Organisatiegedrag

Topical Requirement

Gebruikershandleiding

The Institute of Internal Auditors

Vertaald door

Instituut van Internal Auditors Nederland

Inhoud

Overzicht van Topical Requirements[1]

Topical Requirements vormen een essentieel onderdeel van het International Professional Practices Framework®, samen met de Global Internal Audit Standards™ en de Global Guidance. Het Instituut van Internal Auditors vereist dat de Topical Requirements worden gebruikt in combinatie met de Global Internal Audit Standards, die de gezaghebbende basis vormen voor de beroepspraktijk. Verwijzingen naar de Standaarden zijn in deze gebruikershandleiding opgenomen als bron van meer gedetailleerde informatie.

Topical Requirements formaliseren hoe internal auditors omgaan met veelvoorkomende risicogebieden om kwaliteit en consistentie binnen de beroepsgroep te bevorderen. Het mandaat van de internal auditfunctie bepaalt duidelijk de reikwijdte en de soorten diensten die door de internal auditfunctie worden uitgevoerd, waarbij ook rekening wordt gehouden met Topical Requirements(Standaard 6.1 Internal auditmandaat). Topical Requirements leggen een basis en bieden relevante criteria voor het uitvoeren van assurancediensten met betrekking tot het onderwerp van een Topical Requirement (Standaard 13.4 Evaluatiecriteria). Conformiteit met de Topical Requirements is verplicht voor assurancediensten en wordt aanbevolen voor evaluatie tijdens adviesdiensten. Topical Requirements zijn niet bedoeld om alle mogelijke aspecten te omvatten waarmee rekening moet worden gehouden bij het uitvoeren van assurance-opdrachten; ze zijn eerder bedoeld om een minimale set vereisten te bieden om een consistente, betrouwbare beoordeling van het onderwerp mogelijk te maken.

De Topical Requirements sluiten duidelijk aan bij het Three Lines Model van het IIA en bij de Global Internal Audit Standards. Governance-, risicomanagement- en beheersprocessen zijn de belangrijkste onderdelen van de Topical Requirements ,die aansluiten bij Standaard 9.1 Inzicht in governance-, risicomanagement- en beheersprocessen. In verwijzing naar het Three Lines Model, is governance gekoppeld aan het bestuur/het bestuursorgaan, risicomanagement aan de tweede lijn en beheersing of beheersprocessen aan de eerste lijn. Terwijl het management vertegenwoordigd is in zowel de eerste als de tweede lijn, wordt de internal auditfunctie weergegeven in de derde lijn als een onafhankelijke en objectieve leverancier van zekerheid, die rapporteert aan het bestuur/het bestuursorgaan (Principe 8 Onder toezicht van het bestuur).

---

[1] *Deze vertaling is met de grootste zorgvuldigheid uitgevoerd, maar bij discussie over de vertaling en in het kader van het CIA -examen is de originele, Engelstalige tekst van toepassing. In deze vertaling zijn Engelse termen behouden voor woorden die in het spraakgebruik ingeburgerd zijn danwel tot mogelijke onduidelijkheid zouden leiden bij een vertaling.*
Voor deze vertalingen geldt het Auteursrecht.

Toepasbaarheid, risico en professionele oordeelsvorming

Topical Requirements moeten worden nageleefd wanneer internal auditfuncties assurance-opdrachten uitvoeren met betrekking tot onderwerpen waarvoor een Topical Requirement bestaat of wanneer aspecten van de Topical Requirement worden geïdentificeerd binnen andere assurance-opdrachten.

Zoals beschreven in de Standaarden is het beoordelen van risico's een belangrijk onderdeel van de planning door het hoofd van de internal auditfunctie. Om te bepalen welke assurance-opdrachten in het internal auditplan moeten worden opgenomen, moeten de strategieën, doelstellingen en risico's van de organisatie ten minste jaarlijks worden beoordeeld (Standaard 9.4 Internal Auditplan). Bij het plannen van individuele assurance-opdrachten moeten internal auditors de risico's beoordelen die relevant zijn voor de opdracht (Standaard 13.2 Risicobeoordeling in de opdracht).

Wanneer het onderwerp van een Topical Requirement wordt geïdentificeerd tijdens het risicogebaseerde planningsproces van de internal audit en wordt opgenomen in het auditplan, dan moeten de in de Topical Requirement beschreven vereisten worden gebruikt om het topic binnen de van toepassing zijnde opdrachten te beoordelen. Bovendien, wanneer internal auditors een opdracht uitvoeren (al dan niet opgenomen in het plan) en elementen van een Topical Requirement naar voren komen, moet de Topical Requirement worden beoordeeld op toepasbaarheid als onderdeel van de opdracht. Tot slot, als een opdracht wordt aangevraagd die oorspronkelijk niet in het plan was opgenomen en het onderwerp bevat, moet de Topical Requirement worden beoordeeld op toepasbaarheid.

Professionele oordeelsvorming speelt een belangrijke rol bij de toepassing van de Topical Requirement. Risicobeoordelingen vormen de basis voor beslissingen van chief audit executives over welke opdrachten in het internal auditplan moeten worden opgenomen (Standaard 9.4). Daarnaast gebruiken internal auditors professionele oordeelsvorming om te bepalen welke aspecten binnen elke opdracht aan bod zullen komen (Standaard 13.3 Doel en reikwijdte van de opdracht, 13.4 Evaluatiecriteria en 13.6 Werkprogramma) en om de middelen te identificeren die nodig zijn om de doelstellingen van de opdracht te bereiken (Standaard 13.5 Middelen voor de opdracht).

Er moet bewijs worden bewaard dat elke vereiste in de Topical Requirement is beoordeeld op toepasbaarheid, met inbegrip van een motivering voor de uitsluiting van eisen. Conformiteit met de Topical Requirement moet worden gedocumenteerd op basis van de professionele oordeelsvorming van auditors zoals beschreven in Standaard 14.6 Documentatie van de opdracht.

Hoewel de Topical Requirement een basis geeft van beheersprocessen die moeten worden overwogen, moeten organisaties die het risicothema als zeer hoog beoordelen mogelijk aanvullende aspecten beoordelen.

Indien een hoofd van de internal auditfunctie vaststelt dat de internal auditfunctie niet over de vereiste kennis beschikt om auditopdrachten uit te voeren met betrekking tot een onderwerp van een Topical Requirement , kunnen de werkzaamheden worden uitbesteed aan een externe dienstverlener (Standaarden 3.1 Competentie, 7.2 Kwalificaties van het hoofd van de internal

auditfunctie, 10.2 Beheer van personele middelen). De Standaarden zijn van toepassing op elke persoon of functie die internal auditdiensten levert, ongeacht of een organisatie internal auditors rechtstreeks in dienst heeft, ze inhuurt via een externe dienstverlener, of beide. Het hoofd van de internal auditfunctie behoudt de eindverantwoordelijkheid voor het garanderen van conformiteit. Bovendien, als het hoofd van de internal auditfunctie vaststelt dat de internal audit middelen onvoldoende zijn, moet hij/zij het bestuur informeren over de impact van onvoldoende middelen en hoe eventuele tekorten aan middelen zullen worden aangepakt (Standaard 8.2 Middelen).

Prestaties, documentatie en rapportage

Bij het toepassen van Topical Requirements moeten internal auditors ook voldoen aan de Standaarden en hun werk uitvoeren in overeenstemming met Domein V: Uitvoeren van internal auditdiensten. De standaarden in domein V beschrijven het plannen van opdrachten (Principe 13 Plan Opdrachten Effectief), het uitvoeren van opdrachten (Principe 14 Voer opdrachtwerkzaamheden uit) en het communiceren van de resultaten van opdrachten (Principe 15 Communiceer opdrachtresultaten en monitor actieplannen).

Topical Requirements zijn bedoeld om consistente internal auditpraktijken van hoge kwaliteit te ondersteunen. Ze moeten worden toegepast in combinatie met van toepassing zijnde lokale wet- en regelgeving, verwachtingen van toezichthouders en andere professioneel erkende kaders, die aanvullende of meer specifieke vereisten kunnen opleggen. Internal auditors hebben mogelijk al werkprogramma's en testprocedures ontwikkeld op basis van deze voorschriften en kaders. Internal auditors dienen hun voorgenomen testen van de beheersing van het organisatiegedrag en eventuele betrouwbare testen door andere interne en externe assurance providers (Standaard 9.5 Coördinatie en vertrouwen) in overeenstemming te brengen met de Topical Requirement om een adequate dekking te waarborgen.

Dekking van de Topical Requirement kan worden gedocumenteerd in het internal auditplan of het werkprogramma van de opdracht op basis van het professionele oordeel van de auditors. Eén of meer internal auditopdrachten kunnen de vereisten afdekken. Daarnaast kan het zijn dat niet alle vereisten van toepassing zijn. Er moet bewijsmateriaal worden bewaard waaruit blijkt dat de onderhavige vereiste is beoordeeld op toepasbaarheid, met inbegrip van een motivering voor eventuele uitsluitingen.

Kwaliteit

De Standaarden vereisen dat het hoofd van de internal auditfunctie een programma voor kwaliteitsborging en -verbetering ontwikkelt, implementeert en onderhoudt dat alle aspecten van de internal auditfunctie omvat (Standaard 8.3 Kwaliteit). De resultaten moeten worden gecommuniceerd naar het bestuur en het senior management. In de communicatie moet worden gerapporteerd over de conformiteit van de internal auditfunctie met de Standaarden en het behalen van de prestatiedoelstellingen.

Overeenstemming met de Topical Requirements moet in overweging worden genomen in de supervisie op het niveau van de opdracht (Standaard 12.3 Toezicht op en verbetering van prestaties in opdrachten) en zal worden beoordeeld bij kwaliteitsbeoordelingen.

Organisatiegedrag

Herkaderen van het auditen van cultuur

De overgang van het beschouwen van het auditen van cultuur als een abstract en vaag onderwerp naar een gestructureerde en precieze beoordeling van organisatiegedrag is een noodzakelijke en tijdige evolutie binnen het vakgebied van de internal audit. Ondanks de wijdverspreide erkenning dat culturele tekortkomingen vaak aan de basis liggen van significante tekortkomingen op het gebied van beheersing, heeft dit gebied geen significante aandacht gekregen in de internal auditpraktijk. Het opnieuw framen van het auditen van "cultuur" als het auditen van "organisatorisch gedrag dat niet in lijn is met de doelstellingen van de organisatie" biedt een duidelijkere, meer gestructureerde, precieze en auditbare basis. Zoals met elk risico, kunnen organisaties dit managen door de juiste beheersmaatregelen te ontwerpen en deze effectief te implementeren.

> **Opmerking**
>
> In de Topical Requirements wordt gebruik gemaakt van algemene terminologie voor internal auditing zoals gedefinieerd in de Global Internal Audit Standards. Lezers dienen de termen en definities in de verklarende woordenlijst van de standaarden te raadplegen.

De Organisatiegedrag Topical Requirement neemt deze filosofie over en stelt minimale verplichte vereisten vast om gedrag te beoordelen wanneer een risicobeoordeling bepaalt dat dit binnen het bereik van de beoordeling valt. Deze vereisten zijn volledig compatibel met de traditionele risicogebaseerde auditaanpak en kunnen met minimale aanpassingen in alle auditfuncties worden toegepast. Deze gebruikershandleiding geeft praktische voorbeelden van hoe deze aanpak kan worden ingebed in standaard auditopdrachten, evenals richtlijnen voor het beoordelen van het bredere raamwerk voor organisatiegedrag of individuele componenten. De significante invloed van dit onderwerp op de doelstellingen van de organisatie vraagt om proactieve overweging en aandacht.

