaarheid is in de huidige collegeperiode jaarlijks € 150.000 beschikbaar voor de Agenda Weerbaar Noord-Holland. Per 2021 zet de provincie in op het meer programmatisch uitvoeren van weerbaarheidsscans door gemeenten, annex aan de in 2019/2020 uitgevoerde pilots. Dit gebeurt op basis van cofinanciering van de betreffende gemeenten en het RIEC.

#### 4.4 Bibob-beleid

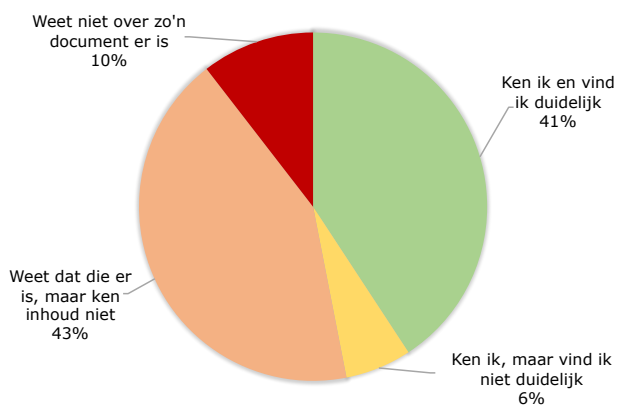
De Wet Bibob (Bevordering integriteitsbeoordelingen door het openbaar bestuur) is een preventief bestuursrechtelijk instrument. Bij dreiging van een ernstig gevaar, bijvoorbeeld dat een vergunning wordt misbruikt, kan de provincie de aanvraag weigeren of de afgegeven vergunning intrekken. De overheid voorkomt hiermee dat zij onbewust criminele activiteiten faciliteert. Bovendien beschermt zij daarmee de concurrentiepositie van bonafide ondernemers.

In de Beleidsregel Wet Bibob Noord-Holland 2019 is vastgelegd hoe de provincie gebruik maakt van het Bibob-instrument. Hierin is vastgelegd dat de provincie de Wet Bibob toepast bij vergunningverlening, subsidies, vastgoedtransacties en opdrachtverlening.

#### 4.5 Vastgestelde protocollen

De provincie heeft naast een vastgestelde ambtelijke gedragscode integriteit ook een protocol hoe te handelen bij een vermoeden van integriteitsschendingen. De helft van de medewerkers geeft in de digitale vragenlijst aan bekend te zijn met de inhoud van de gedragscode. Ruim 40% kent de inhoud niet en 10% weet niet of er zo'n code is. Op dit punt scoort de provincie Noord-Holland vergelijkbaar met de weerbaarheidsaudits die Arena en Pro Facto voor gemeenten en een provincie uitvoerden. Van de extern ingehuurde medewerkers is ruim 60% niet bekend met de gedragscode. Dat is dus substantieel hoger dan de medewerkers die bij de provincie in dienst zijn.

*Figuur 4.1: Bekendheid met de ambtelijke gedragscode (n=601)*



De provincie heeft ook een vastgesteld protocol waarin is aangegeven hoe te handelen bij een vermoeden van integriteitsschendingen ('klokkenluidersregeling'). Ruim 20% van de medewerkers heeft aangegeven hier inhoudelijk mee bekend te zijn; bijna 80% geeft aan niet te weten of zo'n regeling er is dan wel de inhoud daarvan niet te kennen. Hierin is geen verschil met de ingehuurde medewerkers.

De provincie heeft een protocol in voorbereiding waarin wordt aangegeven hoe een melding van (een vermoeden van) integriteitsschending wordt opgevolgd.

De provincie heeft geen protocol voor het melden van signalen die kunnen duiden op ondermijnende activiteiten en voor de wijze waarop opvolging wordt gegeven aan een dergelijke melding. Hetzelfde geldt voor beïnvloedingspogingen waar medewerkers mee te maken zouden kunnen krijgen. Er is ook geen extern aanspreekpunt voor meldingen over integriteitsschendingen of ondermijningskwetsbaarheden.



## 5 Algemene organisatorische waarborgen

### 5.1 Inleiding

Om weerbaar te zijn tegen ondermijning dienen organisatorische waarborgen getroffen te worden. Dit geldt met name voor organisatiefuncties die ondersteunend zijn aan de weerbaarheid: aanpak ondermijning, HRM, informatieveiligheid en intern toezicht (concern-control). Zij hebben een belangrijke rol in het borgen van de weerbaarheidsmaatregelen (zoals het verwerken van signalen, Bibob-toetsen, voldoende functiescheiding, technische beveiliging etc). Ook moeten medewerkers voldoende ondersteund, getraind en geïnformeerd worden over de mogelijke risico's van ondermijning in hun werk. Over deze verschillende waarborgen gaat dit hoofdstuk. Steeds wordt eerst het type waarborg toegelicht waaraan een weerbare organisatie in de praktijk moet voldoen. Vervolgens worden de bevindingen daarover gepresenteerd.

### 5.2 Ondermijning en integriteit

De provincie heeft geen specifieke functie of medewerker(s) met als taakgebied 'weerbaarheid'. De coördinator integriteit en de teamleider Bibob hebben in voorkomende gevallen wel een directe advieslijn richting CdK. Tot het taakgebied van de coördinator behoort het bevorderen van het integriteitsbewustzijn en de interne en externe coördinatie van signalen die medewerkers afgeven over mogelijke criminele activiteiten die ze bij de uitoefening van hun functie krijgen. Wat betreft integriteit zijn er, naast de leidinggevenden, vertrouwenspersonen.

De Eenheid SBA (Screening en Bewakingsaanpak) geeft uitvoering aan het Bibob-beleid. Zij doet onderzoek naar de integriteit van bedrijven en personen die in aanmerking komen voor een vergunning, subsidie, vastgoedtransactie of overheidsopdracht van de provincie Noord-Holland. Het doel van het onderzoek is te voorkomen dat bijvoorbeeld een vergunning wordt misbruikt voor het benutten van crimineel vermogen of het plegen van strafbare feiten. Als door het onderzoek sterke twijfels ontstaan over de integriteit van een bedrijf of persoon, vraagt de Eenheid advies aan bij het Landelijk Bureau Bibob van het ministerie van Justitie en Veiligheid. Het bureau onderzoekt de betrokkene verder en adviseert de Eenheid SBA over de mogelijke risico's. De Eenheid SBA beoordeelt met dit advies in de hand of er een ernstig gevaar is op misbruik van bijvoorbeeld de vergunning en adviseert Gedeputeerde Staten hierover. De provincie Noord-Holland kan in dat geval een vergunning of subsidie weigeren of intrekken, dan wel afzien van een vastgoedtransactie of het gunnen van een overheidsopdracht. Uit de gesprekken blijkt dat dit sporadisch voorkomt.

### 5.3 Ondersteuning vanuit HRM

Weerbaarheid van medewerkers moet een onderdeel van het personeelsbeleid zijn. HRM binnen de provincie heeft geen formele taak waar het gaat om de weerbaarheid van de organisatie, maar geeft wel ad hoc advies. De ondermijningsrisico's binnen de primaire processen van HRM zijn gering, maar de ondersteunende en faciliterende rol van HRM naar

de rest van de organisatie als het gaat om weerbaarheid is eveneens beperkt. Deze rol dicht de afdeling zich bovendien zelf ook niet toe. De afwezigheid van die rolopvatting zou verklaard kunnen worden door het feit dat HRM ook nog nooit gevraagd is om trainingen of cursussen te verzorgen in het herkennen van risico's van ondermijning.

#### 5.4 Informatiebeveiliging

Informatie moet organisatorisch en technisch goed beveiligd zijn en centraal in de organisatie aangestuurd en beheerd. Informatiebeveiliging is belegd bij de Chief Information Security Officer (Ciso). Sinds eind 2020 zijn de sectoren CIO-office en Informatievoorziening en ICT geïntegreerd. Uit gesprekken met medewerkers van de sector blijkt dat cyberveiligheid meer aandacht zou mogen krijgen binnen de organisatie. Een scenario met gijzelsoftware zoals dat zich eind 2019 bij de Universiteit Maastricht en in december 2020 bij de gemeente Hof van Twente heeft voorgedaan, vormt een reëel risico. Een ander belangrijk risico dat gesignaleerd wordt is het hacken van software door criminelen waardoor bruggen, sluizen en andere infrastructurele voorzieningen overgenomen kunnen worden.

Hoewel technische veiligheidsrisico's vanzelfsprekend afgedekt moeten worden zitten de grootste kwetsbaarheden in het menselijk gedrag; laptop mee naar huis, scherm vergrendelen etc. Vanuit Ciso worden met regelmaat phishing-testen gedaan. Daaruit blijkt dat het muisklikgedrag van medewerkers hoog is. Daar zit een risico in als het gaat om ransomware etc. Risico's worden ook gezien bij inhuurkrachten die soms verregaande autorisaties hebben in de systemen. Een goede screening zou helpen risico's te beperken.

De organisatie is niet integraal aangehaakt bij de aanpak van ondermijning. Bij signalen vindt ad hoc afstemming plaats met de coördinator integriteit.

*Bij in- en uitstroom van medewerkers of bij interne wisselingen van functies moesten tot recent de autorisaties voor de ICT-systemen handmatig worden aangepast. Daar zat een kwetsbaarheid. Daartegen is nu een maatregel getroffen waarbij maandelijks automatisch een rapportage wordt uitgedraaid waaruit blijkt welke medewerker (nog) over autorisaties beschikt waar hij of zij geen recht meer op heeft. Die fouten kunnen nu maandelijks worden hersteld.*

#### 5.5 Intern toezicht

Onafhankelijk intern toezicht op het ook feitelijk volgen van de 'spelregels' is belangrijk. Concern-control richt zich op intern financieel toezicht en vormt daarmee een belangrijke maatregel om ondermijningsrisico's te beperken. Van een integrale blik tezamen met overige stafafdelingen (HRM, ICT) op risico's van ondermijning is echter geen sprake. Er is bijvoorbeeld geen periodiek overleg tussen deze stafafdelingen waarbij risico's vanuit de verschillende perspectieven worden besproken. In het verleden keek concern-control met een bredere blik naar de organisatie dan alleen naar de rechtmatigheid van financiële transacties. De consequentie daarvan is dat mogelijk signalen of risico's van ondermijning

gemist worden. In het project 'processen centraal' in het kader waarvan alle processen worden beschreven ('processenhuis') is er weliswaar aandacht voor risico's, maar de focus ligt daarbij vooral op financiële risico's en integriteit; ondermijning is daarbij geen specifiek aandachtspunt.

## 6 Weerbaarheidsmaatregelen kwetsbare processen

### 6.1 Inleiding

Tegenover kwetsbare processen en risico's, moeten maatregelen worden getroffen: het borgen van bijvoorbeeld een vier-ogen-principe, functiescheiding, functieroulatie of fysieke en technische beveiligingen. Tegenover deze zogenaamde 'hard-controls' zijn er ook nog de 'soft-controls' zoals opleiding, training en aandacht voor ondermijningsrisico's in – het geval van de provincie Noord-Holland – het 'goede gesprek'. Dit hoofdstuk schetst welke maatregelen de provincie heeft getroffen en wat aandachtspunten zijn.

### 6.2 Weerbaarheidsmaatregelen per sector

Om te beginnen is aan alle sectormanagers gevraagd welke maatregelen in hun sector zijn genomen.

