De SIRA uitvoeren in Normavix

Van integriteitsdoelstelling naar aantoonbaar ‘in control’ met een iteratief SIRA-stelsel, ingebouwde bewijsvoering, realtime monitoring en directe sturing op integriteitsrisico’s.

normavix

Evolving compliance into intelligence

Leeswijzer en scope

Deze White paper beschrijft hoe Normavix de inrichting en werking van een SIRA (Systematische Integriteitsrisicoanalyse) faciliteert.

Normavix levert structuur, workflows, dashboards en aantoonbaarheid; professioneel oordeel, beleidskeuzes, inrichting en uitvoering blijven bij de organisatie. Voorbeelden zijn illustratief en moeten worden afgestemd op omvang, type dienstverlening, IT-landschap en risicoprofiel.

Noot: deze SIRA-White paper sluit inhoudelijk aan op de Controls OS-methodiek zoals beschreven in de White paper over SKM1/ ISQM 1.

Inhoud

Executive summary

Integriteitsrisico’s raken de kern van vertrouwen in de accountancy: beroepsethiek (VGBA/ViO), privacy, Wwft/AMLR, NOCLAR en aanpalende risicogebieden zoals cyber, datalekken en grensoverschrijdend gedrag.

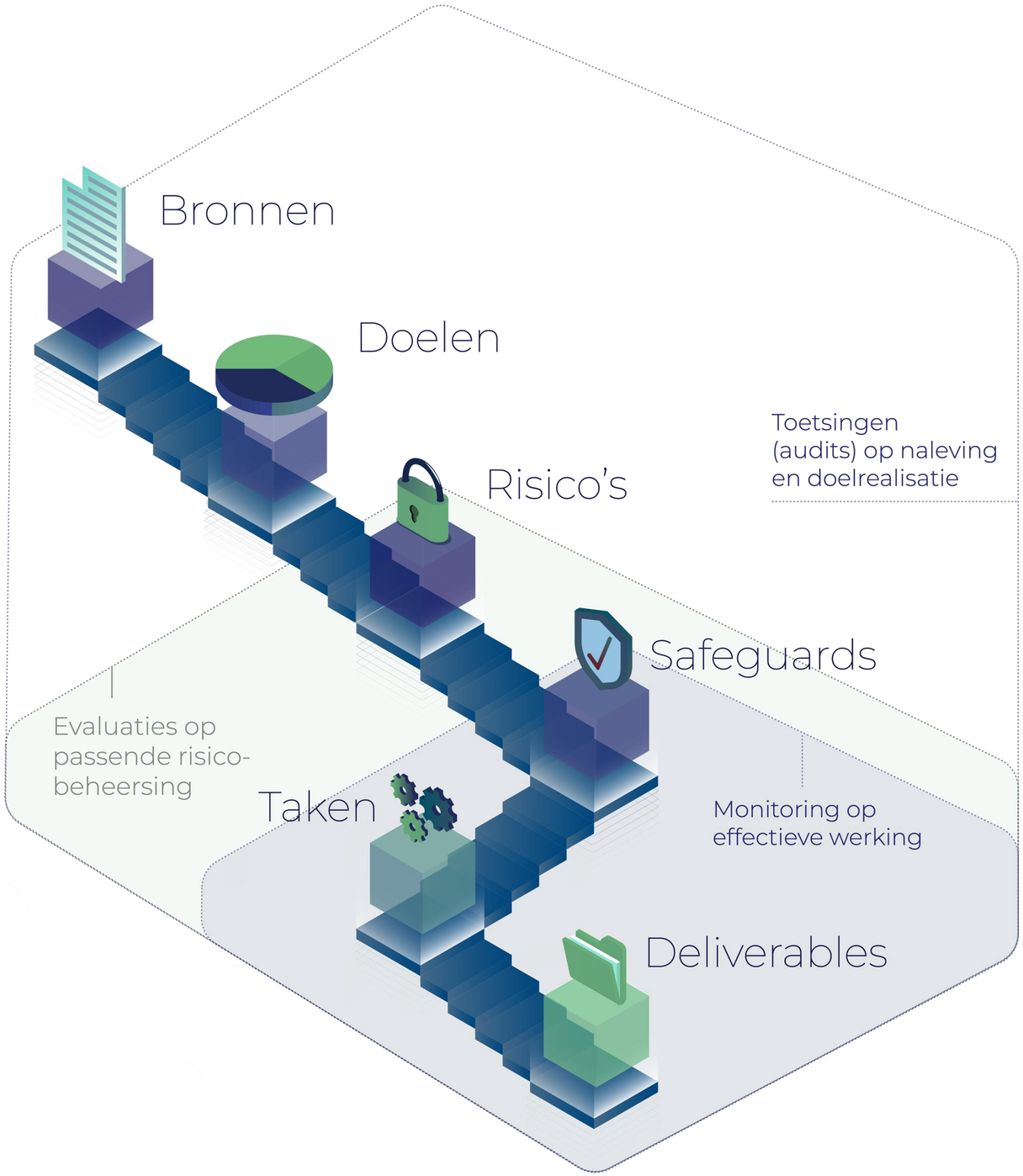
In veel organisaties zijn deze onderwerpen versnipperd over losse documenten, registers en is er sprake van incident gedreven acties. Het gevolg: onduidelijk eigenaarschap, beperkte samenhang en bewijs dat pas achteraf nog moet worden verzameld, leiden tot stressvolle situaties.