De definities van de volgende belangrijke termen zijn nodig om de Topical Requirement te begrijpen en toe te passen. Gezien de onvolwassenheid van het onderwerp gebruiken organisaties deze termen inconsequent. De bijgeleverde definities moeten gebruikers helpen om de terminologie van hun organisatie af te stemmen op de terminologie in de Topical Requirement en deze gebruikershandleiding.

- **belanghebbende** - Een partij met een direct of indirect belang bij de activiteiten en resultaten van een organisatie. Belanghebbenden kunnen het bestuur, management, werknemers, klanten, verkopers, aandeelhouders, regelgevende instanties, financiële instellingen, externe auditors, het publiek en anderen zijn.
- **bestuur** - Het hoogste bestuursorgaan van de organisatie.
- **cultuur** - De keuzes die werknemers maken bij het uitvoeren van hun werk en hoe ze met anderen samenwerken, samen met de drijfveren achter dit organisatiegedrag. Drijfveren zijn formele mechanismen, zoals incentives en doelen, en informele mechanismen zoals collectieve waarden en overtuigingen.
- **gedrag** - Gedrag in relatie tot wettelijke vereisten en verwachtingen.

- **gedragspatronen** - Patronen in gedrag, waarbij gedrag terugkerend of vaker voorkomt. Patronen worden geïdentificeerd als "hoe dingen gedaan worden" in het algemeen, in tegenstelling tot eenmalige situaties.
- **gedragsprikkels (incentives)** - Alles wat gegeven kan worden om gedrag te motiveren, inclusief geldelijke prikkels zoals loonsverhogingen, bonussen of aandelenopties; of niet-geldelijke incentives zoals complimenten, voorkeursopdrachten of vrije dagen.
- **gedragsrisico** - Het risico dat gedrag niet consistent is met de doelstellingen van de organisatie.
- **organisatiegedrag** - De waarneembare keuzes die werknemers maken bij het uitvoeren van hun werk en hoe ze met anderen samenwerken. Dit gedrag beïnvloedt de prestaties en het bereiken van de doelstellingen van de organisatie . Eenvoudig gezegd is organisatiegedrag "de manier waarop we dingen doen" en wordt het beschouwd als een subset van cultuur.
- **prestatie beoordelingen** - Individuele of groepsevaluaties over de toereikendheid van iemands werk.
- **risico-indicatoren voor gedrag** - Actiegerichte managementinformatie over gedrag.
- **waarden** - Principes die bepalen hoe mensen zich moeten gedragen.

Secties

De verplichte eisen in de thematische eis voor organisatiegedrag en de niet-verplichte overwegingen in deze gebruikershandleiding zijn onderverdeeld in drie secties:

- **Governance** - Duidelijk gedefinieerde basisdoelstellingen en strategieën voor organisatiegedrag die de doelen, het beleid en de procedures van de organisatie ondersteunen.
- **Risicomanagement** - Processen om risico's met betrekking tot het gedrag van de organisatie te identificeren, analyseren, beheren en monitoren, inclusief een proces om incidenten direct te escaleren.
- **Beheersing** - Door het management vastgestelde, periodiek geëvalueerde beheersprocessen om risico's met betrekking tot organisatiegedrag te beperken.

In aanvulling op de Topical Requirement en deze gebruikershandleiding kunnen internal auditors aanvullende professionele richtlijnen over organisatiegedrag raadplegen, zoals de Global Guidance van de IPPF en andere specifieke bronnen.

Overwegingen

Internal auditors kunnen de volgende overwegingen gebruiken als hulpmiddel bij hun beoordeling van de eisen in de Organisatiegedrag Topical Requirement. De letters van elke overweging hieronder verwijzen naar de overeenkomstige vereisten in de Topical Requirement. Deze overwegingen zijn illustratief, maar niet verplicht. Internal auditors moeten op hun professionele oordeel afgaan bij het bepalen wat ze in hun beoordelingen opnemen.

Beperkingen in internal auditopdrachten in de publieke sector als gevolg van wetgeving, overheidsstructuur of politieke omgevingen worden gezien als potentiële belemmeringen om bepaalde aspecten van dit werk aan te pakken. Internal auditors in de publieke sector moeten dergelijke reikwijdte-beperkingen documenteren als onderdeel van hun risicobeoordelingsproces en professionele oordeelsvorming toepassen om de op maat gemaakte reikwijdte van hun beoordeling duidelijk te definiëren en te communiceren.

Overwegingen voor governance

Om te beoordelen hoe de bestuursprocessen kunnen worden toegepast op het gedrag van de organisatie, kunnen internal auditors het volgende onderzoeken:

A. Gestructureerde rollen en verantwoordelijkheden om ervoor te zorgen dat het bestuur het zicht en invloed houdt op de gedragsdimensies van de organisatie. Bewijs kan omvatten:
   - Een bestuurscommissie:
     - Richt een speciale raad of subcommissie(s) op die zich richt(t)(en) op organisatiegedrag met een duidelijke taakomschrijving die organisatiegedragstoezicht koppelt aan de strategie.
     - Voert regelmatige beoordelingen uit van gedragsrisico-indicatoren die zijn afgestemd op bedrijfsdoelen op lange termijn. Risico-indicatoren voor gedrag zijn maatstaven om vast te stellen of er actie nodig is om ervoor te zorgen dat het gedrag in lijn blijft met de doelstellingen van de organisatie , de gerelateerde waarden en het doel van de organisatie.
     - Neemt gedragsdoelstellingen op in de prestatie-evaluaties en beloningen van leidinggevenden.
   - Raamwerken voor bestuursrapportage:
     - Inzicht verschaffen in risico-indicatoren op basis van gedrag met behulp van gestructureerde dashboards (bijvoorbeeld betrokkenheid van medewerkers, incidenttrends, klanttevredenheid, erkenning op basis van waarden).
     - Cultuurgerelateerde maatstaven integreren in de strategische prestatierapportage op directieniveau.
   - Feedbackmechanismen van belanghebbenden, zoals enquêtes, geven:
     - Het bestuur directe input van werknemers, klanten en andere belanghebbenden over de afstemming van gedrag op waarden en strategie.

- Feedback om de strategische richting en gedragsinterventies te helpen vormen.

B. Effectief beheer van organisatiegedrag vindt plaats door middel van duidelijk gedefinieerde verantwoordingsplicht in de hele organisatie. Het bestuur is uiteindelijk verantwoordelijk om ervoor te zorgen dat de organisatie gedrag bevordert en in stand houdt dat in lijn is met de doelstellingen van de organisatie , inclusief het stellen van duidelijke verwachtingen voor gedrag, het toezicht houden op risicorapportage over gedrag en het uitdagen van het management als wordt vastgesteld dat het gedrag niet in lijn is met de doelstellingen. Bewijs kan omvatten:

- Het bestuur:
  - Keurt de risicobereidheid op gedrag en de belangrijkste culturele doelstellingen van de organisatie goed.
  - Vereist regelmatige rapportage over indicatoren van gedragsrisico's (bijvoorbeeld trends, incidentpatronen, klokkenluidersthema's).
  - Houdt het uitvoerend management verantwoordelijk voor culturele prestaties door middel van mechanismen zoals beloningsstructuren en "tone at the top"
  - Overlegt met tweede- en derdelijnsfuncties over zaken met betrekking tot escalatie van gedragsrisico's, hiaten in het toezicht en de toereikendheid van corrigerende maatregelen.
- Bedrijfsonderdelen en het operationeel management verankeren gedragsverwachtingen in de dagelijkse activiteiten en zorgen ervoor dat beslissingen, communicatie en teamdynamiek de waarden van de organisatie weerspiegelen. Dit kan inhouden dat je verantwoordelijkheid neemt voor:
  - Modelleren van gewenst gedrag en het handhaven van een psychologisch veilige omgeving.
  - Beheersmaatregelen implementeren die gedrag beïnvloeden, zoals werving, beloning, communicatie en leiderschapsroutines.
  - Proactief gedragsrisico's identificeren en escaleren wanneer deze zich voordoen in operationele omgevingen.
  - Gedragsrisico's beperken die het gevolg zijn van verkeerd afgestemd gedrag binnen hun teams en de behoefte aan beheersmaatregelen (formeel en informeel).
- Risico-, compliance-, personeelszaken en aanverwante toezichtfuncties ontwerpen en onderhouden het gedragsrisicoraamwerk van de organisatie, inclusief:
  - Gedefinieerde rollen en verantwoordelijkheden voor gedragstoezicht.
  - Escalatiepaden en processen voor gegevensanalyse.
  - Dashboards, thematische analyses en periodieke beoordelingen om toekomstgericht inzicht te bieden in de gedragsomstandigheden in de hele organisatie.

- Het vermogen om praktijken aan te vechten waar incentives, communicatie of leiderschapsgedrag afwijken van de gestelde doelen.
- Overleg over alle belangrijke wijzigingen in personeelsgerelateerde beheersmaatregelen, bestuurskaders of strategische transformatie-initiatieven die de cultuur kunnen beïnvloeden.
- Bestuderen van nieuwe trends uit incidentrapporten, auditbevindingen en andere betrouwbaarheidsmechanismen die wijzen op gedragsgerelateerde problemen.

c. Bestuursproces dat zorgt voor gedragstoezicht, regelmatige controle, evaluatie en de afstemming van gedragspatronen op de doelstellingen van de organisatie . Het proces kan bestaan uit:

- Een dashboard gebruiken om belangrijke gegevenspunten aan te bieden uit bronnen zoals de resultaten van tevredenheids- en integriteitsenquêtes onder werknemers, verloop- en verzuimcijfers, inhoud van het spreekkanaal, gegevens over incidenten en prestatie- en innovatiecijfers. Kenmerken van een effectief dashboard voor organisatiegedrag zijn onder andere:
  - Gedefinieerde drempelwaarden om mogelijkheden voor gedragsverbetering te identificeren.
  - Scheiding van gegevens over gedrag (zoals over 'je uitspreken')) van gegevens over drijfveren (zoals duidelijkheid van rollen en verantwoordelijkheden) en resultaatgegevens (zoals klachten van klanten).
  - Kwantitatieve gegevens, zoals uit enquêtes, gecombineerd met kwalitatieve gegevens, zoals uit focusgroepen en spreekkanalen.
- Het bestuur begrijpt hoe huidige aspecten van organisatiegedrag kunnen worden aangepakt om de effectiviteit en prestaties van de organisatie te verbeteren. Deze aspecten omvatten hoe:
  - Er worden beslissingen genomen, inclusief het zoeken naar verschillende perspectieven en uitdagingen.
  - Medewerkers communiceren met elkaar, inclusief het uitspreken van zorgen en verwachtingen.
  - Medewerkers werken samen, ook tussen teams en bij het oplossen van conflicten.
  - Werknemers reageren op mislukkingen door bijvoorbeeld te leren van fouten of te reageren met verwijten of ontkenning.
  - Leiderschapsgedrag in het midden- en hoger management heeft een invloed op de andere gedragscategorieën (bijvoorbeeld hoe leiders reageren op fouten en hoe ze uitdagingen uitlokken in de besluitvorming).

- De strategie en het bedrijfsmodel sturen de besluitvorming, de gedragscodes en het prestatiebeheer met incentives/ontmoedigingen.