Figuur 6.1: Weerbaarheidsmaatregelen per sector

	Vier-ogen-principe	Afwezigheid 'eenplitters'	Functiescheiding	Functieroulatie	Autorisaties	Audits	Training bewustzijn risico's ondermijning	Integriteitstraining	Training weerbaarheid	Screenings, VOG's etc.	Inzet Bibob	Onderdeel van 'het goede gesprek'	Technische en fysieke beveiliging informatie	Beschrijving kwetsbare processen en risico's	Intern toezicht
<b>Algemeen</b>															
Staf algemeen directeur	Blue	Red	Blue	Red	Green	Blue	Red	Red	Red	Red	Red	Yellow	Blue	Green	Blue
Concerncontrol	Green	Red	Green	Red	Green	Yellow	Red	Red	Red	Green	Blue	Yellow	Green	Yellow	Red
Statengriffie	Green	Yellow	Blue	Blue	Green	Red	Red	Yellow	Red	Green	Blue	Red	Blue	Green	Red
<b>Beleid</b>															
Grond	Green	Yellow	Blue	Yellow	Green	Green	Yellow	Yellow	Yellow	Yellow	Green	Green	Yellow	Green	Green
Bestuur en strategie															
Ruimtelijke ontwikkeling	Yellow	Yellow	Blue	Red	Blue	Red	Red	Red	Red	Red	Red	Red	Red	Red	Red
Integrale opgaven en transities	Yellow	Yellow	Blue	Red	Yellow	Red	Red	Red	Red	Yellow	Yellow	Red	Red	Red	Red
Groen	Yellow	Yellow	Green	Red	Green	Red	Red	Yellow	Red	Yellow	Red	Yellow	Red	Red	Green
Onderzoek en informatie	Yellow	Yellow	Green	Red	Green	Red	Red	Yellow	Red	Green	Blue	Yellow	Green	Green	Yellow
Regionale economie en erfgoed															
Secretariaat	Blue		Blue	Blue	Orange	Orange	Orange	Orange	Orange	Orange	Orange	Orange	Orange	Orange	Orange
Mobiliteit	Green		Blue	Yellow	Red	Red	Yellow	Yellow	Green	Orange	Red	Green	Yellow	Orange	Orange
Omgevingsbeleid	Green	Yellow	Blue	Red	Red	Red	Red	Red	Red	Red	Green	Yellow	Red	Red	Red
<b>Concernzaken</b>															
Facility management	Green	Yellow	Green	Yellow	Blue	Blue	Red	Red	Red	Blue	Yellow	Red	Green	Yellow	Orange
Financiën	Green	Red	Blue	Blue	Yellow	Red	Yellow	Orange	Orange	Red	Green	Red	Red	Yellow	Red
Concern service centrum	Green	Green	Green	Yellow	Green	Yellow	Yellow	Yellow	Yellow	Red	Green	Orange	Green	Green	Green
HRM	Green	Green	Blue	Blue	Green	Blue	Blue	Blue	Blue	Blue	Blue	Blue	Blue	Blue	Blue
Subsidies en inkoop	Green	Green	Green	Blue	Green	Red	Green	Yellow	Red	Green	Yellow	Yellow	Yellow	Green	Red
Informatievoorziening en ICT	Green	Yellow	Blue	Red	Green	Green	Yellow	Red	Red	Red	Red	Yellow	Green	Green	Green
CIO-office															
Juridische zaken	Green	Green	Green	Red	Green	Green	Yellow	Yellow	Red	Green	Blue	Green	Green	Green	Red

Figuur 6.1: Weerbaarheidsmaatregelen per sector (vervolg)

Beheer en uitvoering													
Netwerkmanagement	ja	ja	ja	nee	ja	Geen zicht op	nee	ja (niet consequent)	ja (niet consequent)	Geen zicht op	nee	ja	ja
Realisatie infrastructuur	ja (niet consequent)	Geen zicht op	nee	ja	ja	nee	ja	nee	ja	ja	ja	nee	ja
Beheerstrategie / programmering infra	ja	Geen zicht op	nee	ja	ja (niet consequent)	Geen zicht op	nee	Geen zicht op	nee	ja	ja	Geen zicht op	nee
Kwaliteit, beheersing, informatie	ja	Geen zicht op	nee	Geen zicht op	nee	Geen zicht op	nee	Geen zicht op	nee	Geen zicht op	nee	Geen zicht op	nee
Bodem en groen	ja	ja	Geen zicht op	nee	ja	nee	ja (niet consequent)	ja (niet consequent)	ja	ja	ja	nee	Geen zicht op
Ingenieursdiensten													
Smart mobility													

ja  
 ja (niet consequent)  
 Geen zicht op  
 nee  
 Niet ingevuld  
 'niet relevant voor sector'

Uit bovenstaande matrix blijkt dat het vier ogen-principe de meest toegepaste maatregel is binnen de organisatie. De gesprekken bevestigen dit beeld. Het autoriseren van vertrouwelijke informatie en functiescheiding zijn eveneens maatregelen die in veel sectoren worden toegepast.

### 6.3 Financiële transacties

De belangrijkste maatregel om de veiligheid van financiële transacties te borgen en die organisatie breed wordt toegepast is het vier ogen-principe. Uit de intakelijst blijkt dat, voor zover de respondenten daar zicht op hebben, deze maatregel binnen de verschillende sectoren wordt toegepast. Dit beeld wordt bevestigd in de interviews. De grootte van de organisatie en sectoren maken bovendien dat alle financiële transacties linksom of rechtsom via minimaal een tweede paar ogen wordt gecontroleerd.

### 6.4 Aanbestedingen, offertes, opdrachtverlening, inkoop

Aanbestedingen boven de €50.000 moeten langs de sector inkoop en aanbesteding. Zij adviseren en begeleiden de verschillende sectoren bij het inkoopproces. De grootste kwetsbaarheid wordt gezien bij opdrachten tot €50.000, die kunnen zelfstandig door de mandaathouder worden verleend. Het verschilt per sector of daar een vier ogen-principe wordt toegepast. Er moet verderop in het proces binnen de sector wel altijd een akkoordverklaring gegeven worden voor de prestatie; ook daar vindt een vier ogen-principe plaats. Bij aanbestedingen boven de €50.000 worden minimaal drie partijen gevraagd die moeten meedingen op grond van vastgestelde spelregels. Vanaf deze categorie aanbesteding controleert de sectormanager van inkoop de volledige keten van inkoop tot betaling. De Eenheid SBA doet onderzoek naar marktpartijen bij inkoop vanaf de Europese drempelwaarden. Bij opdrachten boven €100.000 volgt een Bibob-toets, maar in de praktijk blijkt het lastig om bedrijven op basis van die bevindingen uit te sluiten van inschrijving op een aanbesteding.

## 6.5 Subsidies en investeringsfondsen

De sector Subsidies en Inkoop heeft mandaat om zelfstandig op subsidieaanvragen te beslissen. Voor bepaalde gevallen doet de eenheid SBA onderzoek naar de subsidieaanvrager, dat is een standaard onderdeel van het beslissingsproces. Indien dit onderzoek daar aanleiding toe geeft kan een Bibob-procedure worden gevolgd. De unitmanager controleert alle subsidiebeschikkingen; daar vindt altijd het vier ogen-principe plaats. Nadat de subsidie is verstrekt moet de aanvrager aantonen dat de activiteiten hebben plaatsgevonden. De betaling van de subsidies wordt niet door de unit zelf gedaan maar door het concern servicecenter.

---

*Aan het Economisch Herstelprogramma en Duurzaamheidsfonds is honderd miljoen euro beschikbaar gesteld om de gevolgen van het coronavirus en de effecten van de maatregelen te verzachten. Veel van die middelen worden via subsidies verstrekt. De risico's worden niet hoger ingeschat dan bij een reguliere subsidie, omdat de subsidieverlening via de geëigende processen verloopt en waarvoor dus dezelfde risico's gelden. Het fonds is bovendien in kleinere stukken opgeknipt en de middelen worden via tranches verdeeld. Er zijn daarnaast geen open-einde-regelingen.*

---

## 6.6 Vastgoedbeheer en grondexploitatie

Voorheen was er weinig transparantie in het proces van de gunning van gronden door de provincie. Daarin werden risico's gesignaleerd. Om die risico's te beperken is het proces nu publiekelijk inzichtelijk gemaakt doordat gronden nu worden aangeboden via een openbare website. Daarnaast geldt het vier-ogen-principe voor het sluiten van transacties als een belangrijke maatregel die is vastgelegd in de werkprocessen. De sector heeft daarnaast een kwaliteitsfunctionaris die controleert of in alle dossiers het vier ogen-principe is toegepast. Het vier ogen-principe is eveneens geborgd in de ICT-systemen. Het proces kan op een bepaald moment niet verder dan nadat een 'tweede paar ogen' een 'vinkje' heeft gezet. Een potentiële kwetsbaarheid is wel dat de sectormanager zelfstandig besluiten kan nemen, zonder 'extra paar ogen'. Deze blijven onopgemerkt tenzij dit besluit tijdens de Verbijzonderde Interne Controle (VIC) wordt gecontroleerd. Als belangrijke risicobeperkende maatregel geldt dat alle transacties in teamverband besproken worden. De regels en uitgangspunten bij de sector vastgoedbeheer en grondexploitatie zijn bovendien strenger dan elders in de organisatie. Alle medewerkers zijn doordrongen van de uitgangspunten, gedragsnormen en cultuur die nagestreefd worden. Daar wordt vanuit de sectorleiding op toegezien.

## 6.7 Omgang met vertrouwelijke informatie

Het is niet eenvoudig maatregelen te treffen tegen de risico's van de omgang met vertrouwelijke informatie. Binnen de sectoren die veelvuldig met vertrouwelijke informatie omgaan is de belangrijkste waarborg vooral gelegen in de integriteit en professionaliteit van de medewerkers. Er vindt echter geen bijzondere screening plaats en hoeven medewerkers niet periodiek een VOG in te dienen. Technische maatregelen zitten bijvoorbeeld in de onmogelijkheid voor werknemers om eigen apps of programma's te

installeren op laptops van de provincie. Tegelijkertijd is het in veel gevallen alsnog mogelijk om deze apps of programma's via een webversie te raadplegen. Daar is technisch weinig aan te doen; voldoende 'digitale weerbaarheid' van de medewerker is dus essentieel.

### **6.8 Vergunningverlening, toezicht en handhaving, inclusief sanctionering**

Dit is belegd bij de omgevingsdiensten en komt terug in hoofdstuk 9 over de verbonden partijen. In algemene zin heeft de provincie geen specifiek zicht op welke waarborgen omgevingsdiensten hebben aangebracht. De aanname is dat dezelfde standaarden worden gehanteerd als door de provincie zelf.

### **6.9 Cross-compliance**

De provincie heeft op verschillende manieren contact met de samenleving. Dat kunnen bestuurlijke of ambtelijke relaties zijn, formele contracten, in de vorm van financiële ondersteuning (subsidies, investeringen etc.), het verstrekken van informatie, het toekennen van rechten (vergunningen, ontheffingen) of het houden van toezicht en waar nodig handhavend optreden. Een weerbare organisatie borgt ook de 'cross-compliance'. Dat wil zeggen dat richting partijen in de samenleving dezelfde signalen uitgaan. Bijvoorbeeld dat wordt voorkomen dat een bedrijf waartegen een strafrechtelijk onderzoek loopt, er geen nauwe bestuurlijke contacten zijn of dat daar subsidies aan worden verleend. En dat er voldoende alertheid is op individuen die zich via verschillende kanalen toegang proberen te verschaffen tot b.v. informatie via verschillende ambtelijke, bestuurlijke en/of politieke lijnen.

Deze cross-compliance is nog geen gemeengoed in de organisatie. En met name ook niet tussen de organisatie (provincie) en verbonden partijen. We komen hier in hoofdstuk 9 over verbonden partijen nog op terug.

## 7 Persoonlijke weerbaarheid

### 7.1 Inleiding

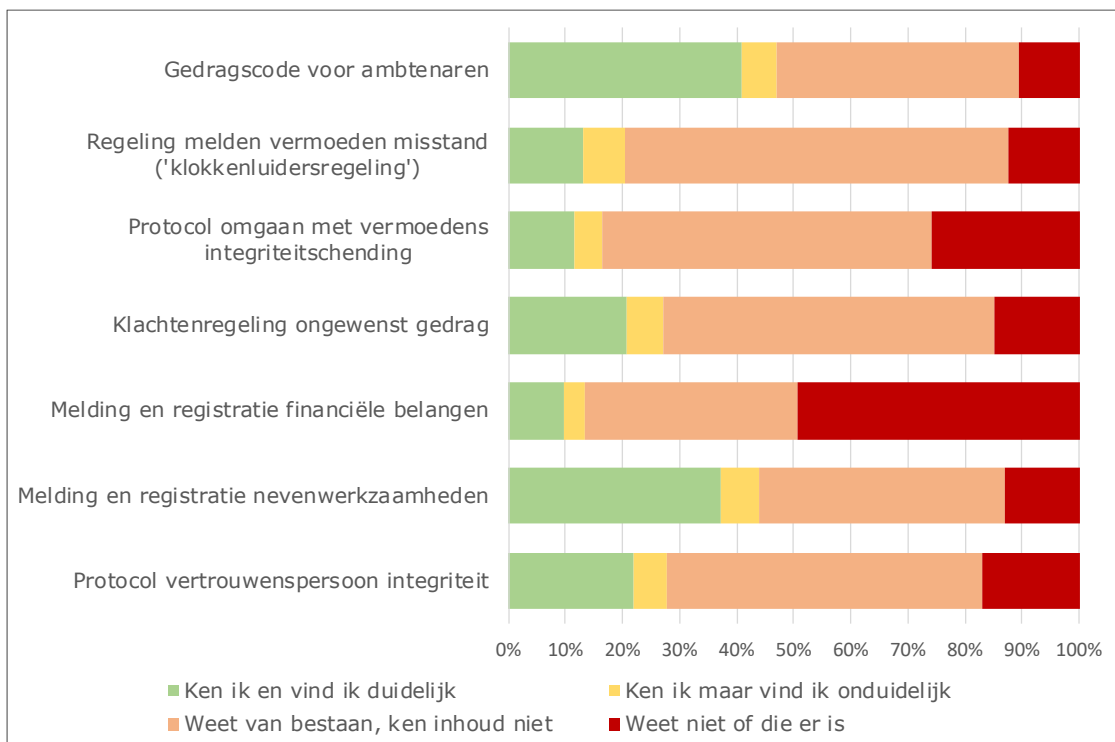
Een weerbare organisatie stelt eisen aan kennis, vaardigheden en competenties van medewerkers. Of medewerkers voldoende weerbaar zijn is afgemeten aan het:

- herkennen van signalen die kunnen duiden op criminele intenties of activiteiten;
- kunnen weerstaan van ongewenste beïnvloeding;
- in relatie tot ondermijning goed geïnformeerd zijn over mogelijke kwetsbaarheden en risico's in het werk dat ze doen;
- zich in dat geheel voldoende gesteund voelen door de organisatie;
- kennen van de gedragslijnen die in verband daarmee gelden.