De SIRA (systematische integriteitsrisicoanalyse) is een instrument om risico’s te beheersen. Normavix maakt de SIRA bestuurbaar en aantoonbaar door integriteitsrisico’s te organiseren als één governance-keten.

De SIRA steunt op dezelfde Controls OS-methodiek als het kwaliteitsstelsel onder SKM 1/ISQM 1, maar met een ander object: integriteitsdoelen en integriteitsrisico’s. Deze worden gepresenteerd op een eigen heatmap en dashboards, naast kwaliteits- en businessrisico’s. Zo ontstaat één integrale governance-omgeving, met gescheiden stuurinformatie per risicodomein.

01

De kern van de SIRA in Normavix



- De SIRA werkt als geïntegreerd stelsel van doelen, risico's en maatregelen met gekoppelde 'test of controls' of risico evaluaties
- Normavix gebruikt dezelfde kwaliteitsrichtlijnen uit SKM1/ ISQM 1, maar dan toegepast op integriteitsdomeinen.
- Integriteit is hiermee eveneens een lerend systeem (onderdeel van de PDCA-cyclus).
- Integriteitsrisico's krijgen een eigen heatmap en dashboards, naast kwaliteits- en businessrisico's.
- Bewijs ontstaat tijdens de uitvoering (workflow, logging, sign-off), niet via reconstructie achteraf.
- Triggers (incidenten, meldingen, NOCLAR, Wwft-tekortkomingen) leiden tot herbeoordelingen.
- Wwft en AMLR-risico's zoals het dienstverleningsverbod worden concreet beheerst via CRA Engine (KYC-workflow met checks & balances).
- Output is altijd toetsbaar en gekoppeld aan de workfow (doelen, risico's en maatregelen).

02

Waarom een goede SIRA-uitvoering nu belangrijk is

De norm- en toezichtdruk neemt toe, maar ook de operationele druk. Meer data, meer uitbesteding, complexe ketens en meer afstemming vergroten de kans op tekortkomingen. Tegelijk blijft de bestuurlijke vraag hetzelfde: wat zijn onze grootste integriteitsrisico's, welke beheersing staat daarop, en zijn we aantoonbaar in control?

Een SIRA is voor accountantskantoren weliswaar niet expliciet verplicht maar wel sterk aanbevolen, mits deze ook van betekenis is en als stuurmechanisme wordt gebruikt (zoals in SKM1). Een SIRA die eindigt als "document" mist vaak ritme, eigenaarschap en bewijswaarde. Een SIRA als stelsel maakt integriteit juist bestuurbaar.

03

SIRA als stelsel: wat het wél en niet is

Een SIRA is geen jaarlijkse “compliance-oefening” en geen checklist in Excel.