- Het bestuur heeft een systeem voor continu leren nodig dat verbetermogelijkheden vaststelt en deze actief en meetbaar aanpakt door:
  - Op feiten gebaseerde inzichten gebruiken die gebaseerd zijn op feitelijk gedrag van werknemers.
  - Focussen op wat bekend is dat er gebeurt binnen de organisatie in plaats van op wat bedoeld of gewenst is.
  - Het beoordelen van een mix van kwalitatieve en kwantitatieve gegevens, vaak verkregen via enquêtes, spreekkanalen, vertrouwelijke gesprekken en focusgroepen.
  - De inzichten toepassen om acties te bepalen die bepaalde aspecten van organisatiegedrag versterken en aanpakken.
  - Het opnemen van een actieplan om gerichte interventies op kritieke gebieden te combineren (bijvoorbeeld communicatiestrategie, training, leiderschapsontwikkeling en discussies op teamniveau).

D. Beleid en procedures met betrekking tot gedragsrisico's worden opgesteld, periodiek herzien, effectief gecommuniceerd en geïntegreerd in de bedrijfsvoering en besluitvorming. Het beleid en de procedures hebben betrekking op ethiek, personeelszaken, naleving, risico, bedrijfsvoering en beslissingsrechten om ervoor te zorgen dat:

- Gedragsverwachtingen zijn formeel vastgelegd in relevant beleid (zoals een gedragscode en/of beleid op het gebied van ethiek, personeelszaken, incentives en het delegeren van bevoegdheden). Dergelijk beleid moet acceptabel en onacceptabel gedrag definiëren met praktische voorbeelden, afgestemd op de risicobereidheid van de organisatie.
- Risicomanagementfuncties brengen gedragsverwachtingen in kaart in belangrijke operationele processen, zoals indienstneming, prestatiebeoordelingen, onboarding en klantbeheer, en zorgen ervoor dat ze worden weerspiegeld in dagelijkse beslissingen. Assurance reviews moeten testen hoe deze verwachtingen het werkelijke gedrag beïnvloeden en hierover rapporteren aan het bestuur.
- Het bestuur zoekt en krijgt de zekerheid dat het beleid van de organisatie toegankelijk is en duidelijk gecommuniceerd wordt via verschillende kanalen (bijvoorbeeld intranet, training, gemeentehuizen). Het opnemen van casestudies en beslisbomen helpt om gedragsverwachtingen in hun context te plaatsen. Dashboards kunnen inzicht en gebruiksgegevens bijhouden.
- Alle beleidsregels en procedures op het gebied van gedrag worden regelmatig herzien en bijgewerkt naar aanleiding van incidenten, bevindingen uit onderzoeken of wijzigingen in de regelgeving. Tweedelijnsfuncties moeten een register van geleerde

lessen bijhouden om hiaten te identificeren die ontstaan tussen gedrag en de doelstellingen van de organisatie .

- Het bestuur ontvangt regelmatig updates over de dekking, duidelijkheid en effectiviteit van het beleid. De tweede lijn moet overtredingen, de gevolgen voor het beleid en de afstemming op gewenst gedrag analyseren. De effectiviteit van het beleid moet worden beoordeeld aan de hand van kwalitatieve feedback en gedragsrisico-indicatoren.

Overwegingen voor risicomanagement

Om te beoordelen hoe risicomanagementprocessen worden toegepast op organisatiegedrag, kunnen internal auditors beoordelen of:

A. Een risicomanagementproces op basis van gedrag is duidelijk gedefinieerd en omvat gedragskenmerken die cruciaal zijn voor het behalen van de doelstellingen van de organisatie . Kenmerken van risicomanagement kunnen zijn:

- De rollen en verantwoordelijkheden zijn afgestemd op de risico- en governance raamwerken van de onderneming en de rapportagelijnen maken onafhankelijkheid en invloed mogelijk.
- Autoriteit om beslissingen aan te vechten en gedragsgerelateerde risicokwesties te escaleren zonder angst voor vergelding of verwatering.
- Onafhankelijkheid van operationeel management met directe toegang tot senior leiderschap en het bestuur.
- Toegang tot gegevens over gedragsrisico's uit meerdere bronnen die relevant en actueel zijn en die getrianguleerd zijn over verschillende bronnen. Deze gegevens omvatten zowel gestructureerde (zoals enquêteresultaten, beleidsovertredingen) als ongestructureerde vormen (bijvoorbeeld verslagen van insprekers, inzichten uit focusgroepen). Gegevensbronnen zijn onder andere personeelszaken (zoals verloop, retentie en enquêtegegevens), klokkenluiders, klachten van klanten en auditbevindingen.
- Gebruik van gegevensanalyse om trends, afwijkingen en nieuwe risico's te identificeren.
- Gebruik van dashboards en risico-indicatoren voor management- en bestuursrapportage.
- Gebruik van gedragsrisico-indicatoren gekoppeld aan organisatorische doelstellingen.
- Het uitvoeren of uitbesteden van onderzoeken naar de hoofdoorzaak van gedragsfouten en culturele onaangepastheid.
- Bekendheid met zowel formele als informele drijfveren van gedrag (bijvoorbeeld incentives, psychologische veiligheid en leiderschapstoon).

- De geloofwaardigheid en het vertrouwen van senior leiders in operationele teams, gecombineerd met het vermogen om besluitvorming in realtime te beïnvloeden.
- Actieve betrokkenheid bij het ontwerp en de beoordeling van beheersmaatregelen met betrekking tot personeelszaken (bijvoorbeeld incentives, werving en training).
- Adviserende rol in strategische veranderingsprogramma's en transformatie-initiatieven.
- Samenwerking met de bedrijfsleiding om de cultuur vorm te geven door invloed uit te oefenen, niet alleen door handhaving.
- Voortdurende verzameling en analyse van gegevens, waaronder mogelijk:
  - Enquêtes over werknemersbetrokkenheid en welzijn.
  - Gegevens over erkenning en beloning voor waardengedreven gedrag.
  - Klokkenluidersrapporten en klachten.
  - Feedback van klanten, met nadruk op zowel tevredenheid als ontevredenheid.
  - Prestatiebeoordelingen die samenwerking, integriteit en innovatie weerspiegelen.
- Gebruik van gegevensanalyse om kwetsbaarheden te identificeren en trends te detecteren.
- Een duidelijk gedefinieerd proces voor snelle escalatie van risico's en gedrag dat niet in lijn is met de doelstellingen van de organisatie.
- Toezicht op de vaststelling en uitvoering van managementactieplannen om risico's aan te pakken en vereist gedrag te versterken.

B. Tijdige controleprocessen voor organisatiegedrag omvatten het rapporteren van resultaten aan belanghebbenden. Voorbeelden van risico-indicatoren in de gedrags-, drijfveren- en resultaatcategorieën en te rapporteren tekortkomingen zijn onder andere:

- Besluitvorming: Een gebrek aan effectieve uitdaging of onvoldoende integratie van verschillende perspectieven.
- Communicatie: Onvoldoende aandacht voor de problemen die door individuen worden gerapporteerd.
- Samenwerking: Gefragmenteerde werkomgevingen waarin werknemers zich alleen op hun eigen werk concentreren.
- Reageren op tekortkomingen: Verwijten maken en straffen voor onbedoelde fouten.
- Formele drijveren: Onduidelijke rollen en verantwoordelijkheden of tegenstrijdige doelen.
- Informele drijfveren: Lage psychologische veiligheid of ineffectieve dynamiek tussen de drie lijnen.
- Prestatiegegevens: Buitensporige klachten van klanten of stagnerende innovatie of digitalisering.

- Personeelsgegevens: Hoge niveaus van verloop en absenteïsme en lage tevredenheidsniveaus in de onderzoeksresultaten.
- Risico- en juridische gegevens: Hoog aantal onderzoeken, beleidsovertredingen of waarschuwingen en situaties die ternauwernood zijn afgewend.

c. Processen om ervoor te zorgen dat afwijkingen tussen verwacht en waargenomen gedrag worden geïdentificeerd en gecommuniceerd met degenen die bevoegd en in staat zijn om op te treden. Internal auditors kunnen beoordelen of:

- Effectieve communicatie komt op het juiste moment, is gebaseerd op feiten en wordt ondersteund door een analyse van onderliggende oorzaken.
- Het ontwerp en de operationele effectiviteit van communicatie-inspanningen voorkomen oppervlakkige oplossingen, reputatieschade of herhaalde mislukkingen.
- Informatie wordt verzameld en samengevoegd uit verschillende bronnen, waaronder feedback van werknemers, klokkenluidersrapporten, auditbevindingen en beoordelingen van incidenten.
- Gestructureerde analysetechnieken - zoals thematische reviews, gedragswetenschappelijke modellen en raamwerken voor onderliggende oorzaken - gaan verder dan oppervlakkige symptomen en identificeren onderliggende oorzaken van slechte afstemming (bijvoorbeeld onduidelijke incentives, lage psychologische veiligheid of ineffectieve toon aan de top).
- Hiaten worden niet alleen gepresenteerd als nalevingsovertredingen of geïsoleerde incidenten, maar als gebeurtenissen met onderliggende gedragsoorzaken die culturele, systemische en/of leiderschapskwesties weerspiegelen.
- In mededelingen wordt benadrukt wat er is gebeurd en waarom, waarbij kwantitatieve en kwalitatieve gegevens worden gebruikt om conclusies te ondersteunen.
- De organisatie scheidt gedragspatronen, kwetsbaarheden die voortkomen uit drijfveren voor gedrag, en organisatorische resultaten (bijvoorbeeld de impact op de prestaties, het vertrouwen van belanghebbenden), waardoor gedrag en de drijfveren kunnen worden aangepakt. Bevindingen worden gecommuniceerd aan het juiste publiek, op het juiste detailniveau:
  - Operationele managers voor onmiddellijke procescorrectie.
  - Senior leiderschap voor toewijzing van middelen, berichtgeving en toon.
  - Het bestuur of relevante commissies voor overzicht en strategische implicaties.
- Visuele en verhalende hulpmiddelen zoals dashboards, heat maps of samenvattingen van casussen leggen bevindingen uit en ondersteunen aanbevelingen en/of actieplannen.
- Implicaties voor risicoblootstelling en de veerkracht van de beheersomgeving worden meegenomen in procesbeoordelingen.

- De communicatie van hiaten wordt gekoppeld aan verbeteracties en er wordt gecontroleerd of deze zijn voltooid.
- De resultaten van interventies worden beoordeeld en gedeeld, waardoor de leercyclus wordt voltooid.
- Communicatie is vrij van ongepaste beïnvloeding en is in lijn met gevestigde escalatieprotocollen, waardoor de onafhankelijkheid en geloofwaardigheid van beoordelingen behouden blijft.