### 7.2 Bekendheid met geldende 'huisregels' integriteit

Bij het in dienst treden van een medewerker wordt bij en in aanvulling op het afleggen van de ambtseed, veel aandacht besteed aan integriteit. Ook bedoeld om medewerkers te doordringen van kwetsbaarheden en hun eigen verantwoordelijkheid waar het gaat om integriteit. Aan de medewerkers is gevraagd in hoeverre ze bekend zijn de inhoud de ambtelijke gedragscode en andere protocollen waar het gaat om integriteit.

Figuur 7.1: Bekendheid met protocollen integriteit





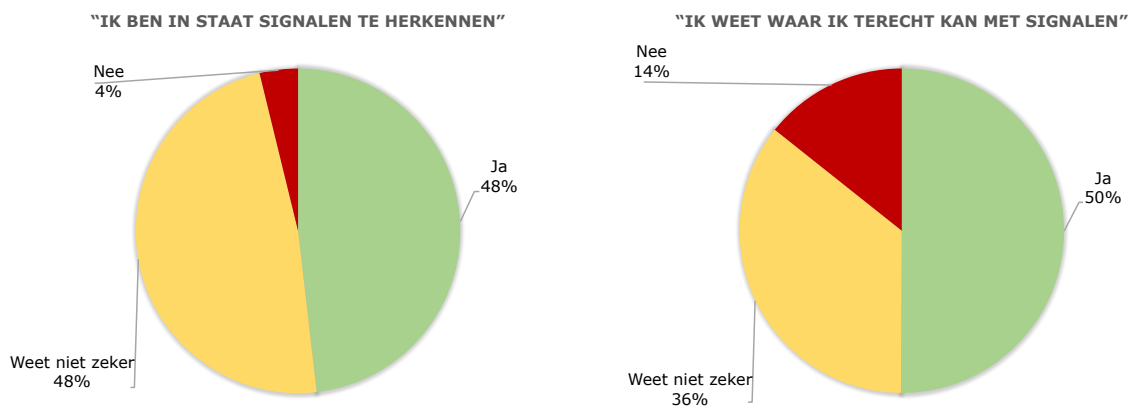
Van de meeste weten de medewerkers dat die er zijn, met uitzondering van het protocol voor het melden van financiële belangen. Met de inhoud is echter slechts een beperkt aantal bekend, nog het meest met de ambtelijke gedragscode (bijna 50%). Het minst op de hoogte zijn medewerkers met de regelingen voor het melden van een vermoeden op misstand, hoe de provincie omgaat met integriteitsschendingen en het protocol voor het melden van financiële belangen. Externe inhuur is (nog) minder bekend hiermee dan het eigen personeel.

### 7.3 Ondernijning

In de enquête is aan medewerkers gevraagd of zij zich in staat achten signalen te herkennen die kunnen duiden op ondernijning. Daarop antwoordt 48 procent dit te kunnen, 4 procent zegt dit niet te kunnen en 48 procent zegt dit niet te weten.

Ook is gevraagd of medewerkers weten waar zij terecht kunnen met signalen die duiden op ondernijning. Op deze vraag antwoordt 50 procent dit te weten, 36 procent van de ondervraagden zegt dit niet zeker te weten en 14 procent weet het niet.

*Figuur 7.2: Achten medewerkers zich in staat signalen die kunnen duiden op ondernijning te herkennen en weten ze waar ze daarmee terecht kunnen?*

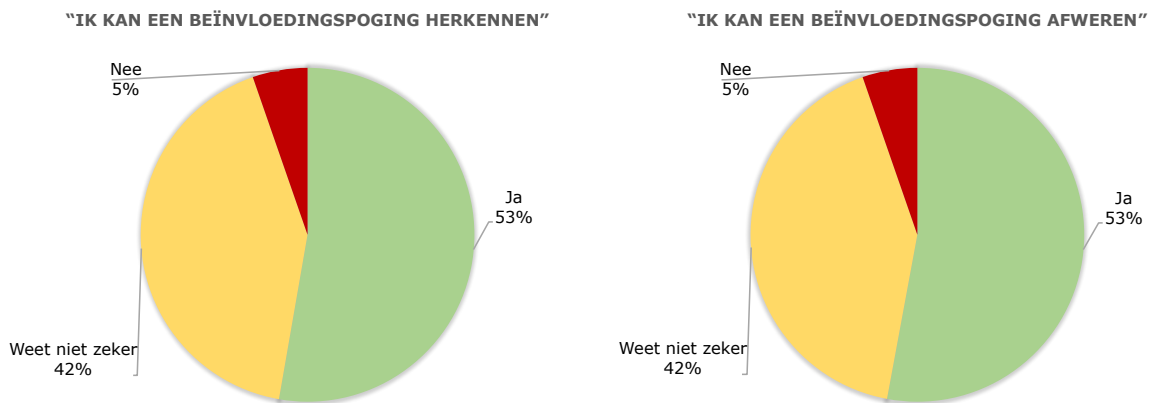


Daarnaast is gevraagd in hoeverre medewerkers voldoende steun ervaren om signalen te kunnen herkennen. Ruim 12% geeft aan dat inderdaad te vinden, maar ruim 36% vindt die steun onvoldoende. Ruim 51% geeft aan daar geen mening over te hebben.

#### 7.4 Weerbaar tegen beïnvloeding?

Van de respondenten geeft ruim de helft aan in staat te zijn om beïnvloedingspogingen te herkennen; 5% verwacht dat niet te kunnen en ruim 40% geeft aan dat niet te weten. Op de vraag of medewerkers voldoende in staat zijn beïnvloedingspogingen af te weren komt eenzelfde respons naar voren.

*Figuur 7.3: Mate waarin medewerkers zich in staat achten beïnvloedingspogingen te herkennen en die af te weren*



Uit een aantal gesprekken komt het beeld naar voren dat men graag weerbaar en omgevingsbewust wil zijn, maar dat het in bepaalde gevallen ontbreekt aan concrete handvatten of voorbeelden waarop dan gelet moet worden. Gesprekspartners vertellen baat te hebben bij concrete voorbeelden of casuïstiek die bijdragen aan het herkennen van signalen die duiden op ondermijning.

## 8 Organisatiecultuur en feitelijk handelen

### 8.1 Inleiding

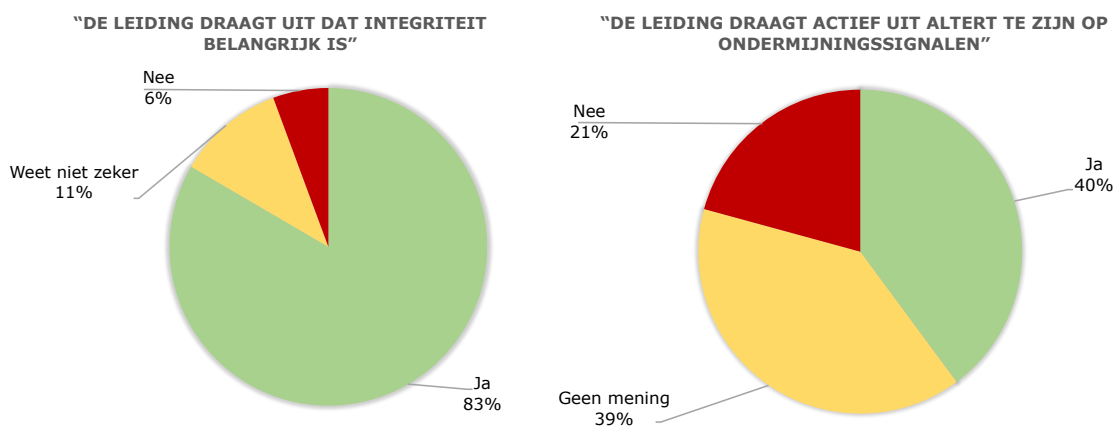
Dit hoofdstuk gaat over normen en waarden en de daaruit voortvloeiende organisatiecultuur. Integriteit en een cultuur waarin collega's elkaar kunnen en durven aanspreken op gedrag vormen namelijk belangrijke barrières voor ondermijning en zijn noodzakelijk voor een weerbare organisatie. Dat houdt in dat spelregels die gelden voor aanbestedingen, het omgaan met vertrouwelijke informatie, het verwerken van persoonsgegevens, gelijke behandeling van gelijke gevallen bij toezicht en handhaving, geen voorkeursbehandeling voor vrienden en bekenden etc., in acht worden genomen. Hoe kijken medewerkers tegen deze waarden en normen aan, hoe ervaren zij dat bestuur en management met die waarden en normen omgaan, hoe typeren zij de cultuur binnen de organisatie en voelen ze zich voldoende veilig om eventuele integriteitsschendingen ter sprake te brengen?

Daarnaast is weerbaar zijn ook weerbaar doen. Wat is het (zelf)beeld van de organisatie als het gaat om integer handelen, het melden van signalen die kunnen duiden op criminele intenties en het door de provincie (actief) optreden bij dergelijke signalen en bij mogelijke integriteitsschendingen?

### 8.2 Uitdragen normen en waarden door de leiding

Een belangrijke waarborg voor de organisatiecultuur zijn de normen en waarden die leidinggevend(en) uitdragen. Als het gaat om weerbaarheid zijn 'integriteit' en 'risicobewustzijn' belangrijke. Aan medewerkers is gevraagd hoe zij op dat punt tegen hun leidinggevend(en) aankijken.

*Figuur 8.1: In hoeverre dragen leidinggevend(en) volgens medewerkers integriteit en alert zijn op ondermijning uit?*

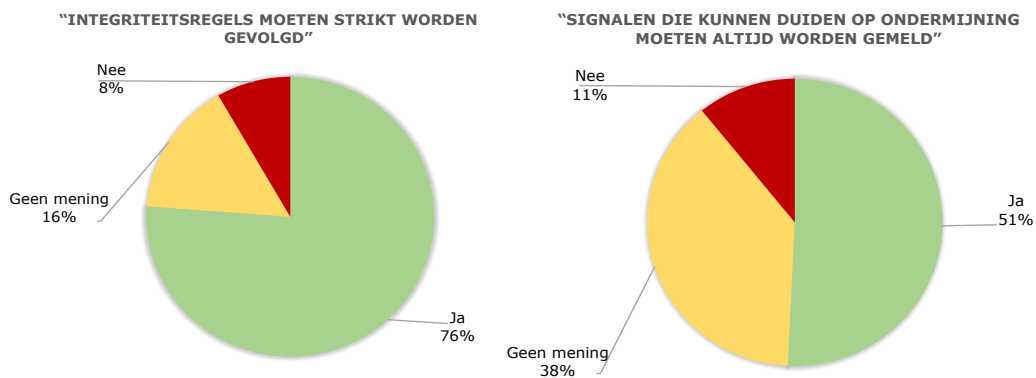


Wat betreft integriteit onderschrijft ruim 80% de stelling dat de leiding dat als belangrijke waarde uitdraagt. Slechts 40% geeft aan dat de leiding ook actief uitdraagt alert te zijn op ondermijningsrisico's.

### 8.3 Normen en waarden: integriteit centraal

Van de respondenten uit de digitale vragenlijst geeft ruim 76% aan dat integriteitsregels strikt moeten worden gevolgd. Ruim 8% is het daar niet mee eens en 16% heeft daarover geen mening.

Figuur 8.2: Hoe kijken medewerkers aan tegen integriteitsregels en het melden van signalen die kunnen duiden op ondermijning?



In de digitale enquête kon een nadere toelichting gegeven worden. Hieronder staat een aantal voorbeelden daarvan:

*"Als het gaat om inkoop zijn de regels soms zo strak dat het ten koste gaat van kwaliteit of financiën. Er zou meer ruimte moeten komen, waarbij vertrouwen aan medewerkers wordt gegeven. Controles kunnen plaatsvinden door audits en/of twee paar ogen systeem."*

*"Enkele jaren geleden was integriteit echt een issue en werd er veel over gesproken. Eigenlijk vind ik dat het de laatste twee jaar erg naar de achtergrond is verdwenen. Ik hoor er niks meer over niet van het Bestuur, niet van uit GS en ook niet vanuit de directie en het management"*

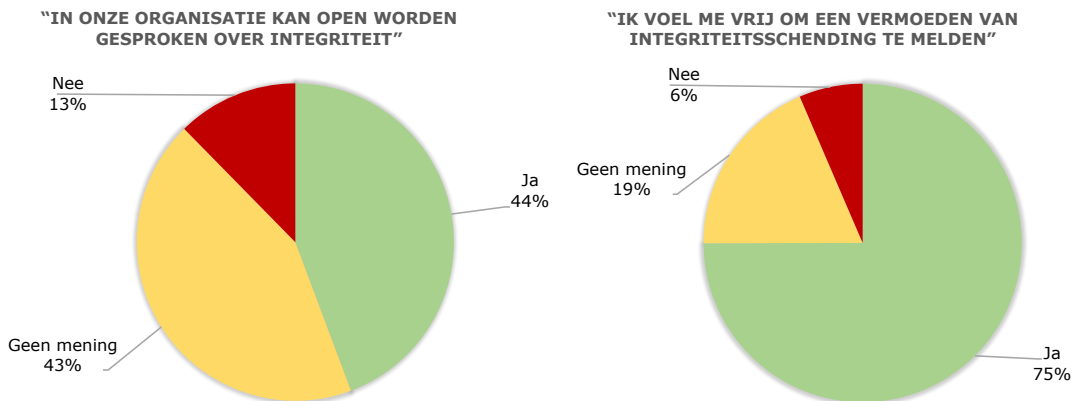
In een aantal interviews komt hetzelfde beeld naar voren; dat de aandacht voor integriteit de afgelopen jaren is verslapt." Tegelijkertijd is de teneur in een aantal gesprekken dat 'regels ook niet ten koste van alles moeten gaan; je kunt niet alles dichttimmeren. Je moet ook gewoon je werk kunnen blijven doen'.

