International Professional Practices Framework

Implementatierichtlijn

Gedragscode: vertrouwelijkheid

Beginsel 3 van de Gedragscode van het IIA: vertrouwelijkheid

Internal auditors hebben respect voor de waarde en het eigendom van de informatie die zij ontvangen. Zij maken geen informatie openbaar zonder daarvoor toestemming te hebben verkregen, tenzij er een wettelijke of professionele plicht daartoe bestaat.

Gedragsregels

Internal auditors:

3.1. Zijn behoedzaam in het gebruik en de bescherming van informatie die zij gedurende hun activiteiten hebben verzameld.

3.2. Gebruiken geen informatie voor persoonlijk gewin of op een wijze die in strijd is met de wet of die schadelijk is voor de wettelijke en ethische doelstellingen van de organisatie.

Aan de slag

De *internationale standaarden voor de beroepsuitoefening van internal auditing* vereisen naleving van de Gedragscode, die vier beginselen omvat. Bij elk beginsel horen gedragsregels die internal auditors moeten toepassen om het beginsel op de juiste wijze uit te dragen. Doel van deze implementatierichtlijn is duidelijk te maken hoe naleving van het beginsel vertrouwelijkheid kan worden bereikt.

Uitgangspunt daarbij is dat internal auditors een goed inzicht hebben in hun beroepsmatige verplichtingen, zoals aangegeven in het IPPF en aanvullende beroepsstandaarden en -richtlijnen die van belang zijn voor de organisatie en de sector waarin zij werkzaam zijn. Door lid te zijn van

beroepsorganisaties kunnen internal auditors op de hoogte blijven van relevante beroepsmatige verplichtingen.

Informatie omvat data in fysieke vorm, zoals gedrukte documenten, en in elektronische vorm, zoals audio-, video- en versleutelde data. Vertrouwelijkheid behelst het beschermen van informatie tegen bekendmaking aan onbevoegde personen en entiteiten, zowel binnen als buiten de organisatie. Internal auditors moeten op de hoogte zijn van de wet- en regelgeving met betrekking tot vertrouwelijkheid en informatiebeveiliging voor de rechtsgebieden waarin hun organisatie opereert. Ook moeten ze de specifieke beleidsmaatregelen van hun organisatie en de internal auditfunctie kennen. Deze beleidsmaatregelen kunnen bijvoorbeeld het soort informatie vaststellen dat bekend mag worden gemaakt, de partijen die de bekendmaking moeten goedkeuren en de te volgen procedures.

Vertrouwelijkheid wordt niet expliciet genoemd in de *Standaarden*. Wel worden de eisen voor het beperken van de publicatie van opdrachtresultaten besproken in de implementatiestandaarden 2201.A1, 2330.A1, 2330.C1, 2410.A3 en 2440.A2. Internal auditors moeten deze standaarden, de implementatierichtlijnen en relevante aanvullende richtlijnen van het IIA bestuderen.

Overwegingen bij de implementatie

Hoofd van de internal auditfunctie

Beleid en procedures

Organisaties vaardigen gewoonlijk een informatiebeveiligingsbeleid uit om de data die ze verkrijgen, gebruiken en voortbrengen te beschermen en om naleving te waarborgen van de wet- en regelgeving met betrekking tot de sector en het rechtsgebied waarin ze actief zijn (bijv. de algemene verordening gegevensbescherming van de Europese Unie of het EU-U.S. Privacy Shield Framework). Deze beleidsmaatregelen worden geïmplementeerd middels specifieke procedures en andere beheersmaatregelen. Doorgaans betreffen deze beleidsmaatregelen gegevensbescherming, bewaartermijnen en fysieke en digitale beveiliging van informatie binnen en buiten de organisatie.

Om een beter inzicht te krijgen in de gevolgen van wettelijke eisen en beschermende regelgeving (bijv. beroepsgeheim of verschoningsrecht), moet het hoofd van de internal auditfunctie juridisch advies inwinnnen. De beleidsmaatregelen en procedures van de organisaties verlangen soms dat bepaalde autoriteiten bedrijfsinformatie beoordelen en goedkeuren voordat deze naar buiten wordt gebracht.