D. Hiaten tussen verwacht en feitelijk gedrag worden op een gestructureerde en participatieve manier opgelost om ervoor te zorgen dat herstel is gebaseerd op inzichten van belanghebbenden, wordt gevolgd tot aan de voltooiing en wordt geëvalueerd op effectiviteit. Internal auditors kunnen beoordelen of:

- De belanghebbenden die het dichtst bij het probleem staan, zoals operationele managers, personeelszaken, zakenpartners, werknemersvertegenwoordigers, nalevingsadviseurs en betrokken individuen of teams, worden op een zinvolle manier betrokken bij het oplossingsproces. Hun inbreng zorgt ervoor dat acties zijn:
  - Contextueel gegrond: Gevoelig voor de operationele realiteit en informele normen die kunnen hebben bijgedragen aan de kloof.
  - Geloofwaardig en geaccepteerd: Meer kans op steun en verankering hebben als de acties worden vormgegeven door degenen die er direct bij betrokken zijn.
  - Constructief uitdagend: Openhartige reflectie mogelijk maken over ondersteunend leiderschapsgedrag, zwakke punten in het ontwerp van de beheersing of groepsdynamiek.
- Inbreng van belanghebbenden wordt gevraagd, samengevat en verwerkt in actieplannen. Feedbackmechanismen kunnen bestaan uit interviews, focusgroepen, enquêtediagnoses en andere methoden.
- Oplossingsacties zijn gedocumenteerd, met gedefinieerde eigenaar, tijdschema's en succescriteria:
  - Acties staan in verhouding tot de ernst van het probleem.
  - Waar nodig richten acties zich op de formele drijfveren (bijvoorbeeld beleid, incentives) en informele drijfveren (bijvoorbeeld psychologische veiligheid, teamdynamiek).
  - Waar meerdere functies bij betrokken zijn (bijvoorbeeld personeelszaken voor training, risicomanagement voor beheersing), worden de cross-functionele levering en verantwoordelijkheid gecoördineerd en verduidelijkt.
- De voortgang wordt gevolgd tot aan de voltooiing en zorgt ervoor dat toezeggingen worden nagekomen en nagekomen worden. Dit omvat:
  - Bijhouden van een gedragskwestie/actieregister of gelijkwaardig mechanisme.
  - Regelmatige check-ins met actie-eigenaren om de status te controleren.

- Vertragingen, gedeeltelijke voltooiing of weerstand escaleren naar de juiste bestuursfora.

- De doeltreffendheid van de resolutie in het dichten van de kloof en het verminderen van het gedragsrisico wordt beoordeeld. Dit kan inhouden:
  - Risico-indicatoren voor gedrag opnieuw beoordelen na implementatie.
  - Feedback verzamelen van betrokken belanghebbenden over waargenomen veranderingen.
  - Testen op gedragsveranderingen via observatie, onderzoek of audittechnieken.
  - Acties aanpassen of versterkingen toevoegen wanneer de resultaten zwak of dubbelzinnig blijven.

Overwegingen voor beheersprocessen

Om te beoordelen hoe beheersprocessen worden toegepast om het risico te beperken dat het gedrag van de organisatie niet is afgestemd op de doelstellingen van de organisatie, kunnen internal auditors een beoordeling uitvoeren van:

A. Beoordeling van gedragsrisico's om het risico te begrijpen dat wordt veroorzaakt door het huidige gedrag van de organisatie (dat wil zeggen, de potentiële onbedoelde gevolgen van de manier waarop dingen worden gedaan). Voorbeelden van dergelijke beoordelingen zijn beoordelingen van projecten nadat ze zijn afgerond, oorzakenanalyses en beoordelingen van gedetailleerde operaties in de praktijk.

B. Gestructureerde feedbackprocessen om te begrijpen welke mechanismen het management gebruikt om gedragsverwachtingen te communiceren (bijvoorbeeld bedrijfsbrede bijeenkomsten, e-mail en vergaderingen tussen individuen en hun leidinggevende) en de effectiviteit van de managementtoon op gedrag binnen een organisatie. Dit kan gedaan worden door de processen te evalueren die de percepties en het begrip van werknemers van de boodschappen van hetbestuur en het senior management vastleggen en analyseren. Internal auditors kunnen organisaties helpen hun communicatiestrategieën voortdurend te verfijnen en ervoor te zorgen dat de toon van de top op alle niveaus effectief overkomt door belangrijke beheersmaatregelen te beoordelen, zoals:

   - Regelmatige enquêtes, interviews en focusgroepdiscussies met werknemers, waarin wordt gevraagd naar de duidelijkheid, consistentie en impact van de communicatie van het leiderschap en die kwantitatieve en kwalitatieve gegevens opleveren over hoe goed de boodschappen worden ontvangen en begrepen op verschillende niveaus van de organisatie.
   - Open kanalen voor anonieme feedback, zodat werknemers hun eerlijke mening kunnen delen zonder bang te hoeven zijn voor represailles. Deze kanalen moeten worden gefaciliteerd via digitale platforms die real-time feedback en suggesties mogelijk maken. Gegevens uit deze kanalen moeten worden geanalyseerd om te

controleren of de toon aan de top goed wordt begrepen door werknemers op alle niveaus.

- Feedback van senior managementvergaderingen verzameld via enquêtes, interviews, focusgroepen, notulen en anonieme kanalen om ervoor te zorgen dat het senior management op de hoogte is van ineffectieve communicatie, misverstanden of gebieden die verbetering behoeven. Het senior management laat zien dat de inbreng van werknemers gewaardeerd wordt door actief te reageren en te handelen naar aanleiding van de feedback. Als dit niet gebeurt, kunnen werknemers minder geneigd zijn om feedback te geven omdat ze het gevoel hebben dat er niets zal veranderen.
- Feedback over de prestaties van het senior management wordt geïntegreerd in hun prestatiebeoordelingen om voortdurend te controleren of de richtlijnen van het leiderschap worden opgevolgd. Dit versterkt het belang van leiderschapsboodschappen en zorgt ervoor dat ze worden weerspiegeld in de dagelijkse activiteiten.

c. Escalatie binnen een organisatie wordt aangemoedigd om vroegtijdig risico's te identificeren en te beperken en om een psychologisch veilige omgeving te creëren waarin werknemers zich op hun gemak voelen om problemen te melden zonder bang te hoeven zijn voor vergelding. Internal auditors kunnen belangrijke beheersmaatregelen beoordelen om effectief risicomanagement te verbeteren, zoals:

- Gemakkelijk te gebruiken feedbackmechanismen, waaronder directe rapportage en anonieme opties, interne en externe fraude- of klokkenluidershotlines, enquêtes, ideeënbussen en digitale platforms om vertrouwelijke rapportage mogelijk te maken en kwesties vast te leggen die mensen misschien niet openlijk willen melden.
- Goed gedefinieerde en eenvoudig te begrijpen processen voor het melden van problemen, met meerdere directe en anonieme interne en externe kanalen, en inspanningen om werknemers bewust te maken. Kenmerken van rapportagekanalen moeten zijn:
  - Vertrouwelijkheidswaarborgen, die de identiteit beschermen van personen die problemen melden.
  - Een strikt beleid dat represailles verbiedt en dat duidelijk wordt gecommuniceerd en consequent wordt nageleefd om mensen te beschermen die problemen melden.
  - Terugcommuniceren naar personen die problemen niet anoniem melden, ongeacht de reden of het resultaat.
  - Regelmatige overzichten voor de hele organisatie van kwesties die in het verleden zijn gerapporteerd en de resultaten daarvan om aan te tonen dat kwesties worden gerapporteerd en dat er actie op wordt ondernomen en om te zorgen voor transparantie over de acties die worden ondernomen om feedback aan te pakken.

- Regelmatige communicatie van het management waarin het belang van open communicatie en het rapporteren van problemen wordt benadrukt en waarin wordt aangetoond hoe het management zelf een dergelijk gedrag laat zien.
- Regelmatige trainingssessies waarin het belang van psychologische veiligheid wordt benadrukt, waarin mensen worden aangemoedigd om problemen te melden en waarin richtlijnen worden gegeven over hoe problemen op de juiste manier kunnen worden geëscaleerd. De training moet regelmatig worden herhaald om het gewenste gedrag na verloop van tijd te versterken.
- Informele beloningen, zoals mondelinge of schriftelijke waardering en publieke erkenning, voor personen die problemen melden.
- Regelmatige beoordeling van het escalatieproces om de effectiviteit en efficiëntie ervan te waarborgen, inclusief het vragen om feedback van werknemers om belemmeringen voor het melden te identificeren en direct aan te pakken.
- Communicatie over het oplossen van feedback.

D. Incentive- en ontmoedigingsprogramma's zijn afgestemd op het gewenste gedrag en de doelstellingen van de organisatie en worden gecommuniceerd. Internal auditors kunnen beheersmaatregelen beoordelen zoals:

- Incentives - zowel monetair (bijvoorbeeld bonussen, promoties) als niet-monetair (bijvoorbeeld erkenning, ontwikkelingsmogelijkheden) - zijn afgestemd op de doelstellingen van de organisatieen gekoppeld aan het vertonen van het gewenste gedrag.
- Evenwichtige prestatiebeoordelingscriteria omvatten de manier waarop doelstellingen worden bereikt (bijvoorbeeld samenwerking, integriteit en klantgerichtheid) en meer traditionele prestatiecijfers (zoals financiële doelen).
- De incentive-criteria en ontmoedigingsdrempels zijn duidelijk gedefinieerd, worden consequent toegepast en worden gecontroleerd door het management of human resources om vooroordelen en onbedoelde resultaten te voorkomen.
- Functieoverschrijdende groepen valideren consistentie en eerlijkheid in incentive-beslissingen tussen bedrijfsonderdelen.
- Consequenties voor wangedrag en culturele overtredingen omvatten duidelijke, evenredige ontmoedigingsmaatregelen (bijvoorbeeld bonusverlagingen en het blokkeren van promoties), waarbij acties worden uitgelegd en gedocumenteerd om transparantie te garanderen.
- Niet-monetaire erkenningsprogramma's zetten werknemers in de schijnwerpers die een voorbeeld zijn van culturele waarden, zoals ethische besluitvorming en psychologische veiligheid.
- De impact van incentive-programma's wordt routinematig beoordeeld aan de hand van feedback van werknemers en gedragsmetingen om beloningsmechanismen te verfijnen of opnieuw in evenwicht te brengen. Incentive-programma's moeten worden geëvalueerd en aangepast om ervoor te zorgen dat:

- De doelen zijn niet te smal of te breed.
- De doelen zijn haalbaar.
- De kortetermijndoelen ondermijnen de langetermijnresultaten niet.
- Er worden aanvaardbare risiconiveaus vastgesteld.
- Er worden waarborgen geïmplementeerd om ethisch gedrag te garanderen terwijl de doelen worden bereikt (bijvoorbeeld leiders als voorbeeld van ethisch gedrag, de kosten van valsspelen veel hoger maken dan de baten en sterk toezicht).
- De doelen zijn afgestemd op individuele capaciteiten en omstandigheden zonder de eerlijkheid uit het oog te verliezen.
- Teamdoelen zijn niet in tegenspraak met individuele doelen.
- Intrinsieke motivatie wordt beoordeeld en het management erkent dat sommige doelen intrinsieke motivatie kunnen beperken.
- De uiteindelijke doelen van de organisatie worden overwogen en het soort doel (bijvoorbeeld prestatie of leren) wordt beoordeeld op geschiktheid.

- De organisatie integreert positieve bekrachtiging en corrigerende acties om proactief gedrag in de organisatie te cultiveren dat in lijn is met de doelstellingen van de organisatie en de wettelijke vereisten. De belangrijkste beheersmaatregelen zijn:
  - Regelmatige beoordeling van de effectiviteit van communicatie- en trainingsprogramma's om ervoor te zorgen dat werknemers het belang van het melden van problemen en de gevolgen van niet-naleving begrijpen en zich aangemoedigd voelen om problemen te melden.
  - Monitoring- en rapportagesystemen houden de naleving bij en identificeren mogelijke onderrapportageproblemen.
  - Disciplinaire maatregelen worden consequent en eerlijk toegepast en zijn niet zo streng dat ze melding ontmoedigen of zo mild dat ze onethisch gedrag niet ontmoedigen.
  - Feedbackmechanismen waarmee werknemers anoniem problemen kunnen melden, worden regelmatig herzien om ervoor te zorgen dat ze effectief zijn en eerlijke rapportage aanmoedigen.