Een volwassen SIRA levert minimaal:

- Integriteitsdoelen en -risico’s per domein (met eigenaarschap)
- Integriteitsheatmap met prioriteiten en risk appetite (periodieke update)
- Controls per top-risico (incl. eigenaar en verwachte werking)
- Monitoringritme met bevindingen, herstel en effect (intensiteit afhankelijk van risico)
- Bestuurlijke evaluatie (‘in control’) met herleidbare onderbouwing (periodiek, met jaarlijkse integriteitsconclusie)

1. Waar zitten onze belangrijkste integriteitsrisico’s?

2. Welke controls hebben we ingericht en wie is eigenaar?

3. Zijn we aantoonbaar in control en wat verbeteren we waar dat nodig is?

04

Normavix als fundament van de SIRA

Normavix ondersteunt de SIRA als één doorlopende structuur:

- **Integriteitsdoelen:** doelen per domein (of gekoppeld aan SKM 1-componenten), met normreferenties (VGBA, AVG, Wwft/AMLR, NOCLAR).
- **Integriteitsrisico's:** risico's gekoppeld aan doelen, met bruto-inschatting (kans × impact) en vastgelegde risk appetite.
- **Controls:** maatregelen gekoppeld aan risico's, met eigenaarschap, scope en verwachte werking.
- **Monitoring:** monitoringactiviteiten gekoppeld aan controls; bevindingen worden direct aan het onderliggende integriteitsrisico gekoppeld.
- **Evaluatie:** risico-evaluaties brengt het nettorisico in beeld (restrisico na beheersing)
- **Herstel & opvolging:** herstelmaatregelen als taken/activiteiten met deadlines en rollen (uitvoerder, controleur, autorisatie).
- **Inzicht:** integriteits-heatmap en dashboards met drill-down naar evidence en status.

Normavix kent de volgende modules of (virtuele) werkplaatsen:

- **CRA Engine:** cliëntdossier, acceptatie/continuering, dienstprofielen, scenario's en workflow
- **Controls OS:** beleid/controls-structuur (waar relevant voor KYC-maatregelen en monitoringinrichting)
- **GRC Insights:** realtime dashboards, voortgang, risicoclassificaties en evidence drill-down
- **AssureDesk:** werkplek voor bureau vaktechniek, werken aan geprioriteerde taken
- **Compliance Ops:** monitoring, bevindingen, opvolging en herstel (operationele sturing)
- **Boardroom:** besluitvorming, escalaties en sign-off (governance-ritme)
- **Guidance Centre:** beleid/werkinstructies, versiebeheer en rechten
- **Feedback Hub:** signalen/meldingen koppelen aan risico's en herbeoordeling

Normavix garandeert geen compliance of integriteit. Het biedt de **voorwaarden** om doelen, risico's, controls, monitoring en bewijsvoering samenhangend in te richten en te besturen. De uiteindelijke inrichting, uitvoering en oordeelsvorming blijven de verantwoordelijkheid van de organisatie.

05 Integriteitsdomeinen: één stelsel, meerdere thema's

Integriteit bestrijkt meerdere domeinen met elk hun eigen dynamiek, zoals:

- **Beroepsethiek en gedrag** (VGBA, ViO, cultuur, grensoverschrijdend gedrag)
- **Privacy en informatie** (AVG, datalekken, autorisaties)
- **AML en CEAC** (Wwft/AMLR, dienstverleningsverbod, cliëntintegriteit)
- **NOCLAR en escalatie** (signalering en opvolging)
- **Cyber en continuïteit** (dreigingen en incident response)

Binnen Normavix maken we expliciet onderscheid tussen twee toepassingen die in de praktijk vaak door elkaar lopen:

1. SIRA voor het kantoor (interne integriteit)
   De SIRA beschrijft de integriteitsdoelen en integriteitsrisico's van de eigen organisatie (bijv. VGBA/ViO, NOCLAR, cyber, cultuur). Daarop worden controls, monitoring, bevindingen, herstel en de periodieke evaluatie 'in control' ingericht en aantoonbaar gemaakt.