Aan de respondenten is ook gevraagd te reageren op de volgende stelling: "Signalen van ondermijning zal ik melden" Op deze vraag antwoordt 51 procent het dat te zullen doen, 11 procent zegt dit niet te zullen doen en 38 procent weet het niet.

#### 8.4 Openheid cultuur

In de enquête is gevraagd aan respondenten of er in de organisatie op een open manier gesproken wordt over mogelijke integriteitsrisico's. 44% onderschrijft dat; 13% niet. 43% geeft aan daar geen mening over te hebben. Dit zijn vergelijkbare percentages als bij eerdere audits. Het hoge percentage 'geen mening' kan een indicatie zijn dat er in de praktijk weinig over wordt gesproken c.q. er geen aanleidingen zijn om erover te spreken.

*Figuur 8.3: Hoe vrij voelen medewerkers zich om over integriteit te spreken of een mogelijke schending te melden?*



Op de vraag of men zich voldoende vrij voelt om vermoedens van integriteitsschendingen te melden antwoordt 75% bevestigend; 6% van niet. 19% geeft aan geen mening te hebben, mogelijk omdat met nog nooit in de situatie is gekomen.

Uit de interviews komt een beeld naar voren dat werknemers binnen de verschillende sectoren het lastig vinden elkaar aan te spreken op gedrag. Er is geen algemene cultuur van elkaar aanspreken. Dit wordt ook in de gesprekken als aandachtspunt gezien; men moet elkaar durven aanspreken en ervoor open staan aangesproken te worden. Een aantal sectorhoofden benadrukt het belang hiervan en zegt hier actief op te sturen richting de medewerkers door dicht op de werkvloer te zitten en door benaderbaar te zijn<sup>4</sup>.

<sup>4</sup> Het laatste is juist een van de zaken die niet kunnen met de COVID-19 maatregelen. Een extra indicatie dat de risico's mogelijk worden onderschat.

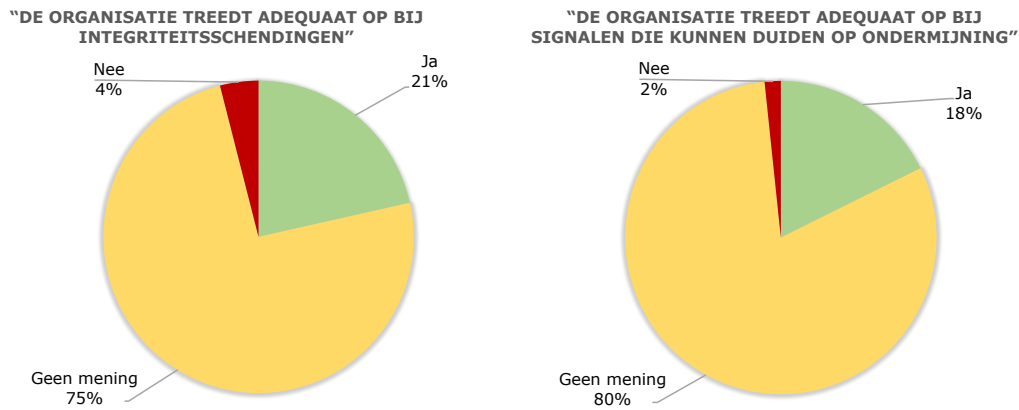
Belangrijk om te vermelden is dat sinds medio 2021 het programma DADEN loopt binnen de provincie Noord-Holland. Dit programma is erop gericht medewerkers te trainen en coachen in het elkaar aanspreken op houding en gedrag.

In de enquête is de vraag gesteld of de organisatie adequaat optreedt bij integriteitsschendingen. Daarop antwoordt 22 procent bevestigend, 4 procent ontkennend en 75 procent van de ondervraagden weet het niet.

In 2019/2020 is circa 20 keer een melding gedaan van mogelijke integriteitsschendingen, ongewenst gedrag niet meegerekend. Er is op centraal niveau geen zicht op het aantal keren dat medewerkers signalen hebben opgepikt die kunnen duiden op ondermijnende criminele activiteiten of dat getracht is medewerkers (vanuit criminele motieven) te beïnvloeden.

In de digitale vragenlijst heeft bijna 6% (35 respondenten) aangegeven de afgelopen twee jaar een (vermoedelijke) integriteitsschending te hebben gesignaleerd. Hiervan antwoordt bijna 35% dit met de betreffende persoon te hebben besproken en ruim 40% (ook) met de leidinggevende. Circa 20% heeft het (ook) besproken met de vertrouwenspersoon en/of coördinator integriteit.

*Figuur 8.4: Wat vinden medewerkers van het optreden van de organisatie bij integriteitsschendingen of signalen die kunnen duiden op een ondermijningspoging?*



Van de respondenten antwoordt ruim 20% dat de organisatie in geval van een integriteitsschending adequaat optreedt. 4% vindt van niet. Bijna 75% heeft daar geen zicht op.

Bijna 4% (32 respondenten) antwoordt de afgelopen jaren één of meerdere keren signalen te hebben opgevangen die kunnen duiden op ondermijning. Ruim 20% geeft aan daar niets mee te hebben gedaan. De helft geeft aan dat intern te hebben gemeld.

Van de respondenten geeft bijna 18% aan dat de organisatie adequaat optreedt bij signalen die kunnen duiden op ondermijning. Ruim 80% heeft daar geen zicht op.

Ruim 8% (51 respondenten) geeft aan dat de afgelopen twee jaar één of meerdere keren is getracht hen op een onwenselijke wijze te beïnvloeden. Daarvan geven er 7 respondenten aan dat daar (zeer waarschijnlijk) criminele motieven een rol hebben gespeeld; 3 respondenten geven aan dat niet zeker te weten. Bijna 4% van de respondenten geeft aan zich niet bewust te zijn van ongewenste beïnvloeding, maar sluiten dat niet uit. Van degenen die zeggen te maken te hebben gehad met een beïnvloedingspoging antwoordt ongeveer 50% dat zelf afgewend te hebben en/of gemeld te hebben bij de leidinggevende. Ruim 40% heeft het (ook) besproken met collega's.

Van degenen die te maken hebben gehad met ongewenste beïnvloeding geeft twee derde aan dat de organisatie hen daarop op adequate wijze heeft ondersteund.

### **8.5 Welke ondersteuning missen medewerkers?**

Uit zowel de enquêtes als uit de gesprekken blijkt een sterke behoefte te bestaan onder medewerkers aan ondersteuning bij het weerbaar zijn tegen onaanvaardbare beïnvloeding en in het herkennen van signalen die kunnen duiden op ondermijning. Hieronder volgt een aantal illustratieve voorbeelden van toelichtingen hierop die zijn gegeven in de enquête.

*"Dus echt gewoon oefenen met een situatie waarin je iemand aan de telefoon hebt die iets van jou wil dat je eigenlijk niet wilt geven of iemand die boos is en zijn zin probeert te krijgen en dan goed leren reageren."*

*"Het herkennen van ondermijning/beïnvloeding is belangrijk voor alle ambtenaren. Door kennisvergroting op deze thema's is het makkelijker te herkennen voor je zelf of voor collega's die daarmee te maken hebben. Je moet in gesprek gaan over wat wel en niet toelaatbaar is, dit is soms een grijs gebied en dat maakt het lastig."*

*"Het is altijd goed om op de hoogte te zijn van recente pogingen en ontwikkelingen aangaande ondermijning in de organisatie."*

*"Het management zou over beïnvloeding van mij en mijn collega's daar meer dan nu over kunnen informeren."*

*"Procedures, handboeken, protocollen sussen de organisatie alleen maar in slaap (en kosten tijd en geld). Een bondige training om te kunnen herkennen en opties voor actie helpt, en dan met regelmaat opfrissen."*

*"Ik weet niet of ik het kan herkennen en als ik het herken bij wie ik vervolgens moet zijn en welke stappen ik moet zetten."*

## 9 Provinciale weerbaarheid en verbonden partijen

### 9.1 Inleiding

De provincie Noord-Holland neemt deel in eenenveertig zogenaamde 'verbonden partijen'. Dat zijn organisaties waarin de provincie een financieel en bestuurlijk belang heeft. Het gaat om negentien privaatrechtelijke participaties, zoals de NV afvalzorg en het Provinciaal Waterbedrijf Noord-Holland (PWN), veertien gemeenschappelijke regelingen zoals de Omgevingsdiensten en recreatieschappen en acht overige deelnemingen zoals het IPO en diverse stichtingen.

Kenmerkend voor verbonden partijen is dat het zelfstandige rechtspersonen zijn met een eigen bestuur en eigen financiële huishouding. De provincie staat daarmee op afstand. In een aantal gevallen is de provincie enig aandeelhouder, zoals bij het PWN en PDENH. Vaak is er een gedeelde deelname of eigenaarschap, meestal met één of meerdere gemeenten.

Ook medewerkers van verbonden partijen kunnen in hun werk in aanraking komen met ondermijning en interessant zijn voor criminelen, bijvoorbeeld door de informatiepositie, de financiële middelen die erin omgaan, het dichtknijpen van een oogje waar een verbonden partij toezicht uitoefent of mogelijk chantage via ransomeware.

### 9.2 Aanpak

Omdat de provincie op afstand staat, is er minder direct zicht op mogelijke kwetsbaarheden en weerbaarheidsmaatregelen. In het onderzoek is tegen het licht gehouden wat voor verschillende typen verbonden partijen de meest kwetsbare processen zijn en waar mogelijke ondermijningsrisico's liggen die uiteindelijk ook de provincie bestuurlijk en/of financieel kunnen treffen. Op basis van het profiel van de lijst van verbonden partijen zijn vijf (hoofd)typen onderscheiden die zijn onderzocht:

1. Omgevingsdiensten
2. Recreatieschappen
3. Nutsbedrijven
4. Ontwikkelingsmaatschappijen
5. Stimuleringsfondsen

Het onderscheid zit daarbij zowel in het taakgebied, de aard van de meest prominent aanwezige kwetsbare processen als in de (juridische) vorm en daarmee de positie van de provincie. Bij elk van deze typen is een concrete verbonden partij geselecteerd die nader is onderzocht. Daarbij ging het dus niet om het vellen van een oordeel over de betreffende organisatie, maar om het krijgen van meer zicht op de typische (potentiele) risico's en kritische aandachtspunten voor de provincie als deelnemer en/of opdrachtgever voor het type verbonden partij. Het onderzoek zelf is uitgevoerd aan de hand van een intake lijst over kwetsbaarheden en maatregelen, een documentenscan en per verbonden partij één of meer verdiepende gesprekken.



### 9.3 Omgevingsdiensten

Omgevingsdiensten zijn opgericht om de uitvoering van vergunningverlening, toezicht en handhaving (VTH) voor gemeenten en provincies robuuster te maken. Dat wil zeggen, voor meer en betere expertise, een meer transparant uitvoeringsproces en waar nodig voldoende bestuurlijke distantie. De provincie neemt deel in vier omgevingsdiensten, waarbij de Omgevingsdienst Noordzeekanaalgebied (ODNZKG) verantwoordelijk is voor de meest risicovolle bedrijven in de hele provincie en de Omgevingsdienst Noord-Holland Noord (ODNHN) voor de groene wetgeving (natuur, landschap).

*Figuur 9.1: kwetsbare processen omgevingsdiensten*

Type verbonden partij	Financiële handelingen	Aanbestedingen	Subsidies	Vastgoed en grondexploitatie	Aanvragen en beoordelen offertes	Opdrachverlening	Inkoop	Omgaan met vertrouwelijke informatie	Vergunningen en ontbreffingen	Toezicht en handhaving	Boetes, opleggen of kwijtschelden	Aangaan deelnemingen of samenwerking private partijen
Omgevingsdiensten												

Komt (bijna) niet voor
  Komt voor maar geen hoofdmoot
  Belangrijk deel van het werk

De uitvoering van VTH-taken betreft in zichzelf kwetsbare processen. Dat is ook de hoofdtak van de omgevingsdiensten. Binnen die taken wordt ook omgegaan met gevoelige informatie, b.v. wat betreft leidingen, installaties, (tunnel)constructies etc in relatie tot mogelijk terroristische motieven. Het werkgebied van de omgevingsdiensten ligt voor een deel ook in gebieden waar in zichzelf een verhoogd ondermijningsrisico ligt, zoals havens (smokkel, mensenhandel) en het buitengebied (drugslabs in lege panden) en branches met een verhoogd risicoprofiel (afval, grondstromen). Medewerkers krijgen regelmatig te maken met vormen van intimidatie of bedreiging.

Belangrijke maatregelen die van omgevingsdiensten mogen worden verwacht zijn:

- Borgen van een cultuur van integriteit en elkaar daarop kunnen aanspreken.
- Consequent inzetten van het Bibob-instrumentarium.<sup>5</sup>
- Beheersmaatregelen als vier-ogen-principe, functieroulatie en functiescheiding (b.v. ook Wob-verzoek niet laten afhandelen door de behandelaar van het dossier).
- Training medewerkers op alertheid kunnen herkennen signalen, bij informatievragen check doen (b.v. bij opvragen informatie over tunnelconstructie) en weerbaarheid (training, coaching in 1<sup>e</sup> jaar van aanstelling).
- Informatieveiligheid (technisch, digitale weerbaarheid) en investeren in inzet digitale middelen (analyses ketens, inzet drones etc.).