E. Het issuemanagementproces van de organisatie identificeert gedrag dat niet in lijn is met de doelstellingen van de organisatie en escaleert dit indien nodig om een actieplan op te stellen om het risico op slechte resultaten te beperken. Internal auditors kunnen de belangrijkste beheersmaatregelen voor effectieve gedragsverandering beoordelen, zoals:

- Op bewijs gebaseerde benaderingen: Het actieplan bevat evidence-based benaderingen om gedrag te veranderen, gebaseerd op gedragswetenschap, gedragsmodellen en verandermanagement. Als de aanpak niet expliciet gebaseerd is op een specifiek gedragsveranderingsmodel, moet de aanpak interventiestrategieën combineren voor:

- Communicatie: Medewerkers en management consequent bewust maken van de noodzaak van gedragsverandering en de transformatie omarmen en ondersteunen.
- Training en ontwikkeling van werknemers: Investeren in trainingsprogramma's op maat van de verschillende functies en werknemers uitrusten met de nodige vaardigheden en gedragingen via workshops, e-learning en mogelijkheden voor voortdurende ontwikkeling. Dit omvat het leren en effectief kunnen toepassen van de nieuwe vaardigheden en gedragingen die nodig zijn om de door de organisatie gewenste veranderingen te realiseren.
- Managementontwikkeling: Managers op alle niveaus denken na over hoe ze gedragsveranderingen in dagelijkse situaties mogelijk kunnen maken en kunnen demonstreren. Dit kan inhouden dat het management zijn eigen gedrag aanpast om het personeel te helpen zich meer op hun gemak te voelen bij het implementeren van nieuw gedrag, rechtstreeks vraagt dat werknemers nieuw gedrag implementeren en het leren aanmoedigt en vraagt om training voor de vaardigheden en gedragingen die nog nodig zijn. Leiderschapsprogramma's en coaching kunnen vaardigheden en zelfvertrouwen verfijnen.

- Consistente versterkingen in dagelijkse situaties: Mensen hebben ondersteuning, aanmoediging en regelmatige herinneringen nodig om nieuw gedrag te ontwikkelen en te integreren in hun dagelijkse werkroutines.
- Congruente versterking: Een interventieplan moet worden afgestemd op leiderschapsberichten, processen, systemen, coaching en informele feedbackmechanismen om de gewenste verandering te versterken. Deze afstemming neemt onzekerheid en verwarring weg en zorgt ervoor dat werknemers begrijpen wat de gewenste gedragsveranderingen zijn, hoe ze deze moeten invoeren en hoe belangrijk ze zijn.
- De drijvende krachten achter gedrag aanpakken: Duurzame gedragsverandering vereist het aanpakken van de onderliggende drijfveren (zie Risicobeheer, C) van gedrag in plaats van alleen het gedrag zelf.
- Meting: Het meten van de voortgang en effectiviteit van interventies helpt om te bepalen of ze de gewenste impact hebben en of er aanpassingen nodig zijn. Regelmatige updates fungeren als positieve versterking en voorzien belanghebbenden van informatie over de voortgang. Een effectieve meetaanpak combineert kwalitatieve en kwantitatieve methoden, zoals enquêtes en interviews, en geeft een uitgebreid inzicht in de voortgang.

F. Trainingsprogramma's die bedoeld zijn om gedrag te beïnvloeden zijn expliciet gekoppeld aan gedefinieerde gedragsverwachtingen of risicobereidheidsverklaringen. Voorbeelden van trainingsonderwerpen zijn ethiek, naleving, leiderschap, inclusie, risicobewustzijn en besluitvorming. Internal auditors kunnen controleren of trainingsprogramma's worden uitgevoerd die:

- Gewenst gedrag en attitudes weerspiegelen en duidelijke, gedocumenteerde leerdoelen bevatten.

- Gebaseerd zijn op gedragsmatig bewijs of leren van incidenten (bijvoorbeeld auditbevindingen, oorzakenanalyses en feedbackmechanismen).
- Gericht zijn op alle relevante rolgroepen, met modules op maat voor senior management, lijnmanagers en medewerkers.
- Verplicht zijn waar relevant (bijvoorbeeld processen met een hoog risico, gereguleerde verantwoordelijkheden en controlerollen).
- Regelmatig worden ververst en de inhoud ten minste jaarlijks wordt herzien om de relevantie en effectiviteit te waarborgen.
- Ontworpen voor:
  - Gebruik praktijkscenario's of casestudy's om gedragsverwachtingen tastbaar te maken.
  - Gebruik technieken die leerlingen betrekken (bijvoorbeeld verhalen vertellen en reflectieve vragen stellen).
  - Betrek het senior management er actief bij om de toon aan de top aan te geven en medewerkers aan te moedigen om gedragsveranderingen door te voeren.
- Inclusief effect- en borgingsbeheersmaatregelen die:
  - De voltooiing van verplichte training bijhouden en uitzonderingen rapporteren.
  - De impact op gedrag en retentie meten door middel van informele enquêtes, eenvoudige tests of beoordelingen op basis van observatie.
  - Het perspectief van de deelnemers en de effectiviteit van de training vastleggen door middel van gestructureerde feedbackprocessen.
  - Ervoor zorgen dat de inhoud van trainingen is afgestemd op risicokaders en controlevereisten en formele beoordelings- en goedkeuringsprocessen omvat.

G. Wervingsprocessen zijn afgestemd op de gedragsverwachtingen van de organisatie en bevatten gedragscompetenties. Internal auditors kunnen beheersfuncties beoordelen, zoals:

- Tools om te beoordelen of kandidaten aansluiten bij de waarden van de organisatie, zoals gestructureerde interviewgidsen en vragen gebaseerd op scenario's.
- Gedragsinterviews en feedback van collega's worden gebruikt om eigenschappen als empathie, ethisch beoordelingsvermogen en verantwoordelijkheid te beoordelen.
- Wervingsadvertenties en employer branding weerspiegelen de culturele aspiraties van de organisatie om cultureel afgestemde kandidaten aan te trekken.
- Feedbackmechanismen maken het mogelijk om de culturele integratie van nieuw aangeworven personen te beoordelen, zodat afwijkingen in een vroeg stadium kunnen worden aangepakt.
- Documentatie (bijvoorbeeld beoordelingskaders en gespreksverslagen) toont aan dat de criteria voor het aannemen van personeel consistent worden toegepast.

- Personeelszaken en het hogere management beoordelen aanwervingspatronen op risico's, zoals vriendjespolitiek, vooringenomenheid of het niet naleven van gedragsnormen.
- Het aanname- en promotiebeleid wordt regelmatig getoetst op consistentie met de waarden van de organisatie en effectiviteit in de praktijk.

Bijlage A. Voorbeelden van praktische toepassingen

De volgende voorbeelden beschrijven scenario's waarin de Organisatiegedrag Topical Requirement van toepassing is.

Voorbeeld 1: Afzonderlijke evaluatie van het gedragskader van de organisatie

De internal auditfunctie startte een op zichzelf staande beoordeling van het overkoepelende raamwerk van een organisatie om het ontwerp en de werking bij het beheren van gedragsrisico's te evalueren. De reikwijdte van deze opdracht omvatte de bestuursstructuren, risicomanagementactiviteiten en gedragsbeheersmaatregelen die de afstemming binnen de organisatie ondersteunen.

Internal auditors beoordeelden of de verantwoordelijkheden voor gedragstoezicht duidelijk waren gedefinieerd en of er geen sprake was van belangenverstrengeling. Het team beoordeelde de taakomschrijving van het bestuur en controleerde of het bestuur regelmatig rapportages had ontvangen over risico-indicatoren op basis van gedrag, zoals enquêteresultaten en trends op het gebied van meldingen. De beoordeling omvatte ook het evalueren of cultuurgerelateerd beleid, zoals dat met betrekking tot klokkenluiden en ethisch gedrag, routinematig werd bijgewerkt en gehandhaafd.

Internal auditors beoordeelden ook elementen van risicomanagement, te beginnen met het beheerskader voor gedragsrisico's dat door de tweede lijn wordt onderhouden, waarbij ze zich concentreerden op de vraag of het de belangrijkste factoren voor gedragsrisico's identificeerde (zoals een lage psychologische veiligheid of slecht afgestemde prestatiedoelen). De beoordeling benadrukte hoe de organisatie de verschillen tussen verwacht en waargenomen gedrag bijhield en aanpakte, inclusief of afwijkingen in gedrag systematisch werden geëscaleerd en aangepakt.

De beheersomgeving werd onderzocht om te bepalen of formele processen de gedragsverwachtingen ondersteunden. De auditors evalueerden wervingsprotocollen voor op waarden gebaseerde beoordeling, of de inwerkinhoud was afgestemd op de normen van de cultuur van de organisatie en de mate waarin (monetaire en niet-monetaire) incentives werden beoordeeld op onbedoelde gevolgen. Trainingsprogramma's, ‘speak up’-kanalen, leiderschapsberichten en gegevensanalyse om gedragsproblemen op te sporen werden ook getest.

Deze opdracht gaf een uitgebreid beeld van de manier waarop gedragsrisico's worden beheerst op organisatieniveau en vormde de basis voor aanbevelingen voor verbeteringen aan de gedragsinfrastructuur van de organisatie.

Voorbeeld 2: Thematisch onderzoek van incentives

Deze auditopdracht was gericht op het beoordelen van de manier waarop de incentive-programma's van de organisatie gedrag beïnvloeden en of ze in overeenstemming zijn met het doel, de waarden en de wettelijke verwachtingen van de organisatie. De internal auditfunctie heeft dit thema gekozen vanwege de toenemende bezorgdheid over het risico op wangedrag en ontdekt bewijs van op druk gebaseerd gedrag in bedrijfsonderdelen.

De evaluatie begon met het evalueren van de governance-regelingen voor het ontwerpen en goedkeuren van incentivestructuren. De auditfunctie beoordeelde of degenen die verantwoordelijk zijn voor het uitvoeren van bestuursbeslissingen, zoals personeelszaken- of beloningscommissies, formeel toezicht hadden op het ontwerp van beloningen en of hun werk onafhankelijk werd beoordeeld door risico-, compliance- of auditfuncties.

Een risicomanagementperspectief werd toegepast om te begrijpen of bij de ontwikkeling van incentive-structuren rekening werd gehouden met de implicaties ervan op het gedrag. De auditors onderzochten of de organisatie scenario's had getest of gedragsrisico's had geanalyseerd voor haar beloningsstructuren. Ze onderzochten ook of belangrijke prestatie-indicatoren voor gedrag, zoals samenwerkingsscores, werden bijgehouden en gebruikt om resultaten te beoordelen.

Controletesten bestreken een reeks mechanismen die ontworpen zijn om beloningsgerelateerd gedrag vorm te geven. Deze omvatten balanced scorecards met prestatiecriteria die prestaties meten en hoe ze werden bereikt, de toepassing van malus (een straf of vermindering in loon) en/of terugvorderingsbepalingen en het bestaan van 360-graden feedbackprocessen. De auditors onderzochten ook de training die lijnmanagers kregen over het geven van feedback op gedrag en onderzochten niet-geldelijke erkenningsprogramma's die op waarden gebaseerd gedrag beloonden.