3. Risicobereidheid voor cliënten en relaties (cliënt-/relatierisico)
   Veel accountantskantoren hanteren óók een "SIRA-achtige" benadering richting cliënten: welk type cliënt of relatie past bij het kantoor, welke risicocategorieën accepteren we, welke escalatie- en stopcriteria gelden, en hoe leggen we dat consistent vast. Dit is strikt genomen geen interne SIRA, maar een risicomodel voor acceptatie en continuering.

Normavix ondersteunt dit onderscheid bewust, omdat het andere objecten, workflows en beslismomenten kent. De risicobereidheid voor cliënten en relaties wordt daarom geconfigureerd in de CRA Engine: je stelt daar eenvoudig de risicocategorieën, acceptatiegrenzen, escalatieroutes en stopcriteria per dienst in.

Cliënt- en opdrachtacceptatie

Met de configuratie van de risicobereidheid stuur je vervolgens de acceptatie- en continueringflow (inclusief dossiervorming en besluitvastlegging), zodat cliënt-/ relatierisico's consistent en aantoonbaar worden beoordeeld, zonder dat dit wordt vermengd of verward met de interne SIRA van het kantoor.

06 Doelenstructuur bepalen (twee opties)

Er zijn twee opties om integriteitsdoelen onder te brengen:

Optie 1: Integriteitsdoelen koppelen aan SKM 1-componenten

Kies dit als je één governance-taxonomie wilt en rapportage maximaal uniform moet zijn.

Optie 2: Eigen integriteitsdoelcategorieën per domein bepalen

Kies dit als je integriteit herkenbaar wilt organiseren, afzonderlijk van de componenten van SKM1.

In Controls OS configureer je eenvoudig je eigen doelenstructuur of portfolio's waarmee je inzicht en overzicht creëert zoals je het wil. De risico's gekoppeld aan kwaliteitsdoelen, Integriteitsdoelen en businessdoelen worden altijd in aparte secties gepresenteerd op heatmaps in **GRC Insights**.