<sup>5</sup> Voor provinciale bedrijven doet de provincie dit zelf.

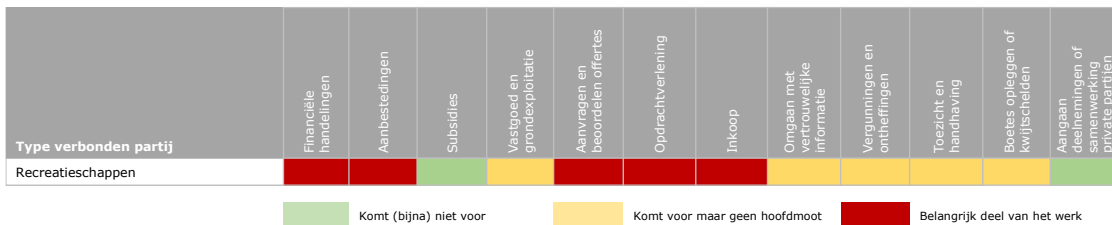
Mogelijk bijzondere aandachtspunten in relatie tot de weerbaarheid van de provincie zijn, zo blijkt uit de gesprekken:

- Potentiële risico's van indirecte vormen van beïnvloeding waarbij druk wordt gezet op gemeenten en van een omgevingsdienst een 'ruimhartige' afweging wordt gevraagd bij het verlenen van een vergunning of bij het toezicht. Dit raakt weliswaar niet de directe verantwoordelijkheid van de provincie maar als deelnemer in de regeling, kan zij hier wel bestuurlijk in worden geraakt.
- De cross-compliance tussen de waarneming en beoordeling die een omgevingsdienst doet bij bedrijven vanuit VTH, de mogelijk economische relaties die er zijn tussen dezelfde bedrijven en provincie en de ondermijningsaanpak vanuit de provincie.

#### 9.4 Recreatieschappen

Recreatieschappen zijn verantwoordelijk voor het beheer en onderhoud van recreatiegebieden, ze maken het landschap toegankelijk en houden zich bezig met natuurontwikkeling, voorlichting en educatie. De provincie Noord-Holland neemt samen met gemeenten deel aan 5 recreatieschappen. De uitvoering van het beheer is uitbesteed aan Recreatie Noord-Holland NV (waarvan de provincie enig aandeelhouder is) en Recreatie Midden-Nederland.

Figuur 9.2: kwetsbare processen recreatieschappen



Qua kwetsbare processen zijn de meest voorkomende financieel gerelateerd, namelijk aanbestedingen/opdrachtverlening en inkoop (met name enkelvoudige onderhandse aanbestedingen). De gebieden die door recreatieschappen worden beheerd kunnen echter wel een basis zijn voor ondermijning of criminele activiteiten, los van de vraag of daar ook formele taak of verantwoordelijkheid ligt van een recreatieschap. Als belangrijkste aandachtspunten gelden:

- aanwezigheid vastgoed en horeca (witwassen)
- leegstaande bebouwing (drugslabs)
- recreatieparken (mensenhandel, drugscriminaliteit)
- smokkelroutes tussen Noorzeekanaal en Amsterdam

Beheersmaatregelen die van recreatieschappen mogen worden verwacht zijn:

- borging financiële processen (vierogenprincipe, mandatering etc.);
- bij vastgoedbeheer en -ontwikkeling het uitvoeren van een due diligence (DD)- of Bibob-onderzoek<sup>6</sup> (ook bij tenders);
- in het toezicht ook in staat zijn om signalen op pakken die kunnen duiden op ondermijning.

Er zijn geen specifieke risico's die de weerbaarheid van de provincie beïnvloeden.

## 9.5 Nutsbedrijven

De provincie is deelnemer in nutsbedrijven zoals het waterleidingbedrijf (PWN), een afvalverwerkingsbedrijf (NV Afvalzorg) en een netbeheerder (Aliander). Nutsbedrijven zijn zelfstandige private bedrijven in handen van de overheid (overheids-NV's) en die diensten verlenen die van algemeen belang worden beschouwd.

Figuur 9.3: kwetsbare processen Nutsbedrijven

Type verbonden partij	Financiële handelingen	Aanbestedingen	Subsidies	Vastgoed en grondexploitatie	Aanvragen en beoordelen offertes	Oprachverlening	Inkoop	Omgaan met vertrouwelijke informatie	Vernuningen en ontberingen	Toezicht en handhaving	Boetes opleggen of kwijtschelden	Aangaan beslissingen of overeenkomsten met private partijen
Nutsbedrijven	Belangrijk deel van het werk	Belangrijk deel van het werk	Komt (bijna) niet voor	Belangrijk deel van het werk	Belangrijk deel van het werk	Belangrijk deel van het werk	Belangrijk deel van het werk	Belangrijk deel van het werk	Komt voor maar geen hoofdmoot	Belangrijk deel van het werk	Belangrijk deel van het werk	Belangrijk deel van het werk

■ Komt (bijna) niet voor     
 ■ Komt voor maar geen hoofdmoot     
 ■ Belangrijk deel van het werk

Nutsbedrijven hebben – afhankelijk van de aard – een breed palet aan kwetsbare processen, dat wil zeggen, processen waarin grote geldstromen omgaan (aanbesteding, inkoop, investeringen), vastgoedbeheer en het omgaan met vertrouwelijke informatie (zoals persoonsgegevens). Een grote kwetsbaarheid zit ook in de functie van de bedrijven: de installaties en systemen die bloot kunnen staan aan cyberaanvallen met het oogmerk deze te hacken met als doel afpersing (ransomware) of sabotage (terroristische motieven). De bescherming van de nutsfunctie is dus essentieel. Hierin heeft ook de NCTV een rol, voor het beschermen van vitale functies.<sup>7</sup> Maatregelen die mogen worden verwacht van een nutsbedrijf zijn:

- Beheersmaatregelen wat betreft de financiële processen (inkoop, aanbesteding) en beheer vastgoed zoals functiescheiding, vier-ogen-principes, mandatering, interne controles.
- Technische beveiliging van persoonsgegevens en beveiliging tegen het hacken van de systemen. Daarbij hoort ook een voldoende digitale weerbaarheid van medewerkers.

<sup>6</sup> Afhankelijk of de beheerende organisatie publiek (inzet Bibob) of privaat (DD) is.

<sup>7</sup> In het Dreigingsbeeld Statelijke Actoren van de Nationaal Coördinator Terrorismedbestrijding en Veiligheid (NCTV) (feb 2021) worden nutsbedrijven waaronder waterleidingbedrijven benoemd als onderdeel van de 'vitale infrastructuur'.

Cybersecurity zou hoog op de agenda moeten staan en zijn geborgd in de organisatie (security officer).

- Niveaus van screening in verhouding tot de kwetsbaarheid van functies en toegang tot vitale systemen.
- Voor zover sprake is van deelnemingen in andere bedrijven, een juridische scheiding tussen de uitvoering van publieke taken (nutsfunctie) en overige marktactiviteiten.

De weerbaarheid van nutsbedrijven tegen eventuele (cyber)criminele of terroristische acties is voor de provincie zowel van bestuurlijk als groot maatschappelijk belang.

## 9.6 Ontwikkelingsmaatschappijen

Ontwikkelmaatschappijen ondersteunen bedrijven bij het doen van investeringen en nieuwvestiging. De ondersteuning kan gaan om het leggen van verbindingen bij bijvoorbeeld het vinden van een geschikte locatie (gemeente) of pand (vastgoedeigenaren), het vinden van de juiste partners (samenwerking), investeerders, kredietverstrekkers of subsidieverleners (makelaarsrol). Dat doen ontwikkelingsbedrijven zowel vraaggestuurd als in de vorm van actieve acquisitie om bedrijven naar de regio te halen. Een andere lijn is dat ontwikkelbedrijven zelf deelnemen in (terrein)ontwikkelingen of ondernemingen. De provincie participeert in twee ontwikkelingsmaatschappijen. Het ontwikkelbedrijf NHN richt zich enkel op de 'makelaarsrol'; de Regionale Ontwikkelingsmaatschappij Noordzeekanaalgebied NV met name ook op deelnemingen. Er loopt nu een traject om te komen tot één regionale ontwikkelingsmaatschappij (ROM) op de schaal van provincie, inclusief de Metropoolregio Amsterdam (MRA).

Figuur 9.4: kwetsbare processen ontwikkelingsmaatschappijen

Type verbonden partij	Financiële handelingen	Aanbestedingen	Subsidies	Vastgoed en grondexploitatie	Aanvragen en beoordelen offertes	Opdrachtverlening	Inkoop	Omgaan met vertrouwelijke informatie	Verunningen en ontberfingen	Toezicht en handhaving	Boetes opleggen of kwijtschelden	Aangaan deelnemingen of aandelen van private partijen
Ontwikkelingsmaatschappijen	Geel	Geel	Groen	Rood	Geel	Geel	Geel	Geel	Geel	Geel	Geel	Rood

■ Komt (bijna) niet voor     
 ■ Komt voor maar geen hoofdmoot     
 ■ Belangrijk deel van het werk

De kwetsbaarheid hangt af van het profiel van een ontwikkelingsmaatschappij. Die zit enerzijds in het omgaan met vertrouwelijke informatie, zowel bij participatie in ontwikkelingen (voorkennis, crimineel geld) als bij het vervullen van de 'makelaarsrol'. De ontwikkelingsmaatschappij beschikt vaak eerder dan de buitenwereld over informatie over (bedrijfs)economische ontwikkelingen. Voor criminelen kan een ontwikkelingsmaatschappij ook een toegangspoort zijn tot informatie over het beschikbaar komen van panden of mogelijkheden tot financiering. Bij (private) participaties kunnen ook malafide partijen zich aandienen, bijvoorbeeld wat betreft de herkomst van investering (denk aan de ontwikkeling van de jachthaven in Velsen). In geval van investeringen acteert een ontwikkelingsbedrijf mogelijk ook in een gebied dat ondermijningsgevoelig is, zoals een havengebied.

- Belangrijke maatregelen bij ontwikkelingsmaatschappijen zijn dus ook onderzoek naar de achtergrond van een potentiële partner (due diligence) of geïnteresseerden in

informatie over vestigings- of financieringsmogelijkheden. Ook screening natuurlijke personen en toetsing/afstemming met SBA zijn relevant.

- Beheersmaatregelen als het vier-ogen-principe, functiescheiding en functieroulatie met het oog op langdurige relaties en financieel processen.
- Screening / VOG eigen medewerkers, in elk geval op de meest kwetsbare processen en bij langdurige relaties.

In termen van weerbaarheid liggen hier voor de provincie hier potentieel vooral bestuurlijke risico's (imago schade als malafide partijen toegang weten te krijgen tot informatie of middelen) en het voet aan de grond krijgen van criminelen.

### 9.7 Stimuleringsfondsen

De provincie heeft een aantal verzelfstandigde fondsen in het leven geroepen met het oog op gewenste maatschappelijke ontwikkeling. Daaronder vallen het stimuleren van een duurzame economie of slimme technologie en het (economisch en maatschappelijk) herstel van de coronacrisis. De fondsen hebben een aanzienlijke hoeveelheid middelen beschikbaar om te investeren in initiatieven. In de kern moeten de fondsen 'revolverend' zijn. Dat gebeurt in drie stappen:

- het acquireren en beoordelen van een initiatief en het nemen van een investeringsbesluit;
- het doorontwikkelen van het initiatief tot het zich heeft ontwikkeld tot een zelfstandig renderend bedrijf;
- het uitstappen en onttrekken van de eerder gedane investering.

Figuur 9.5: kwetsbare processen stimuleringsfondsen

Type verbonden partij	Financiële handelingen	Aanbestedingen	Subsidies	Vestgoed en grondexploitatie	Aanvragen en beoordelen offertes	Oprachtoverlening	Inkoop	Omgaan met vertrouwelijke informatie	Vergunningen en ontheffingen	Toezicht en handhaving	Boetes opleggen of kwijtschelden	Aangaan deelnemingen of samenwerking private partijen
Stimuleringsfondsen	Belangrijk deel van het werk	Komt (bijna) niet voor	Komt (bijna) niet voor	Komt (bijna) niet voor	Komt voor maar geen hoofdmoot	Komt voor maar geen hoofdmoot	Komt voor maar geen hoofdmoot	Belangrijk deel van het werk	Komt (bijna) niet voor	Komt (bijna) niet voor	Komt (bijna) niet voor	Belangrijk deel van het werk

■ Komt (bijna) niet voor     
 ■ Komt voor maar geen hoofdmoot     
 ■ Belangrijk deel van het werk

De kwetsbare processen zijn vooral gelegen in het omgaan met vertrouwelijke informatie en in de privaatrechtelijke participaties. Het kan voor malafide partijen interessant zijn daarin en een positie te verwerven, enerzijds vanuit direct financieel gewin (binnenhalen investering, boedel leeg achterlaten) en anderzijds mogelijk ook vanuit een oogpunt van witwassen of het creëren van faciliteiten voor de ondersteuning van criminele activiteiten ('witwassen' afval).