Tijdens de hele opdracht hebben de internal auditors geprobeerd vast te stellen of incentive-programma's onbedoeld ongewenst gedrag in de hand kunnen werken, zoals het nemen van buitensporige risico's, het nemen van kortere routes of terughoudendheid om problemen te escaleren. Er werden aanbevelingen gedaan om de transparantie te verbeteren, op waarden gebaseerde doelen consequenter in te bedden en onafhankelijke beoordelingen van het tweedelijnsmanagement tijdens het proces van het ontwerpen van beloningen te versterken.

Voorbeeld 3: Integratie in een traditionele audit - management van cyberrisico's

In dit voorbeeld integreerde de internal auditfunctie overwegingen inzake gedragsrisico's in een traditionele opdracht om het beheer van cyberrisico's te beoordelen. In het besef dat veel cyberstoringen niet alleen het gevolg zijn van technische problemen, maar ook van menselijk gedrag, hebben de auditors gedrag tijdens de opdracht beoordeeld.

De opdracht begon met het beoordelen van de mate waarin gedragsrisico werd erkend binnen de governance van cyberweerbaarheid. De auditors onderzochten het toezicht van het bestuur en het senior management op de cyberstrategie en zochten naar bewijs dat de organen controleerden en bespraken of het gedrag, zoals naleving van veilige praktijken of leiderschapsmodellen voor veilig gedrag, aansloten bij de organisatiedoelstellingen.

Op het gebied van risicobeheer evalueerde het team of de cyberrisicobeoordelingen van de organisatie rekening hielden met menselijke factoren. Dit omvatte ook het beoordelen of gedragsgegevens (bijvoorbeeld de frequentie van mislukte phishingtests, inbreuken op systeemtoegang of lage voltooiingspercentages van trainingen) werden gebruikt om risico's te bewaken en te escaleren. In het kader van de opdracht werd ook onderzocht of de hoofdoorzaak van eerdere beveiligingsincidenten was vastgesteld om mogelijke gedragsbepalende factoren te identificeren, zoals onduidelijke verantwoordingsplicht of managementtoon.

Het testen van beheersmaatregelen richttte zich op het gewenste gedrag en veilige bedrijfsvoering. Auditors onderzochten of screening van gedrag was opgenomen in het wervingsproces voor functies met bevoorrechte toegang. Incentive-structuren werden beoordeeld om te zien of ze veilige online praktijken aanmoedigden of onbedoeld risicovol gedrag prioriteit gaven boven veiligheid. Cybersecurity-trainingen werden ook geëvalueerd om te bepalen of ze boeiend waren, regelmatig werden vernieuwd en simulaties bevatten die gedragsreacties op phishing en social engineering testten.

Tot slot werd gekeken hoe het management veilig gedrag versterkte door middel van communicatie en of werknemers zich op hun gemak voelden bij het melden van onveilig cybergedrag. Een organisatiecultuur die werknemers aanmoedigt om hun stem te laten horen werd beschouwd als een essentiële factor om veerkrachtte realiseren.

Het opnemen van gedragsaspecten in deze cyberaudit leidde tot diepere inzichten en nuttige aanbevelingen, waardoor de organisatie beter in staat was om risico's te beheersen in een van haar meest kritieke domeinen.

Bijlage B. Casestudies van specifieke audits

Casestudie 1: Afdeling Huisvesting (Publieke Sector)

De voorbeelden in deze casestudy laten zien hoe de internal auditfunctie van een overheidsinstantie de Organisatiegedrag Topical Requirement zou toepassen om te beoordelen hoe de instantie voldoet aan haar doelstelling om rechtvaardige huisvestingsdiensten aan het publiek te leveren. Internal auditors moeten erkennen dat de politieke beleidskeuzen, politieke gevoeligheden, begrotingstoewijzingen en sommige beleidskeuzes buiten hun bereik liggen. Echter, de manier waarop leidinggevenden en managers dit beleid interpreteren en toepassen en de interne cultuur van het departement vallen wel binnen de scope.

Governance

A. Rollen en verantwoordelijkheden - De afdeling heeft een duidelijke organisatiestructuur met een scheiding tussen de verantwoordelijkheid voor beleidsontwerp (hoge ambtenaren) en huisvesting. Een deel van de doelstelling van de internal auditfunctie voor de opdracht is om te bepalen of structurele belangenconflicten worden vermeden: is de verantwoordelijkheid voor de naleving van het beleid bijvoorbeeld gescheiden van het toezicht op aannemers?

B. Verantwoording afleggen - Het hoofd van de organisatie en het senior management hebben verantwoordelijkheden toegewezen gekregen voor organisatorische doelstellingen die gekoppeld zijn aan culturele resultaten, zoals eerlijkheid in de toewijzing van huisvesting en het welzijn van het personeel. De internal auditfunctie evalueert of verantwoording zichtbaar is en geaccepteerd wordt.

C. Toezicht en controle - Een "cultuurcommissie" onder voorzitterschap van een senior manager beoordeelt elk kwartaal de personeelsenquêtes, klokkenluidersgegevens en klachten van belanghebbenden. Auditors beoordelen of deze processen vroegtijdig waarschuwen voor afwijkend gedrag.

D. Beleid en procedures - Gedragscodes, richtlijnen voor de toewijzing van huisvesting en registers van belangenconflicten die op de juiste manier zijn geautoriseerd, bestaan en worden periodiek herzien (bijvoorbeeld minimaal twee keer per jaar). De internal auditfunctie beoordeelt of updates de lessen weerspiegelen die zijn geleerd uit huisvestingschandalen en openbare auditrapporten.

Risicomanagement

A. Kader voor gedragsrisico's - De afdeling identificeert culturele risico's die van invloed kunnen zijn op het leveren van openbare diensten, zoals vriendjespolitiek bij het toewijzen van huisvesting, buitensporige bureaucratie of terughoudendheid bij

werknemers om overheidsrichtlijnen aan te vechten. De internal auditfunctie zorgt ervoor dat deze risico's formeel worden vastgelegd in het risicoregister, door het management worden overwogen en indien nodig worden aangepakt.

B. Indicatoren en analyses - Dashboards houden gedragsgegevens bij, zoals personeelsverloop, klachten, aantal informele klachten van huurders en het publiek, en reacties op verzoeken om openbare documenten of vrijheid van informatie. Auditors beoordelen of indicatoren en analyses betrouwbaar zijn en binnen het agentschap worden besproken.

C. Managen van afwijkingen - Als er verschillen ontstaan (bijvoorbeeld gevallen van klokkenluiden waaruit blijkt dat er wordt afgeweken van de principes van eerlijkheid), worden deze geëscaleerd naar de hogere leidinggevenden. Auditors controleren of de analyse van afwijkingen leidt tot corrigerende maatregelen.

D. Inbreng van belanghebbenden in oplossingen - Bevoegde autoriteiten, woningcorporaties, vakbonden en burgerpanels worden geraadpleegd wanneer culturele problemen (zoals onbeleefdheid van eerstelijns personeel of vooringenomenheid bij de toewijzing) worden vastgesteld. Auditors gaan na of de feedback invloed heeft op de resolutieplannen.

Beheersing

A. Beoordeling van gedragsrisico's - Beoordeling achteraf wordt uitgevoerd na mislukkingen van huisvestingsprojecten (bijvoorbeeld vertragingen in de bouw van sociale woningen). Auditors controleren of de onderliggende oorzaken van gedrag (zoals slechte samenwerking, schuldcultuur) worden beoordeeld.

B. Toonzetting - Senior managers communiceren verwachtingen over eerlijkheid, onpartijdigheid en servicekwaliteit via bedrijfsbrede bijeenkomsten en intranetvideo's. Internal auditors gaan na of men zich bewust is van deze verwachtingen en of ze worden nageleefd.

C. Escalatiemechanismen - De afdeling heeft een hotline voor klokkenluiders die toegankelijk is voor het publiek en een klachtenprocedure voor huurders, personeel en het algemene publiek. De auditors onderzoeken de tijdigheid, vertrouwelijkheid en het bewijs dat meldingen zonder represailles zijn gedaan.

D. Incentives - Prestatiebeoordelingen benadrukken de samenwerking tussen medewerkers, de betrokkenheid van belanghebbenden en eerlijkheid in de interacties met huurders. Auditors beoordelen of promoties en beloningen dit gedrag versterken.

E. Monitoren van gedrag - Lijnmanagers beoordelen medewerkers op gedragsnormen (integriteit, empathie met kwetsbare huurders) tijdens jaarlijkse beoordelingen. Auditors bepalen of resultaten consistent zijn en of patronen van slecht gedrag worden aangepakt.

F. Training - Verplichte programma's over onbewuste vooroordelen, conflictoplossing en ethische besluitvorming bij de toewijzing van woningen. Auditors gaan na of de voltooiingspercentages hoog zijn en beoordelen de resultaten van enquêtes na de training.

G. Herstelprocessen - Wanneer culturele inbreuken (zoals manipulatie van wachtlijsten voor huisvesting) worden vastgesteld, worden analyses van de hoofdoorzaken uitgevoerd en actieplannen opgevolgd. Auditors controleren of de herstelmaatregelen effectief en duurzaam zijn.

Inzicht

Hoewel publieke beleidskeuzes en het ontwerp van beleid op hoog niveau buiten de scope en invloed van de internal auditfunctie vallen, zijn de bestuurs-, risico- en beheersstructuren van de afdeling rond gedrag wel te auditen. Het toepassen van alle 15 vereisten in Organisatiegedrag Topical Requirement zorgt ervoor dat internal auditors kunnen evalueren of organisatiegedrag van invloed is op de manier waarop huisvestingsdiensten worden geleverd, zoals op een eerlijke, transparante en op waarden afgestemde manier, ondanks de politieke context.

Casestudie 2: Klein bouwbedrijf (kleine internal auditfunctie)

De internal auditfunctie van een fictief bouwbedrijf van 50 personen is bezorgd dat de Organisatiegedrag Topical Requirement is ontworpen voor grote, complexe organisaties. Dezelfde principes zijn echter van toepassing - op maat geschaald. Zelfs zonder een subcommissie van het bestuur of geavanceerde dashboards kan het bedrijf nog steeds aantonen dat het voldoet aan alle 15 vereisten in de actuele vereiste.

Governance

A. Rollen en verantwoordelijkheden - De senior manager van het bedrijf delegeert de personeelsverantwoordelijkheid formeel aan de officemanager en het projecttoezicht aan de locatiemanagers. Internal auditors beoordelen of de rollen duidelijk zijn en of conflicten (bijvoorbeeld beide rollen keuren goed en houden toezicht op de uitgaven van contractanten) worden vermeden.

B. Verantwoording afleggen - Elke manager tekent elk kwartaal een verklaring waarin de verantwoordelijkheid voor het gedrag van het team wordt bevestigd, inclusief het naleven van de veiligheidsregels en de behandeling van onderaannemers. Auditors beoordelen of deze verklaringen redelijk zijn en er toezicht op is.

C. Toezicht en monitoring - Het management komt maandelijks bijeen om het personeelsverloop, klachten van klanten en veiligheidsrapporten over projecten te bespreken. Auditors controleren of cultuurgerelateerde kwesties worden aangekaart en bijgehouden.

D. Beleid en procedures - De auditors controleren of schriftelijke gedragscodes, veiligheidsprotocollen en richtlijnen tegen pesten jaarlijks worden herzien en aan het personeel worden meegedeeld.