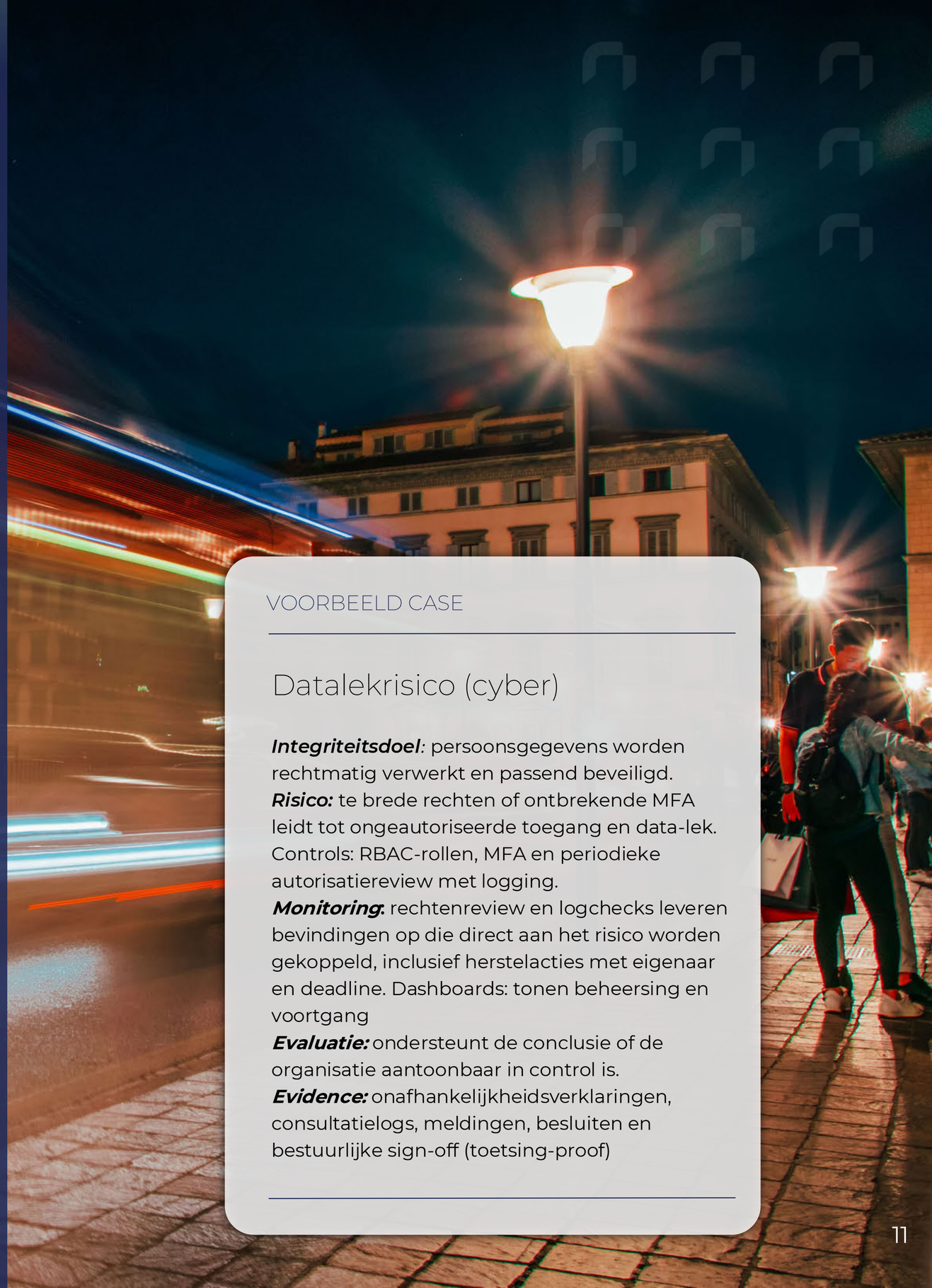
07

Risico-identificatie en scoring: de integriteitsheatmap

Integriteitsrisico’s worden beoordeeld met bruto-inschatting (kans × impact) en vervolgens geprioriteerd aan de hand van de risk appetite. De uitkomsten zijn integriteitsheatmaps die de toprisico’s inzichtelijk maken en de prioriteiten over alle risico’s ten behoeve van een al dan niet noodzakelijke respons.

Respons-principes:

Top-risico’s (hoog of boven appetite) kun je directe prioriteit geven voor beheersing; middengebied wordt gemonitord en geoptimaliseerd; lage risico’s worden expliciet geaccepteerd met rationale en eventuele basiscontrols (optioneel).



VOORBEELD CASE

Datalekrisico (cyber)

Integriteitsdoel*:* persoonsgegevens worden rechtmatig verwerkt en passend beveiligd.
Risico: te brede rechten of ontbrekende MFA leidt tot ongeautoriseerde toegang en data-lek. Controls: RBAC-rollen, MFA en periodieke autorisatiereview met logging.
Monitoring: rechtenreview en logchecks leveren bevindingen op die direct aan het risico worden gekoppeld, inclusief herstelacties met eigenaar en deadline. Dashboards: tonen beheersing en voortgang
Evaluatie: ondersteunt de conclusie of de organisatie aantoonbaar in control is.
Evidence: onafhankelijkheidsverklaringen, consultatielogs, meldingen, besluiten en bestuurlijke sign-off (toetsing-proof)

08

Controls & monitoring: evidence by design

In Normavix worden controls uitvoerbaar gemaakt: eigenaarschap, scope, taken/activiteiten, deadlines, controle en autorisatie.

Controls worden gekoppeld aan monitoringactiviteiten, zodat bewijs tijdens uitvoering ontstaat.