Belangrijke weerbaarheidsmaatregelen zijn:

- Onderzoek naar de achtergrond (inclusief investeerders) van een bedrijf (due diligence) en screening van natuurlijke personen. En ook toetsing/afstemming met SBA.
- Een (onafhankelijke) bedrijfseconomische beoordeling van het businessplan.

- Screening dan wel VOG eigen medewerkers op de meest kwetsbare functies.
- Overige beheersmaatregelen zoals vier-ogen-principe en functiescheiding

Wat betreft de specifieke risico's voor de provincie zit dat vooral in imago en beeldvorming indien malafide bedrijven investeren of voet aan de grond krijgen in (mede door de provincie) geïnitieerde initiatieven. Ook kan er een financieel risico ontstaan.

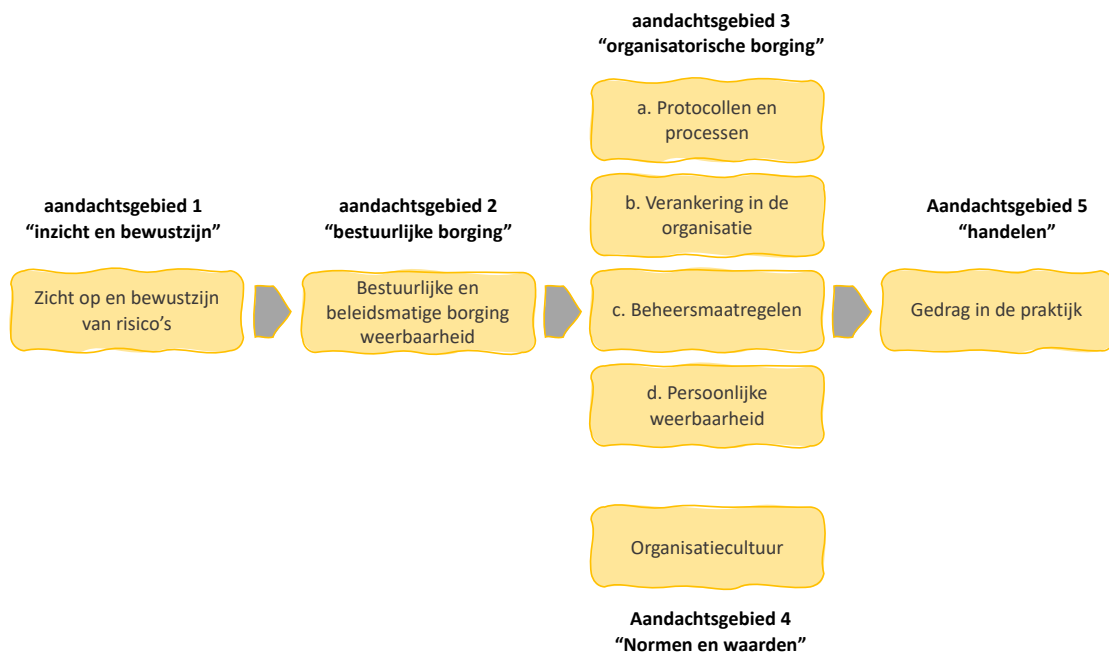
## 10 Samenvattende conclusies

In het voorgaande zijn de bevindingen van het onderzoek naar de weerbaarheid van de organisatie van de provincie Noord-Holland geschetst. In dit slothoofdstuk worden de belangrijkste zaken aan de hand van het analysekader samengevat en worden overkoepelende conclusies getrokken. Op basis daarvan doen we een aantal aanbevelingen met het oog op het versterken van de weerbaarheid.

### 10.1 Algemeen beeld: basis op orde, wel tijd voor enig onderhoud

Het algemene beeld is dat de provincie de basis voor een weerbare organisatie op orde heeft. Er is een algemeen bewustzijn van het belang van integer handelen; bestuurlijk en ambtelijk. Dit is ook in bestuur en beleid verankerd. In de organisatie zijn veel checks & balances aangebracht, zowel vanuit het interne toezicht, zij het vooral financieel, als vanuit informatieveiligheid. Op de meeste kritische functies zijn ook beheersmaatregelen getroffen om de integriteit en rechtmatigheid te borgen. Onder andere door een brede toepassing van het vier-ogen-principe, functiescheiding en autorisaties.

Figuur 10.1: Aandachtsgebieden weerbaarheidsscan



Alhoewel de bestuurlijke aanpak van ondermijning gemeengoed is, is de 'ondermijning' van de eigen organisatie en 'weerbaarheid' daartegen een relatief nieuw aandachtsgebied. Risico's worden laag ingeschat, zonder dat er altijd een duidelijke onderbouwing is voor een dergelijke inschatting. De constatering is dat er nog vooral veel onbekendheid is. Met ondermijning (en welke vormen men in het werk mee in aanraking zou kunnen komen), met het herkennen ervan en met de kwetsbaarheden en risico's in de processen. Vooral de 'soft-controls' zijn onderbelicht. Maar de basis die er ligt, biedt voldoende fundament om een volgende stap in de weerbaarheid van de organisatie te zetten. Meer specifiek komen we tot de volgende conclusies.

## 10.2 Conclusie 1: bewustzijn wisselend en waarschijnlijk kennisachterstand

Alle sectoren in de organisatie hebben in meerdere of mindere mate met kwetsbare processen te maken. Bijna 80% van de medewerkers geeft aan in het werk met vertrouwelijke informatie van doen te hebben, waarvan circa 30% aangeeft dat dat de hoofdmoot van het werk betreft. Daarnaast geeft 60-70% aan in hun werk met verschillende vormen van opdrachtverlening (inhuur, inkoop, aanbesteding etc.) te maken te hebben, waarvan circa 20% als hoofdactiviteit.

Van de respondenten die aangeven dat kwetsbare processen de hoofdmoot van hun werk betreffen, verwacht ruim 30% dat criminelen zouden kunnen proberen hen te beïnvloeden; circa 50% geeft aan dat niet te weten. Van degenen die wel met kwetsbare processen van doen hebben, maar waar het slechts een klein deel van het werk is, is dit respectievelijk circa 20% en 30-40%. Daarbij worden als mogelijke risico's gezien:

- Beïnvloeding bij aanbestedingen, subsidies etc. (preferente leveranciers, langdurige relaties etc.) of enkelvoudige onderhandse aanbestedingen ('onzichtbaarder', meer vertrouwen dan controle).
- Geen zicht hebben op achterliggende structuren en waarborgen van consortia en organisaties waarmee wordt samengewerkt, waar subsidies aan worden verleend of die namens de provincie taken uitvoeren (verbonden partijen).
- Beïnvloeding van lobbyisten bij het binnenhalen van Europese subsidies (waarbij mogelijk niet altijd duidelijk is wat er achter een bedrijf waarvoor gelobbyd wordt, schuilgaat).
- Het verkrijgen van informatie over mogelijke investeringen of ruimtelijke ontwikkelingen.

Over de vraag in hoeverre COVID-19 een risicoverhogende factor is, wordt verschillend gedacht. Enerzijds wordt aangevoerd dat de werksituatie in de kern niet anders is dan bij 'normaal' thuiswerken, inclusief de daarbij behorende technische beveiligingen. Anderzijds is er minder zicht op wat zich 'buiten het beeldscherm' afspeelt. Zowel in de uitvoering van het werk zelf (wie kijkt er mee waar het gaat om vertrouwelijke informatie?) als in de thuissituatie (maakt Corona-stress iemand kwetsbaarder en daarmee bevattelijker voor beïnvloeding?).

Van de respondenten die met kwetsbare processen van doen hebben, geeft gemiddeld ruim 40% aan geen beïnvloedingsrisico's te zien. Bij degenen waar kwetsbare processen slechts een deel van het werk betreft, ligt dit hoger, bij degenen waar het een structureel onderdeel is, lager. Ze voeren dit er (deels) op terug ook niet goed te weten wat de ondermijningsrisico's zijn in hun werk.

*Conclusie: Het risicobewustzijn laat een ambivalent beeld zien. Medewerkers die beperkt met kwetsbare processen te maken hebben denken minder vaak dat criminelen hen zouden kunnen beïnvloeden dan medewerkers waarvoor kwetsbare processen de hoofdmoot van het werk vormt. Dat er een relatief grote groep is die aangeeft niet te weten of ze risico lopen terwijl ze in kwetsbare processen zitten, is een indicatie voor een informatieachterstand op dit punt.*



### 10.3 Conclusie 2: Integriteit bestuurlijk verankerd, niet specifiek weerbaarheid

Integriteit is een basisvoorwaarde voor weerbaarheid. In het coalitieakkoord 2019-2023 is de aanpak van ondermijning en de weerbaarheid van het (lokale) bestuur als een van de speerpunten opgenomen. Dit is (was) ook de basis voor het project 'Versterking kwaliteit en integriteit lokaal bestuur' en de 'Agenda Weerbaar Noord-Holland'. Voor die agenda is gedurende de collegeperiode ook jaarlijks budget beschikbaar (€150k). Zo zet de provincie per 2021 in op het faciliteren van weerbaarheidsscans voor gemeenten.

Wat betreft de integriteit van het college van Gedeputeerde Staten en Provinciale Staten is een bestuurlijke gedragscode vastgesteld voor integriteit. Hierin ontbreekt echter de context van ondermijning. Het college draagt het belang van integriteit ook uit naar de organisatie. Dit wordt door ruim 60% van de respondenten uit de digitale vragenlijst onderschreven. Ruim 4% is het daar niet mee eens. De overige geven aan daar geen zicht op te hebben.

Naast een bestuurlijke gedragscode is er ook een ambtelijke gedragscode voor integriteit en zijn er richtlijnen voor het melden van nevenfuncties en neveninkomsten. De gedragscode is over het geheel bij 90% van de medewerkers bekend. Van de eigen medewerkers geeft 40% aan de inhoud niet te kennen of deze onduidelijk te vinden; bij de inhuur is dat 60%. Net als in de bestuurlijke gedragscode ontbreekt ook in de ambtelijke gedragscode de context van ondermijning. Integer handelen maakt immers weerbaar tegen ondermijning. Er is geen specifiek beleid voor de weerbaarheid van de eigen organisatie, bijvoorbeeld waar het gaat om het omgaan met signalen die kunnen duiden op ondermijning of het omgaan met beïnvloedingspogingen van medewerkers. Een meer uitgewerkt integraal beleid voor de aanpak van ondermijning is in voorbereiding. De aanpak is wel verankerd in een (strikt) Bibob-beleid dat is gespecificeerd voor vastgoed en grondtransacties, subsidieaanvragen, vergunningaanvragen en aanbestedingen/opdrachtverlening. Voor de zogenaamde 'klokkenluidersregeling' geeft bijna 80% aan de inhoud of het bestaan ervan niet te kennen. Een mogelijke verklaring hiervoor is dat hieraan na het afleggen van de ambtseed, geen specifieke aandacht meer wordt besteed.

*Conclusie: de bestuurlijke awareness van het belang van de aanpak van ondermijning en de weerbaarheid van het bestuur en zijn uitvoeringsorganisatie, is hoog. Er is een aanzet tot beleidsmatige verankering, doch deze is nog niet uitwerkt. Er is bij de medewerkers, en nog meer bij de inhuur, veel onbekendheid met de 'letter van de gedragscode'. Mogelijk dat die bekendheid er 'in de geest' wel is, maar er een zeker risico op 'eigen invulling' is en daarmee uiteenlopende referentiekaders voor integriteit.*

### 10.4 Conclusie 3: Goede basis organisatorische verankering; HRM nog witte vlek

De provincie heeft geen specifieke functie of medewerker(s) met als taakgebied 'weerbaarheid'. De coördinator integriteit en de teamleider Bibob hebben wel een algemene adviesrol (richting CdK). De coördinator heeft o.a. als taak het bevorderen van het integriteitsbewustzijn en het coördineren van de verwerking van signalen die medewerkers

oppakken. Voor wat betreft integriteit zijn naast de leidinggevendenden vertrouwenspersonen aanspreekpunt.

Het onderzoek naar de integriteit van bedrijven en personen is ondergebracht bij de eenheid Screening en Bewakingsaanpak (SBA). Bij twijfels over een persoon of bedrijf wordt advies gevraagd van het landelijk bureau Bibob. Het doel is om te voorkomen dat de provincie (onbedoeld) meewerkt aan het ontplooiën of in stand houden van criminele activiteiten door b.v. een vergunning te verlenen of dat financiële middelen als subsidies worden gebruikt voor het plegen van strafbare feiten.

De sector HRM heeft – behoudens waar het gaat om ad hoc adviesvragen - geen specifieke taak waar het gaat om de weerbaarheid van de organisatie. Zowel wat betreft de inrichting als de persoonlijke weerbaarheid van medewerkers.