Risicomanagement

A. Kader voor gedragsrisico's - Het bedrijf identificeert risico's zoals het overhaasten of vermijden van het volgen van alle vereiste veiligheidsprocedures om deadlines te halen,

vriendjespolitiek bij het toewijzen van overuren en pesterijen op bouwplaatsen. Auditors controleren of deze risico's zijn opgenomen in het risicoregister.

B. Indicatoren en analyses - In plaats van dashboards gebruikt het bedrijf eenvoudige spreadsheets om afwezigheden, klachten en veiligheidsincidenten bij te houden. Auditors beoordelen of deze gebieden aan het licht brengen die zouden moeten worden herzien.

C. Beheer van afwijkingen - Als uit personeelsenquêtes blijkt dat er een kloof is tussen de "verwachtingen" en de "werkelijke ervaring", moeten managers tijdens de volgende vergadering corrigerende maatregelen voorstellen. Auditors bepalen of acties worden geïmplementeerd en afgesloten.

D. Inbreng van belanghebbenden in oplossingen - Bevoegde autoriteiten, werknemersvertegenwoordigers en soms belangrijke klanten worden uitgenodigd om commentaar te geven wanneer er culturele problemen opduiken. Auditors bepalen of het antwoord de ontvangen feedback weerspiegelt.

Beheersing

A. Risicobeoordelingen op basis van gedrag - Na elke mislukking van een project (zoals kostenoverschrijdingen door slechte samenwerking) houdt de senior manager een sessie over "geleerde lessen". Auditors controleren of culturele oorzaken (schuld, slechte communicatie) worden geregistreerd en of er beheersmaatregelen zijn geïmplementeerd om acties in de toekomst te corrigeren.

B. Toonzetting - De senior manager houdt elk kwartaal briefings voor het personeel om de waarden van eerlijkheid, kwaliteit en respect te versterken. Internal auditors verzamelen feedback van medewerkers om te testen of de toon aanslaat.

C. Escalatiemechanismen - Er is geen formele hotline, maar een gesloten ideeënbus en directe toegang tot de senior manager bieden rapportagekanalen. De auditors gaan na of het personeel ze gebruikt en of er een beschermingsbeleid bestaat.

D. Incentives - Bonusbetalingen zijn bescheiden, maar gekoppeld aan teamwerk en feedback van klanten, niet alleen aan het halen van projectdeadlines. Auditors controleren of de toewijzing van beloningen consistent en redelijk is.

E. Monitoren van gedrag - Supervisors geven informele feedback over het gedrag van medewerkers tijdens functioneringsgesprekken. Auditors beoordelen of feedback consistent wordt toegepast in teams.

F. Training - Jaarlijks worden er korte workshops gegeven over respect op het werk en veiligheid op de werkplek. Auditors verifiëren aanwezigheid en effectiviteit door middel van steekproeven.

G. Herstelprocessen - Als er sprake is van pesten of wangedrag, onderzoekt de senior manager (of indien nodig een hogere autoriteit) de zaak, documenteert deze en dwingt resultaten af. Auditors controleren of sancties of corrigerende maatregelen tijdig en proportioneel zijn.

Inzicht

Zelfs zonder een tweede lijn of een subcommissie van het bestuur kan een klein bedrijf alle 15 vereisten van de organisatorische gedragsvereiste toepassen via kleinere mechanismen - eenvoudige registers, direct toezicht van de senior manager, informele beoordelingen en proportionele training. Dit toont aan dat de Topical Requirement praktisch en relevant is voor alle organisaties, ongeacht hun omvang.

Bijlage C. Optioneel hulpmiddel voor documentatie

Van internal auditors wordt verwacht dat zij hun professionele oordeel gebruiken bij het bepalen van de toepasbaarheid van de vereisten op basis van de risicobeoordeling en dat zij de uitsluiting van bepaalde vereisten op passende wijze documenteren. De Topical Requirement kan worden gedocumenteerd in het internal auditplan of in de werkdocumenten van de betreffende opdracht, op basis van de professionele oordeelsvorming van de auditor. Eén of meer internal auditopdrachten kunnen de vereisten afdekken. Daarnaast kan het zijn dat niet alle vereisten van toepassing zijn. Het afdrukbare formulier hieronder biedt een optie voor het documenteren van conformiteit met de Organisatiegedrag Topical Requirement, maar het gebruik ervan is niet verplicht.

Governance van organisatiegedrag

Vereiste	Uitgevoerde dekking of reden voor uitsluiting	Documentatie Referentie
A. Het bestuur houdt toezicht en het senior management structureert rollen en verantwoordelijkheden om onbedoelde gevolgen van ongewenst organisatiegedrag te voorkomen. Onbedoelde gevolgen omvatten belangenconflicten of onduidelijke besluitvormingsprocessen.		
B. Het bestuur houdt toezicht en het senior management stelt en handhaaft individuele en groepsverantwoordelijkheid voor gewenst gedrag en zorgt ervoor dat rollen en verantwoordelijkheden worden erkend, begrepen en consistent in lijn zijn met de doelstellingen van de organisatie.		

Vereiste	Uitgevoerde dekking of reden voor uitsluiting	Documentatie Referentie
C. Er zijn bestuursprocessen om te zorgen voor regelmatig toezicht, evaluatie en ter discussie stellen van de afstemming tussen het vertoonde gedrag en organisatiedoelstellingen en om actie te ondernemen bij eventuele discrepanties.		
D. Beleid en procedures met betrekking tot gedrags(risico)protocollen worden opgesteld en periodiek beoordeeld op relevantie en nauwkeurigheid. Dit beleid en deze procedures worden effectief gecommuniceerd en geïntegreerd in de activiteiten en besluitvormingsprocessen van de organisatie.		

Risicomanagement van organisatiegedrag

Vereiste	Uitgevoerde dekking of reden voor uitsluiting	Documentatie Referentie
A. De organisatie heeft op de juiste manier een aanpak gedefinieerd voor het managen van gedragsrisico's, inclusief de gedragskenmerken die cruciaal zijn voor het behalen van de organisatiedoelstellingen.		
B. Het monitoren van organisatiegedrag is adequaat en tijdig, met resultaten die worden gecommuniceerd naar belanghebbenden.		
C. Hiaten tussen gedragsverwachtingen en feitelijk gedrag, samen met bijbehorende oorzakenanalyses, worden effectief en consistent gecommuniceerd naar belanghebbenden.		

Vereiste	Uitgevoerde dekking of reden voor uitsluiting	Documentatie Referentie
D. Verschillen tussen gedragsverwachtingen en feitelijk gedrag worden opgelost met inbreng van belanghebbenden. De oplossingen worden gevolgd tot ze zijn voltooid en effectief gemeten om ervoor te zorgen dat voldoende acties zijn ondernomen.		

Beheersing van organisatiegedrag

Vereiste	Uitgevoerde dekking of reden voor uitsluiting	Documentatie Referentie
A. De organisatie heeft een aanpak ontworpen om gedragspatronen die risico's kunnen opleveren voor het behalen van de organisatiedoelstellingen binnen de organisatie te identificeren en te beperken. Voorbeelden hiervan zijn prestatiebeoordelingen en beoordelingen van operationele risico's met betrekking tot gedrag.		
B. De organisatie zet een duidelijke en consistente toon met betrekking tot gewenst gedrag en communiceert deze verwachtingen via vertrouwde en toegankelijke kanalen. Er is een gestructureerd feedbackmechanisme om het begrip en de steun van werknemers te beoordelen en waar nodig veranderingen mogelijk te maken.		
C. Er zijn processen ingesteld om het rapporteren van organisatiegedrag dat in strijd is met het bereiken van de doelstellingen van de organisatie aan te moedigen. De processen omvatten beschermings- en oplossingsprotocollen.		

Vereiste	Uitgevoerde dekking of reden voor uitsluiting	Documentatie Referentie
D. Stimuleringsprogramma's, waaronder beloningen en niet-monetaire beloningen, zijn aanwezig, worden gecommuniceerd en zijn afgestemd op de doelstellingen van de organisatie en wettelijke vereisten. Ontmoediging en consequenties voor ongepast organisatiegedrag zijn daarin ook opgenomen.		
E. Er is een proces om problemen te managen, inclusief het identificeren en corrigeren van gedragspatronen die niet in lijn zijn met de doelstellingen van de organisatie en het escaleren van problemen indien nodig.		
F. Trainings- en bewustwordingsprogramma's die zijn ontworpen om ervoor te zorgen dat het gedrag van de organisatie en de doelstellingen van de organisatie op elkaar zijn afgestemd, worden periodiek en effectief gegeven.		
G. De processen voor het werven en inwerken van talent zijn afgestemd op de gedragsverwachtingen van de organisatie en omvatten gedragscompetenties.		

Bijlage D. Mapping met het COSO-raamwerk

De onderstaande grafiek vergelijkt de vereisten voor governance, risicomanagement en beheersprocessen van de Organisatiegedrag Topical Requiremen met het *COSO Internal Control - Integrated Framework* (2013) en het *COSO Enterprise Risk Management Framework* (2017). Deze kruisverwijzing stelt internal auditors in staat om hun op COSO gebaseerde tests af te stemmen op de dekking van de Organisatiegedrag Topical Requirement.

Vereisten voor Governance

Vereiste	COSO Internal Control (2013) Referentie	COSO ERM (2017) Referentie
A. Het bestuur houdt toezicht en het senior management structureert rollen en verantwoordelijkheden om onbedoelde gevolgen vanongewenst organisatiegedrag te voorkomen. Onbedoelde gevolgen zijn bijvoorbeeld belangenconflicten of onduidelijke besluitvormingsprocessen.	Beheersomgeving - Principes 2 (onafhankelijkheid van bestuur en toezicht op escalatiekanalen), 3 (structuur, autoriteit en verantwoordelijkheid).	Governance & Cultuur - Principe 1 (oefent als bestuur toezicht uit op risico), 2 (stelt operationele structuren vast).
B. Het bestuur houdt toezicht en het senior management stelt en handhaaft individuele en groepsverantwoordelijkheid voor gewenst gedrag en zorgt ervoor dat rollen en verantwoordelijkheden worden erkend, begrepen en consistent in lijn zijn met de doelstellingen van de organisatie.	Beheersomgeving - Principes 1 (integriteit en ethische waarden), 5 (verantwoording en prestatiemetingen).	Governance & Cultuur - Principes 4-5 (toont betrokkenheid bij kernwaarden; trekt bekwame mensen aan, ontwikkelt ze en houdt ze vast).

Vereiste	COSO Internal Control (2013) Referentie	COSO ERM (2017) Referentie
C. Er zijn bestuursprocessen om te zorgen voor regelmatige toezicht, evaluatie en ter discussie stellen van de afstemming tussen het vertoonde gedrag en organisatiedoelstellingen en om actie te ondernemen bij eventuele discrepanties.	Monitoring - Principe 16 (doorlopende/afzonderlijke evaluaties), 17 (evalueert en communiceert tekortkomingen); Informatie & Communicatie - Principe 13 (gebruikt relevante informatie), 14 (communiceert intern), 15 (communiceert extern, indien relevant).	Governance & Cultuur - Principe 1 (oefent als bestuur toezicht uit op risico); Prestaties - Principes 10-14 (identificeert risico's, beoordeelt de ernst ervan, prioriteert risico's, implementeert risicomaatregelen); Informatie, Communicatie & Rapportage - Principes 18-20 (training/rapportage over bewustzijn).
D. Beleid en procedures met betrekking tot gedrags(risico)protocollen worden opgesteld en periodiek beoordeeld op relevantie en nauwkeurigheid. Dit beleid en deze procedures worden effectief gecommuniceerd en geïntegreerd in de bedrijfsactiviteiten en besluitvormingsprocessen.	Controleactiviteiten - Uitgangspunten 10 (selecteert en ontwikkelt beheersactiviteiten), 12 (implementeert door middel van beleid en procedures).	Review & Herziening - Principes 15-17 (beoordeelt verandering; reviewt prestaties; streeft naar verbetering).