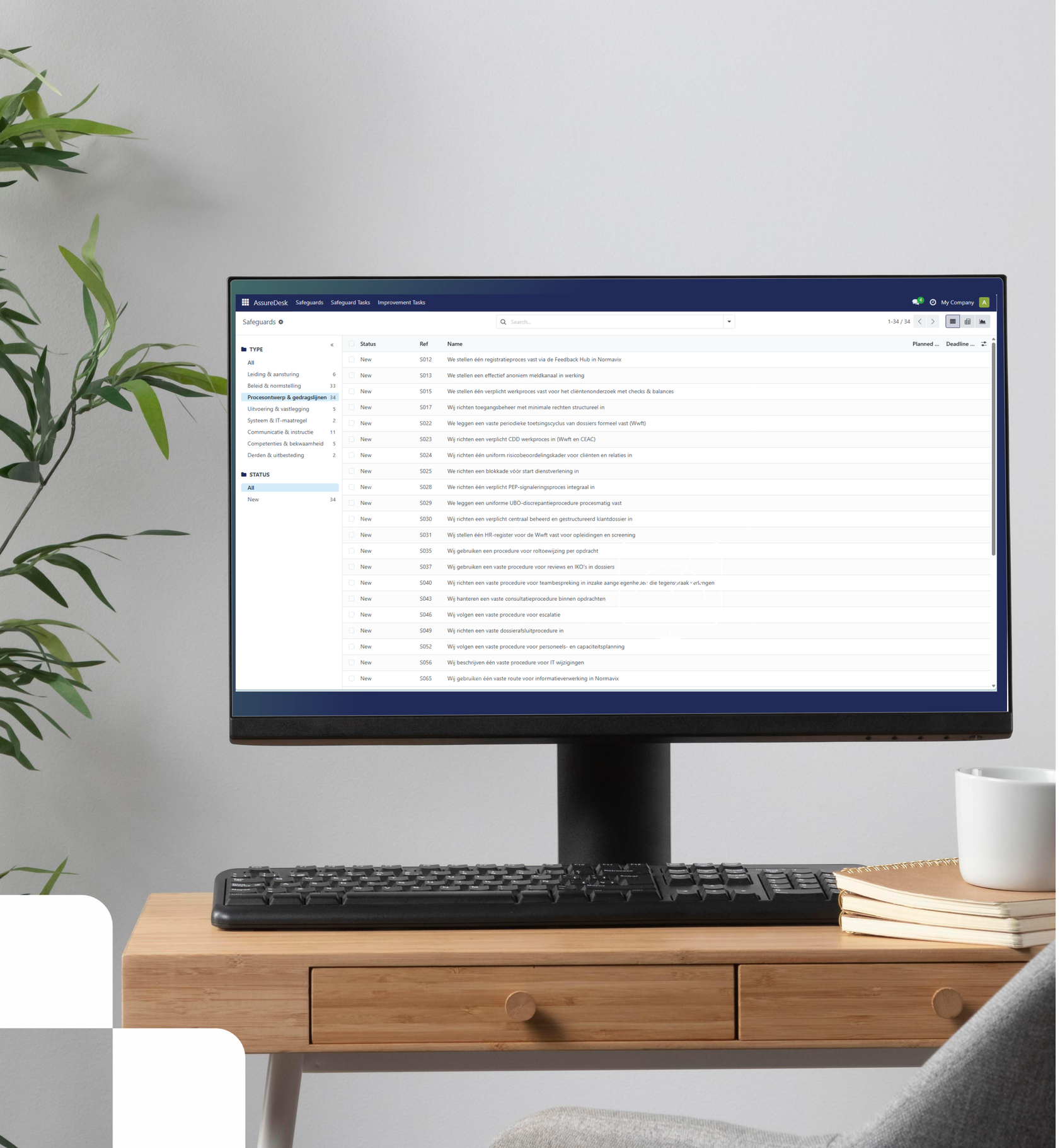
Bevindingen worden direct aan het integriteitsrisico gekoppeld en leiden tot herstelmaatregelen die aan het risico zijn gekoppeld. Zo ontstaat een gesloten loop: tekortkoming → herstel → effect.
Alles is zichtbaar in de interface, op het dashboard en opvolgagenda's (bijvoorbeeld van AssureDesk).