De informatieveiligheid is belegd bij de sectoren Informatievoorziening en ICT en CIO-office. Deze zijn eind 2020 geïntegreerd. Informatieveiligheid krijgt (technisch) veel aandacht. Er is wel de notie dat cybercrime om permanente alertheid en doorontwikkeling vraagt. Bijvoorbeeld waar het gaat om gijzelsoftware. Complicerende factoren zijn niet alleen de techniek maar ook dat informatiesystemen (steeds meer) aan elkaar gekoppeld zijn. Vanuit ICT worden de belangrijkste risico's echter gezien in het gedrag van gebruikers. Bijvoorbeeld bij phishingmail-tests blijkt steeds weer dat medewerkers toch op linkjes klikken. Ook het veel thuiswerken i.v.m. de COVID-19 maatregelen worden vanuit ICT als extra risico gezien (wie kijkt mee?); dit wordt niet door de gehele organisatie zo gezien. Een aandachtspunt is integraal beleid ten aanzien van informatieveiligheid. Bijvoorbeeld in relatie tot screening en autorisaties van externen die toegang hebben tot de interne systemen en data (tot voor kort tot aan de aanbestedingsprocedures toe).

Het interne toezicht gebeurt door concerncontrol. De focus ligt vooral op de rechtmatigheid van financiële transacties. Integriteit en het beheersen van ondermijningsrisico's behoren niet tot het taakgebied. Er is bijvoorbeeld ook geen toezicht (controle) op voldoende cross-compliance tussen verschillende domeinen. Zo kan het voorkomen dat een bedrijf enerzijds financiële ondersteuning ontvangt van de provincie terwijl er anderzijds een handhavingstraject loopt via een van de omgevingsdiensten.

*Conclusie: vanuit de organisatie zijn de integriteitsbeoordeling van organisaties en/of personen waaraan de provincie diensten verleent dan wel faciliteert of financiert en de (technische) informatieveiligheid geborgd. Aandachtspunten zijn vooral de digitale weerbaarheid van de medewerkers en mogelijke integriteitsrisico's door oneigenlijke inzage in gegevens (door inhuur). Dat HRM geen rol en functie heeft in de weerbaarheid van de organisatie is een aandachtspunt. Vooral wat betreft het versterken van de persoonlijke weerbaarheid van medewerkers. Er is geen systematisch intern toezicht op het voldoende afdichten van ondermijningsrisico's in de werkprocessen.*

### 10.5 Conclusie 4: Goede basis van maatregelen; enig onderhoud nodig

Elke sector heeft in meerdere of mindere mate maatregelen getroffen die kunnen bijdragen aan het versterken van de weerbaarheid. Dit geldt met name voor de financiële processen waar het gaat om inkoop, aanbestedingen, subsidies etc. en vastgoed/grondtransacties. Daar geldt het vier-ogen-principe, functiescheiding en (boven een bepaalde grens) de inzet van Bibob. De maatregelen zijn evenwel meestal genomen vanuit een oogpunt van integriteit (en voorkomen fraude) en rechtmatigheid en – behoudens de inzet van Bibob – niet specifiek gericht op de weerbaarheid. Het vier-ogen-principe, functiescheiding en autorisaties voor het omgaan met vertrouwelijke informatie worden in de hele organisatie toegepast voor meerdere kwetsbare processen. Eenpitters komen – mede door de grootte van de organisatie – zeer beperkt voor. Overige maatregelen, als functieroulatie (bij langdurige relatie), audits (of andersoortig onderzoek) en screenings (inhuur, functiewisseling), worden niet altijd consequent ingezet. De softcontrols zoals trainingen en aandacht voor ondermijningsrisico's in "het goede gesprek" zijn, met uitzondering van enkele sectoren, geen gemeengoed. Dit lijkt vooral ook een aandachtspunt voor het omgaan met vertrouwelijke informatie.

*Conclusie: de instrumentele borging van vooral de financiële processen is voor de hele organisatie grotendeels op orde. Maatregelen als interne controles en vooral de softcontrols zijn nog onderbelicht.*

### 10.6 Conclusie 5: Persoonlijke weerbaarheid heeft ondersteuning nodig

De persoonlijke weerbaarheid heeft niet alleen te maken met het bewustzijn van ondermijningsrisico's maar ook kennis hebben welke spelregels (integriteit) er gelden, hoe signalen die kunnen duiden op ondermijning te kunnen herkennen, wat de risico's van kwetsbare processen zijn en weten wat te doen bij een beïnvloedingspoging. Zoals eerder aangegeven kent een belangrijk deel van de medewerkers en inhuur de inhoud van de ambtelijke gedragscode niet. Circa 45% van de eigen medewerkers en 60% van de ingehuurd medewerkers geven aan te denken dat ze in staat zijn om signalen te herkennen die kunnen duiden op ondermijnende activiteit. Ruim 50% (inhuur: 40%) weet waar ze daarmee terecht kunnen. Ingehuurd krachten pakken dus mogelijk eerder signalen op maar weten minder waar ze daarmee terecht kunnen. Van de eigen medewerkers geeft ruim 50% aan zich in staat te achten een beïnvloedingspoging te kunnen herkennen en zelf af te weren. Bij de inhuur is dat 60%. Medewerkers geven aan behoefte te hebben aan meer informatie en training op dit punt, zowel in algemene zin als aan de hand van casuïstiek.

*Conclusie: Er is een kennisachterstand bij een groot deel van de medewerkers wat betreft het kunnen herkennen van signalen en beïnvloedingspogingen en onzekerheid over het zelf kunnen afweren van een beïnvloedingspoging. Er is duidelijke behoefte aan ondersteuning.*

### 10.7 Conclusie 6: Integriteit de norm; geen algehele cultuur van aanspreken

Een belangrijke bouwsteen voor een weerbare organisatie is de organisatiecultuur. Dat gaat om de normen en waarden, over waarop wordt gestuurd en de vraag hoe open kan worden gesproken over zaken als integriteit en ondermijning. Bijna 85% van de medewerkers die de enquête hebben ingevuld vindt dat de leiding integriteit als belangrijke waarde uitdraagt en ruim 75% vindt dat integriteitsregels strikt moeten worden gevolgd. Dat laatste is interessant in combinatie met de constatering dat de helft van de medewerkers de integriteitsregels niet (in detail) kent.

Bijna 40% vindt dat er in de organisatie vrij kan worden gesproken over integriteitsrisico's en integriteitsschendingen. Ruim 20% vindt van niet. De overige hebben daarover geen mening gegeven. Ongeveer 75% voelt zich vrij om een (vermoeden van) integriteitsschending te melden. Ruim 6% niet.

Er is in de organisatie geen cultuur van elkaar aanspreken. En ook de mate waarin er wordt gesproken over ondermijningsrisico's wisselt. Sinds medio 2019 loopt het programma DADEN binnen de provincie Noord-Holland. Dit programma is erop gericht medewerkers te trainen, begeleiden en coachen op het elkaar aanspreken op gedrag.

*Conclusie: integer zijn is de norm binnen de organisatie, maar er is nog geen algehele cultuur om daarover vrij te spreken en elkaar erop aan te spreken.*

### 10.8 Conclusie 7: De organisatie handelt, maar gevoelde steun wisselt

In 2019/2020 zijn door medewerkers naar schatting circa 20 meldingen gedaan van integriteitsschendingen, ongewenst gedrag niet meegerekend. Er is geen (centraal) inzicht in of en hoe vaak medewerkers signalen hebben opgepikt die kunnen duiden op ondermijning of dat getracht is medewerkers te beïnvloeden.

Van degenen die hebben aangegeven de afgelopen twee jaar een (vermoedelijke) integriteitsschending te hebben gezien (6%), zegt 35% de betreffende persoon daarop te hebben aangesproken en dat 40% dat (ook) met de leidinggevende heeft besproken. Van de respondenten die één of meerdere keren een signaal hebben opgevangen dat kan duiden op ondermijning, geeft de helft aan dat intern te hebben gemeld. Ruim 8% van de respondenten geeft aan dat de afgelopen jaren is getracht hen één of meerdere keren oneigenlijk te beïnvloeden, waarvan 10 (mogelijke) pogingen met een crimineel motief. Nog eens 4% zegt zich niet bewust te zijn geweest van (criminele) beïnvloedingspogingen, maar sluiten dat niet uit. Van degenen die hebben aangegeven daar zicht op te hebben, zegt bijna 85% dat de organisatie adequaat optreedt bij integriteitsschendingen. Ruim 65% voelde zich voldoende gesteund in situaties dat gepoogd werd hen te beïnvloeden. Er is in geval van poging tot beïnvloeding vooral behoefte aan actieve steun van de leiding (verantwoordelijkheid niet bij de medewerker laten) en voldoende gehoor vinden.

In algemene zin voelt ruim 30% zich voldoende geïnformeerd over de kwetsbaarheid van processen, handelingen en functies waarin medewerkers zich bevinden. Ruim 20% vindt

dat ze voldoende ondersteuning krijgen in het weerbaar zijn tegen criminele beïnvloeding; 80% niet.

*Conclusie: (vermoedens van) integriteitsschendingen worden doorgaans opgepakt. Signalen die kunnen duiden op ondermijnende activiteiten niet. Als sprake is van ongewenste beïnvloeding, voor zover zichtbaar en gemeld, treedt de organisatie op maar de mate waarin een medewerker die het overkomt zich voldoende gesteund voelt, wisselt. Er is grote behoefte aan meer structurele ondersteuning wat betreft inzicht in en omgaan met ondermijningsrisico's.*

### **10.9 Conclusie 8: Wederzijdse afhankelijkheid in weerbaarheid**

De verschillende typen verbonden partijen hebben verschillende kwetsbaarheidsprofielen. Het gaat daarbij deels om dezelfde type kwetsbaarheden als bij de provincie zelf, maar deels en deels om bijzonder kwetsbaarheden. De 'algemene' kwetsbaarheden en risico's zitten vooral in financiële transacties (inkoop/aanbesteding, opdrachtverlening, subsidies) en het omgaan met vertrouwelijke informatie. Specifieke potentiële risico's en kwetsbaarheden zijn:

- 'gijzeling' of 'aanslag' op nutsvoorzieningen<sup>8</sup>
- participaties van ontwikkelingsbedrijven waarin ook criminelen de hand kunnen hebben en de bijzondere informatiepositie van ontwikkelingsbedrijven
- vergunningverlening, toezicht en handhaving door omgevingsdiensten en hun informatiepositie wat betreft kwetsbare objecten
- grote geldstromen waarin kleine bedragen weg kunnen vallen
- indirect beïnvloeding, daar waar criminelen/malafide ondernemers gemeenten beïnvloeden en provincie als mede deelnemers bestuurlijk kunnen worden geraakt (imago).

Deze kunnen indirecte weerbaarheidsrisico's voor de provincie met zich meebrengen wat betreft imagoschade en financiële schade en mogelijke ook maatschappelijke schade. Behalve het treffen van de 'reguliere' maatregelen zullen verbonden partijen ook maatregelen moeten treffen op deze specifieke kwetsbaarheden.

Daarnaast is er ook een zekere wederzijdse afhankelijkheid in de weerbaarheid, dan wil zeggen tussen verbonden partijen onderling en tussen verbonden partijen en provincie. Bijvoorbeeld waar het gaat om geldstromen (investeringen, subsidies etc.) of gebiedsontwikkeling enerzijds en toezicht en handhaving bij malafide bedrijven anderzijds. Een goed samenspel waar het gaat om informatie-uitwisseling en signalering voor elkaar, een afdoende cross-compliance én het waar nodig en mogelijk inzetten van elkaars instrumenten en bevoegdheden (zoals de rol van SBA) is daarbij essentieel.

---

<sup>8</sup> Dit is ook vooral een zaak voor bijvoorbeeld de NCTV.

Dit zicht op elkaar en het bewustzijn van de afhankelijkheid is nog geen gemeengoed, waarbij de behoefte aan het verbeteren daarvan wel wordt geproefd in de gesprekken.

*Conclusie: verbonden partijen kennen deels specifieke kwetsbaarheden die ook om specifieke aandacht en maatregelen vragen. Er is in de weerbaarheid van verbonden partijen en provincie sprake van een wederzijdse afhankelijkheid. Daarvan is ook een zekere notie maar die is nog niet vertaald in een structurele samenhang van maatregelen.*

## 11 Aanbevelingen

Op basis van het voorgaande komen we tot vier kernaanbevelingen om de weerbaarheid van de provinciale organisatie te versterken.

### 11.1 Aanbeveling 1: Vergroot kennis en het bewustzijn van medewerkers

De eerste aanbeveling is het opzetten van een programma tot versterking van het risicobewustzijn wat betreft ondermijning en van de persoonlijke weerbaarheid, meer specifiek het verhogen van het kennis- en bewustzijnsniveau door middel van voorlichting, bespreken casuïstiek, informatie op intranet, eventueel training etc. wat betreft:

- De (meest waarschijnlijke) vormen van criminaliteit en ondermijning waarmee medewerkers in verschillende werkvelden te maken kunnen krijgen én wat signalen zijn die kunnen duiden op de feitelijke aanwezigheid daarvan. Buitendienstmedewerkers zullen (deels) met andere verschijningsvormen van criminaliteit of ondermijning en signalen te maken krijgen dan bijvoorbeeld medewerkers die werken met aanbestedingsprocessen of subsidieverlening.
- De specifieke kwetsbaarheden van de werkprocessen, handelingen en functies waarmee medewerkers te maken hebben.
- De wijzen waarop criminelen via misleiding, manipulatie, verleiding, kunnen pogen een medewerker te beïnvloeden dan wel zich toegang zouden kunnen verschaffen tot informatie, middelen, diensten/rechten etc. en wat signalen zijn die daarop kunnen duiden.
- Besteed in het integriteitsbeleid expliciet aandacht aan de risico's op (ambtelijke/bestuurlijke) ondermijning. De mechanismen zijn weliswaar hetzelfde als bij 'gewone' integriteitsschendingen (giften, omkoping, manipulatie) maar de gevolgen kunnen breder zijn (minder individueel).