Vereisten voor Risicomanagement

Vereiste	COSO Internal Control (2013) Referentie	COSO ERM (2017) Referentie
A. De organisatie heeft op de juiste manier een aanpak gedefinieerd voor het managen van gedragsrisico's, inclusief de gedragskenmerken die cruciaal zijn voor het behalen van de organisatiedoelstellingen.	Risicobeoordeling - Principes 6 (specificeert geschikte doelstellingen), 7 (identificeert en analyseert risico), 8 (beoordeelt frauderisico), 9 (identificeert en analyseert significante verandering).	Governance & Cultuur - Principes 3-5 (toont betrokkenheid bij kernwaarden; trekt bekwame mensen aan, ontwikkelt ze en houdt ze vast); Strategie &Doelstellingbepaling Principes 6-9 (definieert risicobereidheid, evalueert alternatieve strategieën, houdt rekening met risico's in doelstellingen).
B. Het monitoren van organisatiegedrag is adequaat en tijdig, met resultaten die worden gecommuniceerd naar belanghebbenden.	Informatie & Communicatie - Principe 13 (gebruikt relevante informatie), 14 (communiceert intern); Monitoring - Principe 16 (doorlopende/afzonderlijke evaluaties), 17 (evalueert en communiceert tekortkomingen).	Prestaties - Principes 10-14 (identificeert risico's, beoordeelt de ernst ervan, prioriteert risico's, implementeert risicomaatregelen); Informatie, communicatie & Rapportage - Principes 18-20 (training/bewustzijnsrapportage).

Vereiste	COSO Internal Control (2013) Referentie	COSO ERM (2017) Referentie
C. Verschillen tussen gedragsverwachtingen en feitelijk gedrag worden, samen met bijbehorende oorzakenanalyses, effectief en consistent gecommuniceerd naar belanghebbenden.	Informatie & Communicatie - Principes 14 (communiceert intern), 15 (communiceert extern, indien relevant).	Informatie, communicatie & Rapportage - Principes 19-20 (communiceert informatie over risico's; rapporteert over risico's, cultuur en prestaties).
D. Verschillen tussen gedragsverwachtingen en feitelijk gedrag worden opgelost met inbreng van belanghebbenden. De oplossingen worden gevolgd tot ze zijn voltooid en effectief gemeten om ervoor te zorgen dat voldoende acties zijn ondernomen.	Controleactiviteiten - Principe 10 (selecteert en ontwikkelt beheersactiviteiten), 12 (implementeert door middel van beleid en procedures); Monitoring - Principe 16 (doorlopende/afzonderlijke evaluaties), 17 (evalueert en communiceert tekortkomingen).	Herziening & Herziening - Principes 15-17 (beoordeelt verandering; reviewt prestaties; streeft naar verbetering).

Vereisten voor beheersing

Vereiste	COSO Internal Control controle (2013) Referentie	Documentatie Referentie
A. De organisatie heeft een aanpak ontworpen om gedragspatronen die risico's kunnen opleveren voor het behalen van de organisatiedoelstellingen binnen de organisatie te identificeren en te beperken. Voorbeelden hiervan zijn prestatiebeoordelingen en beoordelingen van operationele risico's met betrekking tot gedrag.	Risicobeoordeling - Uitgangspunten 7 (identificeert en analyseert risico's), 8 (beoordeelt frauderisico's), 9 (identificeert en analyseert significante verandering); Toezicht - Uitgangspunten 16 (doorlopende/afzonderlijke evaluaties), 17 (evalueert en communiceert tekortkomingen).	Prestaties - Principes 10-14 (identificeert risico's, beoordeelt de ernst ervan, prioriteert risico's, implementeert risicomaatregelen); Beoordeling & Herziening - Principes 15-17 (beoordeelt verandering; beoordeelt prestaties; streeft naar verbetering).
B. De organisatie zet een duidelijke en consistente toon met betrekking tot gewenst gedrag en communiceert deze verwachtingen via vertrouwde en toegankelijke kanalen. Er is een gestructureerd feedbackmechanisme om het begrip en de steun van werknemers te beoordelen en waar nodig veranderingen mogelijk te maken.	Beheersomgeving - Principes 1 (integriteit en ethische waarden), 5 (verantwoording en prestatiemetingen); Informatie & Communicatie - Principes 13 (gebruikt relevante informatie), 14 (communiceert intern), 15 (communiceert extern, indien relevant).	Governance & Cultuur - Principes 1 (oefent als bestuur toezicht uit op risico's), 4 (toont betrokkenheid bij kernwaarden), 5 (trekt bekwame mensen aan, ontwikkelt ze en houdt ze vast); Informatie, communicatie & Rapportage - Principes 18-20 (training/bewustzijnsrapportage).

Vereiste	COSO Internal Control controle (2013) Referentie	Documentatie Referentie
C. Er zijn processen om het rapporteren van organisatiegedrag dat in strijd is met het bereiken van de doelstellingen van de organisatie aan te moedigen. De processen omvatten beschermings- en oplossingsprotocollen.	Informatie & Communicatie - Principe 14 (interne communicatiekanalen); Beheersomgeving - Principe 2 (onafhankelijkheid van het bestuur en toezicht op escalatiekanalen).	Governance & Cultuur - Principes 1 (oefent als bestuur toezicht uit op risico's), 4 (toont betrokkenheid bij kernwaarden), 5 (trekt bekwame mensen aan, ontwikkelt ze en houdt ze vast); Informatie, communicatie & Rapportage - Principes 19-20 (communiceert over risico-informatie; rapporteert over risico's, cultuur en prestaties).
D. Stimuleringsprogramma's, waaronder beloningen en niet-monetaire beloningen, zijn aanwezig, worden gecommuniceerd en zijn afgestemd op de doelstellingen van de organisatie en wettelijke vereisten. Ontmoedigingen en consequenties voor ongepast organisatiegedrag zijn daarin ook opgenomen.	Beheersomgeving - Principes 1 (integriteit en ethische waarden integriteit en ethische waarden), 5 (verantwoording en prestatiemetingen).	Governance & Cultuur - Principes 4 (toont betrokkenheid bij kernwaarden), 5 (bekwame mensen aantrekken, ontwikkelen en behouden); Prestaties - Principes 10-14 (identificeert risico's, beoordeelt de ernst ervan, prioriteert risico's, implementeert risicomaatregelen).
E. Er is een proces om problemen te managen, inclusief het identificeren en corrigeren van gedragspatronen die niet in lijn zijn met de doelstellingen van de organisatie en het escaleren van problemen indien nodig.	Monitoring - Principe 16 (doorlopende/afzonderlijke evaluaties), 17 (evalueert en communiceert tekortkomingen); Informatie & Communicatie - Principe 13 (gebruikt relevante informatie).	Review & Herziening - Principes 15-17 (beoordeelt verandering; beoordeelt prestaties; streeft naar verbetering); Prestaties - Principes 10-14 (identificeert risico's, beoordeelt de ernst, prioriteert risico's, implementeert risicomaatregelen).
F. Trainings- en bewustwordingsprogramma's die zijn ontworpen om ervoor te zorgen dat het gedrag van de organisatie en de doelstellingen van de organisatie op elkaar zijn afgestemd, worden periodiek en effectief gegeven.	Beheersomgeving - Principe 4 (toewijding aan competentie); Informatie & Communicatie - Principe 13 (gebruikt relevante informatie).	Governance & Cultuur - Principe 5 (bekwame mensen aantrekken, ontwikkelen, behouden); Informatie, Communicatie & Rapportage - Principes 18-20 (training/bewustzijnsrapportage).
G. De processen voor het werven en inwerken van talent zijn afgestemd op de gedragsverwachtingen van de organisatie en bevatten gedragscompetenties.	Beheersomgeving - Principes 1 (integriteit en ethische waarden), 4 (toewijding aan competentie).	Governance & Cultuur - Principe 5 (bekwame mensen aantrekken, ontwikkelen en behouden).

Bijlage E. Audit- en controleactiviteiten gericht op gedrag

Internal auditors kunnen merken dat het werk dat ze al doen van pas komt bij het toepassen van de Organisatiegedrag Topical Requirement. Deze tabel noemt een aantal gerichte audits en veelvoorkomende auditelementen die kunnen overeenkomen met de vereisten en die kunnen worden gebruikt om conformiteit aan te geven, indien van toepassing. Deze voorbeelden moeten niet worden gezien als verplichte audits; ze worden eerder gegeven om te laten zien hoe vaak uitgevoerde auditactiviteiten mogelijk dekking bieden voor Topical Requirements.

Voorbeelden van audits en assurance-activiteiten die gedrag direct/indirect kunnen adresseren, zijn onder andere:

Gebied	Gerichte audits	Veelvoorkomende beoordelingselementen in audits
Governance	• Risicocultuur • Corporate governance • Beoordeling effectiviteit bestuur/leiderschap • Reactie op wet-/regelgeving • Prestatiebeloning • Prestatiemetingen • Bedrijfsstrategie en -planning • Transformatieplanning • Fusies en overnames	• Bedrijfsbeleid en -procedures • Beheersmaatregelen op entiteitsniveau/ managementbeoordeling • Aanpak van organisatiebrede regelgevingskwesties (bijvoorbeeld bedrijfsverbeteringsplan) • Delegatie van bevoegdheden
Risicomanagement	• Juridische functie en compliance • Raamwerk voor risicomanagement • Programma voor ethiek en compliance • ESG • Fraudeonderzoek/ klokkenluidershotline	• Bijhouden van risico- en beheersregisters • Zelfevaluaties van het management • Reactie op falende beheersmaatregelen en audit/andere bevindingen
Beheersing	• Personeelszaken (inclusief werving en behoud) • Verkoopprocessen (bijvoorbeeld verkoopgedrag en compliance) • Inkoop (bijvoorbeeld onafhankelijkheid van leveranciers, entertainment) • Sector/entiteit (bijvoorbeeld management en beoordeling) • Fraude/klokkenluidershotline	• Functiescheiding • Managementbeoordeling en toezicht op beheersmaatregelen • Individuele frauderisico's • Competentievaardigheden en risicobewustzijn • Herstel van processen en beheersmaatregelen

Over het Instituut van Internal Auditors

Het IIA is een internationale beroepsvereniging die wereldwijd meer dan 265.000 leden telt en wereldwijd meer dan 200.000 Certified Internal Auditor® (CIA®) certificeringen heeft uitgereikt. Het IIA is opgericht in 1941 en wordt over de hele wereld erkend als de leider van het internal auditberoep op het gebied van standaarden, certificeringen, onderwijs, onderzoek en technische begeleiding. Ga voor meer informatie naar theiia.org.

Disclaimer

Copyright

December 2025

The Institute of Internal Auditors

Global Headquarters
The Institute of Internal Auditors
1035 Greenwood Blvd., Suite 401
Lake Mary, FL 32746, USA
Phone: +1-407-937-1111
Fax: +1-407-937-1101