09

Triggers, signalen en incidenten: SIRA als lerend systeem

De SIRA behoort gevoelig te zijn voor signalen:

Datalekken, meldingen, klachten, NOCLAR-cases, Wwft-tekortkomingen of cyber-incidenten. Normavix ondersteunt het lerend vermogen door signalen te registreren (Feedback Hub) en direct te koppelen aan het relevante integriteitsrisico. Dat triggert herbeoordeling van het risico, aanpassing van controls of intensivering van monitoring, waardoor incidenten structureel verbeteren en niet “los” blijven.



10

Integriteit zichtbaar in besluitvorming

Normavix maakt integriteit bestuurbaar via rolgerichte sturing:

- **Compliance Ops** voor monitoring, bevindingen en herstelopvolging
- **AssureDesk** waar vaktechniek/beleid betrokken is bij (her)inrichting van controls
- **Boardroom** voor besluitvorming, escalaties en periodieke evaluatie
- **GRC Insights** voor realtime dashboards en drill-down naar evidence

11 Integriteitsmapping

Onderstaande mapping geeft per integriteitsdomein een compacte “bouwtekening”: doel, kernrisico’s, controls en monitoring/evidence (als voorbeeld). Eigenaar-tags vergroten directe bestuurbaarheid.

Domein	Integriteits-doel (kort)	Kernrisico’s (voorbeelden)	Controls	Monitoring/ evidence
Privacy & informatie (AVG) (Eigenaar: FG/IT)	Rechtmatig + passend beveiligd	Data-lek (rechten/MFA/koppelingen); bewaartermijnfout	Rollen, MFA, autorisatiereview	Logreview autorisaties, incidentlog + herstel
Cyber & continuïteit (Eigenaar: IT/Security)	Weerbaar & beschikbaar	Ransomware/phishing; back-up faalt	Patchmanagement, EDR, restore-tests	Patch-compliance, restore-test bewijs, incidentrapport
AML (Wwft/AMLR) (Eigenaar: Compliance)	Dienstverlening binnen AML-kaders	Onvoldoende CDD → dienstverleningsverbod; te late reviews	CRA-workflow, stop-/escalatiecriteria, periodieke reviews	CDD-dossiertoetsing, steekproef stop-criteria, review-timelines
Beroepsethiek & gedrag (VGBA/ViO) (Eigenaar: HR/ Compliance)	Volgens beroeps-regels	Belangenconflict; ongewenst gedrag	Gedragscode/meldproces, Independence checks, consultatie	Meldingen-register, onafhankelijk-heids-check log, traininglog
NOCLAR & escalatie (Eigenaar: Vaktechniek/ Compliance)	Signaleren en opvolgen	Signalen gemist; slechte vastlegging	NOCLAR-protocol, consultatie, besluitvorming + rationale	Casuslog, besluit-/ consultatielog, dossier-review

12

Documentatie en aantoonbaarheid

Een SIRA moet aantoonbaar maken wat voor de organisatie belangrijk is om na te streven en na te leven, hoe risico's zijn beoordeeld, welke controls zijn gekozen, wat is gemonitord, welke tekortkomingen zijn hersteld en wat de status is.

Normavix ondersteunt dit met audit-trails, logging en evidence per ketenstap, plus automatische rapportages per domein en organisatie breed. Deze worden rechtstreeks gekoppeld aan uitgevoerde taken en de beheersmaatregel. Of worden centraal opgeslagen in het Q&E Library.

Dit alles neem aanzienlijke tijds- en kostenbespraringen met zich mee en brengt de kwaliteit van doelrealisatie naar het optimale niveau.

VOORBEELD CASE

Dienstverleningsverbod (Wwft) bij onvoldoende KYC (CDD)

Integriteitsdoel: dienstverlening vindt uitsluitend plaats als het cliëntenonderzoek adequaat is uitgevoerd en vastgelegd.
Risico: onvoldoende KYC/CDD leidt tot onterecht aangaan van dienstverlening (schending dienstverleningsverbod) en verhoogde integriteits- en toezichtrisico's.
Controls: CRA-workflow (via CRA Engine), stop-/ escalatiecriteria en periodieke reviews. Werkprincipe: zonder afgerond KYC-proces volgt blokkade en eventueel besluit tot stopzetting dienstverlening.
Monitoring: dossiertoetsing en steekproeven op stop-criteria leveren bevindingen op die direct aan het risico worden gekoppeld, met herstelacties tot afronding. Dashboards tonen status en trends; Evaluatie ondersteunt een onderbouwde conclusie 'in control'.