In meer algemene zin is in het licht van de COVID-19 maatregelen voorlichting en training wat betreft de digitale weerbaarheid aan te bevelen.

### 11.2 Aanbeveling 2: Organiseer het verwerken van signalen

De tweede aanbeveling betreft het organiseren van het verwerken van signalen. Daarbij gaat het zowel om de vraag of er beïnvloedingspogingen worden gedaan (dat kan b.v. ook gaan om phishingmails) als om de vraag of medewerkers in hun werk signalen oppikken die kunnen duiden op ondermijnende activiteiten. Los van de vraag of ze hier zelf ook 'doelwit' van ondermijning zijn. Dat kan bijvoorbeeld ook gaan om beheerders of buitenmedewerkers die signalen oppakken.

Het (centraal) verwerken van signalen draagt bij aan het borgen van de meer systematische en eenduidige opvolging van signalen (zoals doormelden aan de politie) en versterkt de informatiepositie. Voor de provincie geven de patronen in signalen indicaties of bepaalde delen van de organisatie mogelijk extra risico lopen en er maatregelen moeten worden getroffen.

### **11.3 Aanbeveling 3: versterk de functie van HRM**

Weerbaarheid is op dit moment geen onderdeel van het taakgebied van HRM. Dat zien we als een gemis. Het advies is om die functie te versterken en bij HRM – in samenspraak met SBA en mogelijk het RIEC - de volgende taken onder te brengen:

1. Opstellen en realiseren van het programma ter vergroting van het bewustzijn en persoonlijke weerbaarheid van medewerkers.
2. Het in de strategische personeelsplanning meenemen wat toekomstige eisen zijn die aan (de competenties, kennis en vaardigheden) aan medewerkers moeten worden gesteld, in elk geval op de meest kwetsbare functies.
3. Het integreren van de persoonlijke weerbaarheid in het HRM-instrumentarium bij instroom (functieomschrijvingen, screenings), doorstroom (b.v. naar kwetsbare functie), evaluatie ("het goede gesprek"), ontwikkeling (zoals weerbaarheidstraining) en uitstroom.

### **11.4 Aanbeveling 4: voer een APK-controle meest kwetsbare processen uit**

De vierde aanbeveling is een 'onderhoudsprogramma kwetsbare processen' door te voeren. Dit aanhakend op het project 'processen centraal'. De belangrijkste aandachtspunten daarbinnen zijn:

1. Inventarisatie van de kwetsbare functies in de organisatie en treffen maatregelen, met name wat betreft functies in combinatie met:
  - langdurige relaties met marktpartijen (functieroulatie)
  - langdurige inhuur (screenings, autorisaties)
  - omgaan met vertrouwelijke informatie (digitale weerbaarheid, autorisaties)
2. Borgen van cross-compliance financiële processen (subsidies, investeringen aanbestedingen) en processen toezicht en handhaving.
3. Toevoegen ondermijningsrisico's aan de interne controles op de meest kwetsbare functies en processen.
4. Screening organisatie op risico's informatielekken door structurele thuiswerksituatie ten gevolge van de COVID-19 maatregelen.

### **11.5 Aanbeveling 5: haak de weerbaarheid van verbonden partijen aan**

De vijfde en laatste aanbeveling betreft borgen van de weerbaarheid in het samenspel tussen provincie en verbonden partijen. Dit met als belangrijkste punten:

1. Verlang van de verbonden partijen minimaal dezelfde 'standaarden' als voor de weerbaarheid van de provincie zelf. Vraag in de jaarrapportages ook verantwoording over de weerbaarheidsmaatregelen.
2. Organiseer ervaringsuitwisseling; verbonden partijen zijn ook zelf bezig met weerbaarheid.
3. Zorg voor voldoende cross-compliance (b.v. VTH en investeringen, subsidies etc) en benut elkaars informatiepositie, instrumenten en bevoegdheden (zoals Bibob) bij de aanpak van ondermijning én het (daarmee) ook samen weerbaarder zijn.



## BIJLAGEN

## Bijlage 1: Onderzoeksmodel

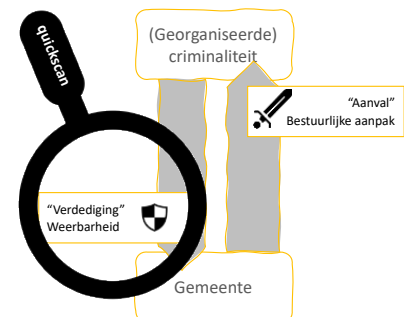
Georganiseerde criminaliteit kan alleen bestaan bij de gratie van diensten van de 'bovenwereld'. Dat kan gaan om vergunningen, toegang tot regulier bankverkeer en het beschikken over legale 'productiemiddelen' (panden, transportmiddelen, grondstoffen, facilitators). Het kan ook gaan om het kweken van 'goodwill' om geaccepteerd te worden in de samenleving waardoor het moeilijker wordt om gunsten te weigeren. Die verwevenheid van onderwereld en bovenwereld wordt aangeduid als *ondermijning*. Overheden krijgen grosso modo op twee manieren te maken met georganiseerde criminaliteit en ondermijning.

### BESTUURLIJKE AANPAK ONDERMIJNING ("AANVAL") ....

De eerste wijze waarop de provincie te maken kan hebben met de georganiseerde criminaliteit is dat het actief barrières kan opwerpen tegen criminelen, bijvoorbeeld door te voorkomen dat criminelen vergunningen krijgen waardoor ze legale bedrijven kunnen gebruiken voor witwaspraktijken, mensenhandel of drugshandel. Dit gebeurt samen met politie, justitie, belastingdienst, woningcorporaties etc. Samenwerking vindt vaak plaats in RIEC-verband. De burgemeester speelt daarbij een belangrijke rol. In de ambtelijke organisatie is vaak een coördinator of afdeling openbare orde en veiligheid (OOV) verantwoordelijk voor die bestuurlijke aanpak van de georganiseerde criminaliteit.

### .... EN WEERBAARHEID ORGANISATIE ("VERDEDIGING")

Tegenover de 'aanval op' georganiseerde criminaliteit staat in de tweede plaats de 'verdediging tegen' georganiseerde criminaliteit. *Daar richt deze methodiek zich op*. De provincie en haar medewerkers kunnen zelf doelwit zijn van ondermijning. Vooral bij zogenaamde 'kwetsbare processen' als vergunningverlening, toezicht en handhaving, grondtransacties, financieel verkeer, inkoop, opdrachtverlening, verstrekken van reisdocumenten, subsidies of zorg, werk en inkomen. Ondermijning kan op slinkse wijze plaatsvinden waarbij de provincie niet in de gaten heeft dat ze met criminelen te maken heeft. Denk aan een aanvraag voor een drank- en horecaverunning om de horecagelegenheid te gebruiken voor het witwassen. Soms gaat het ook minder subtiel en wordt getracht om via verleidingen, manipulatie en intimidatie of zelfs regelrechte bedreigingen of geweld, beslissingen te beïnvloeden of informatie los te krijgen.

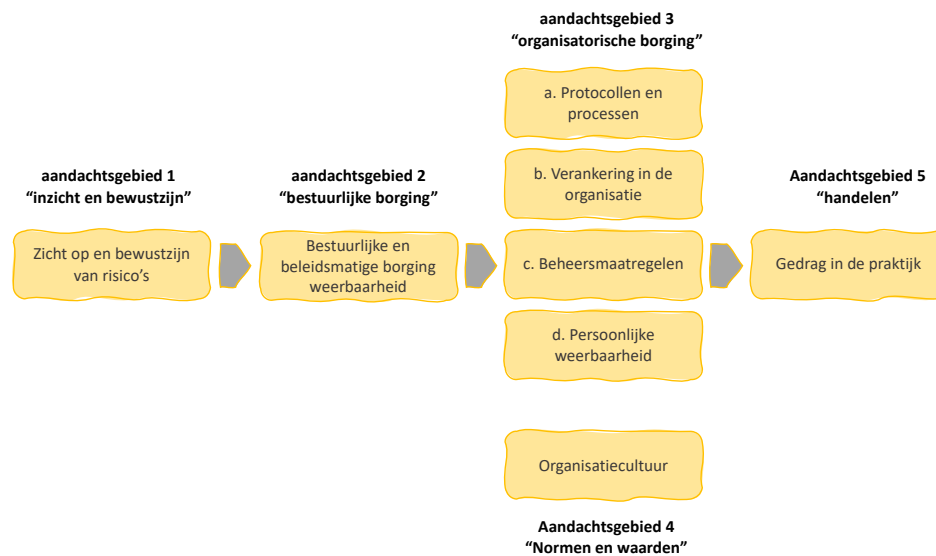


### AANDACHTSGEBIEDEN WEERBAARHEID IN HET ONDERZOEK

De provincie moet weerbaar zijn tegen pogingen tot beïnvloeding met een crimineel oogmerk. Weerbaarheid betreft de wijze waarop de provincie en haar medewerkers in staat zijn ondermijningspogingen te 'neutraliseren'. De methodiek gaat er in het kort vanuit dat een weerbare organisatie de volgende kenmerken heeft:

1. Bewustzijn van de mogelijke aanwezigheid van criminele activiteiten en van wat mogelijke kwetsbaarheden in de uitvoering van taken zijn.
2. Integriteit en weerbaarheid van de organisatie zijn als bestuurlijke prioriteit (portefeuille binnen het college, beleid geformuleerd, middelen beschikbaar) vastgelegd.
3. Het borgen van de weerbaarheid (waaronder integriteit) van de organisatie door onder meer het vastleggen van kwetsbare processen en integriteitsregels, ondersteuning voor medewerkers, bijzondere aandacht voor kwetsbare functies, bieden van veiligheid etc.

4. Een organisatiecultuur die open is voor wat betreft integriteit maar ook duidelijke normen stelt.
5. Een handelen gericht op het ook feitelijk melden én oppakken van signalen die kunnen duiden op ondermijning of integriteitsschendingen.



Deze vijf aandachtsgebieden vormen de kern van het onderzoek. Voor elk is in beeld gebracht wat de provincie formeel heeft geregeld en georganiseerd en hoe dit in de praktijk werkt. Het laatste is in beeld gebracht op basis van interviews, toegespitst op de meest kwetsbare processen en een digitale vragenlijst die is uitgezet onder de medewerkers.

De focus in het onderzoek ligt op de zogenaamde 'kwetsbare processen'. Dit zijn werkprocessen, handelingen of functies die potentieel doelwit kunnen zijn van criminelen.

<b>Financiële transacties</b>	<ul style="list-style-type: none"> <li>- Betalingen in de vorm van declaraties (facturering)</li> <li>- Innen belastingen, boetes, verkopen, leges etc.</li> <li>- Subsidies, sponsoring etc.</li> </ul>
<b>Opdrachtverlening (aanbesteding, projecten, etc.)</b>	<ul style="list-style-type: none"> <li>- Opstellen beoordelingskaders</li> <li>- Procedure aanbesteding bepalen</li> <li>- Aanvragen en beoordelen offertes</li> <li>- Voeren onderhandelingen</li> <li>- Beoordelen offertes</li> <li>- Toekennen opdracht/instemmen zorg/inkomen (mandaat?)</li> <li>- Toestaan meerwerk</li> </ul>
<b>Vergunningen, toestemmingen en ontheffingen</b>	<ul style="list-style-type: none"> <li>- Beoordelingscriteria en toepassing daarvan</li> <li>- Procedure beoordelen/controleren aanvraag/aanvrager (incl Bibob, legitimatie etc.)</li> <li>- Advies en toekenning (mandaat?)</li> </ul>
<b>Inkoop goederen en diensten</b>	<ul style="list-style-type: none"> <li>- Besluiten tot inkoop of inhuur (mandaat?)</li> </ul>
<b>Omgaan met vertrouwelijke informatie</b>	<ul style="list-style-type: none"> <li>- Voorkennis (RO, investeringen, budgetten, verordening, strategie aanpak ondermijning etc.)</li> <li>- Beheren en delen vertrouwelijke informatie</li> <li>- Beheren en delen persoonsgegevens</li> </ul>
<b>Toezicht en handhaving</b>	<ul style="list-style-type: none"> <li>- Prioriteitstelling</li> <li>- Vaststellen overtredingen/naleefgedrag</li> <li>- Registratie daarvan</li> <li>- Opleggen sanctie</li> <li>- Innen en kwijtschelden boetes?</li> </ul>

Het doel van criminelen kan daarbij zijn:

- Toegang krijgen tot financiële middelen (subsidies, inkoop etc.).

- Toegang krijgen tot strategische informatie (welke investeringen gaat de provincie doen? Voorinformatie aanbestedingen etc) of persoonsinformatie.
- Rechten krijgen, b.v. in de vorm van vergunningen die nodig zijn om een legale basis te krijgen voor criminele activiteiten, bijvoorbeeld milieuvergunningen.
- Toegang krijgen tot vastgoed (mensenhandel, drugslab etc.).
- Bewerkstelligen dat 'een oogje wordt dichtgeknepen' bij toezicht en handhaving.

Beïnvloeding kan zowel subtiel (misleiding, verleiding) maar ook door intimidatie, manipulatie of (dreigen met) geweld.