13 Implementatie in 5 stappen (SIRA-stelselopzet)

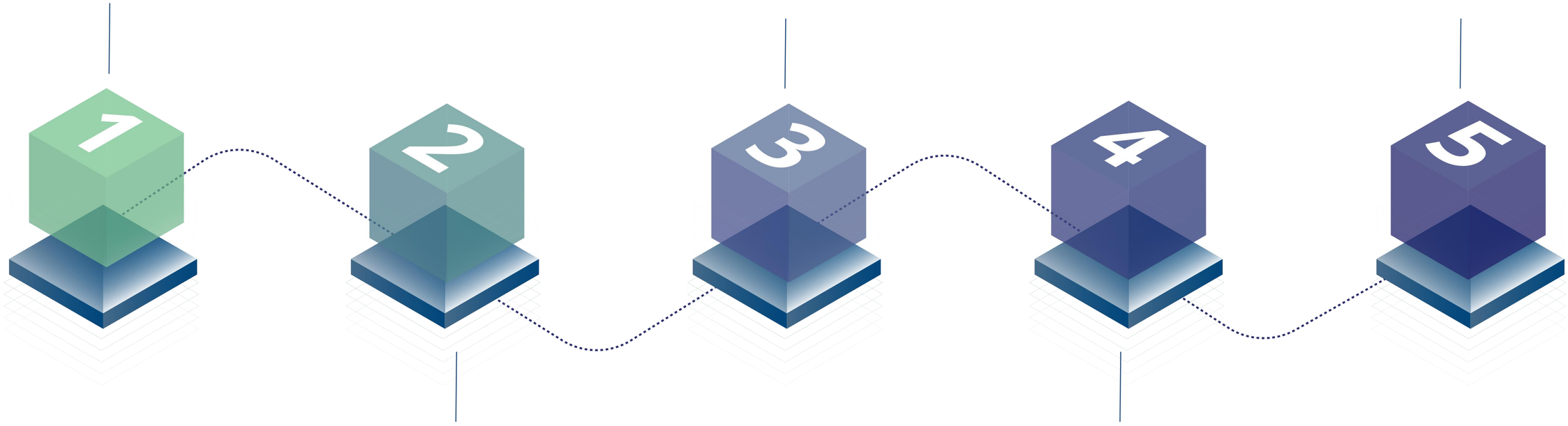
1. Bepaal integriteitsdomeinen en formuleer integriteitsdoelen en risico’s.

2. Identificeer top-risico’s, score (kans×impact) en bepaal de risk appetite.

3. Ontwerp Safeguards per top-risico en leg verwachte werking vast.

4. Richt monitoringritme en evidence in (bevinding > herstel > effect).

5. Borg Boardroom-evaluatie: besluiten, escalaties en periodieke ‘in control’-conclusie.



14

Conclusie

Integriteitsrisico’s vragen om een stelselmatige aanpak die bestuurbaar, uitvoerbaar en aantoonbaar is.

Normavix organiseert de SIRA als een gesloten governance-keten met eigen heatmaps en dashboards voor integriteitsrisico’s, zonder dat integriteit los komt te staan van kwaliteits- en businesssturing. De methode is consistent, de stuurinformatie is gescheiden, en de uitkomst is helder: integriteit wordt een continu proces met bewijs dat ontstaat tijdens uitvoering. Een goed ingerichte SIRA biedt rust, zekerheid en efficiency.

Wil je snel scherp krijgen hoe jullie SIRA er in Normavix uit kan zien?

Vraag een SIRA-demo aan: in één sessie brengen we integriteitsdomeinen, een eerste top-3 integriteitsrisico’s en een passende set controls/monitoring in kaart, als startpunt voor jullie integriteitsheatmap en governance-ritme.

Plan een live demo

www.normavix.com | info@normavix.com | +31 85 401 84 52