Het hoofd van de internal auditfunctie kan aanvullende beleidsmaatregelen, processen en/of procedures implementeren waar de internal auditfunctie en externe consultants zich aan moeten houden. Vaak sluiten deze maatregelen en processen nauw aan op de Verplichte richtlijnen van het IPPF. Internal auditors moeten zich houden aan de beleidsmaatregelen en procedures die door de organisatie en het hoofd van de internal auditfunctie zijn vastgesteld, en ook relevante wet- en regelgeving in acht nemen.

Ter bescherming van bedrijfseigen informatie kunnen beleidsmaatregelen en procedures internal auditors soms verplichten de volgende voorzorgsmaatregelen te nemen, ook wanneer ze informatie intern verwerken:

- Verzamel alleen data die nodig zijn om de toegewezen opdracht uit te voeren en gebruik deze informatie uitsluitend voor de beoogde doelen van de opdracht.
- Bescherm informatie tegen opzettelijke of niet-opzettelijke bekendmaking door het toepassen van beheersmaategelen, zoals dataversleuteling, beperking van de verspreiding van e-mails en beperking van de fysieke toegang tot informatie.
- Vernietig kopieën van of voorkom toegang tot dergelijke data wanneer deze gegevens niet langer nodig zijn.

Een voorbeeld van informatie die gewoonlijk wordt beschermd tegen interne bekendmaking is persoonlijke informatie van de personeelsafdeling. Denk hierbij aan individuele salarissen en gegevens van berispingen of persoonlijke problemen die met leidinggevenden en HR-medewerkers zijn besproken. Toegang tot deze informatie kan worden beperkt of bewaakt via fysieke maatregelen, zoals afgesloten archiefkasten, en via controlemaatregelen in het informatiesysteem, zoals wachtwoordbeveiliging en versleuteling van data. Het hoofd van de internal auditfunctie moet periodiek beoordelen en bevestigen of internal auditors toegang moeten hebben tot ruimtes en databanken met vertrouwelijke informatie. Ook dient het hoofd te bevestigen dat de toegangsmaatregelen doeltreffend werken.

Volgens de implementatiestandaarden die horen bij Standaard 2330 – Documenteren van informatie, moet het hoofd van de internal auditfunctie de toegang tot opdrachtdossiers beheren door onder andere eisen op te stellen voor het bewaren van de dossiers, ongeacht het medium waarop elk dossier is opgeslagen. Deze regels moeten overeenstemmen met de richtlijnen van de organisatie en met alle toepasselijke regelgeving of overige vereisten.

Daarnaast verplicht Standaard 2440.A2 het hoofd van de internal auditfunctie om het potentiële risico van verspreiding van de resultaten van een assurance-opdracht te evalueren en om het gebruik van resultaten van de assurance-opdracht te beperken, behalve voor zover dit wettelijk, statutair of reglementair is vereist. Opdrachtrapporten bevatten vaak distributielijsten die zijn goedgekeurd door het hoofd van de internal auditfunctie, het senior management en het bestuur. Het feit dat de standaard rekening houdt met wettelijke, statutaire of reglementaire vereisten waarborgt dat het hoofd van de internal auditfunctie en internal auditors verzoeken van toezichthouders kunnen inwilligen. Ook kunnen ze hierdoor voldoen aan wetgeving op het gebied van transparantie voor organisaties in de publieke sector.

Training

Tijdens bijeenkomsten of trainingen van de internal auditfunctie kan het hoofd van de internal auditfunctie de beginselen, regels, beleidsmaatregelen en verwachtingen met betrekking tot vertrouwelijkheid bespreken. Internal auditors kunnen van de gelegenheid gebruikmaken om te brainstormen en te discussiëren over de mogelijke gevolgen van het delen van verschillende soorten vertrouwelijke informatie van de organisatie. Het hoofd van de internal auditfunctie mag internal auditors verzoeken een formulier te ondertekenen waarin ze verklaren dat ze deze sessies hebben bijgewoond en de toepasselijke beleidsmaatregelen, procedures en verwachtingen begrijpen. Het is voor het hoofd van de internal auditfunctie vooral van belang om als leider van deze functie de toon te zetten voor de waarde van ethiek binnen het team door de beginselen en gedragsregels van de Gedragscode hoog te houden.

Individuele internal auditors

Uiteindelijk zijn individuele internal auditors zelf verantwoordelijk voor het naleven van de Gedragscode. Dit speelt vooral tijdens het uitvoeren van internal auditopdrachten, waarbij internal auditors vertrouwelijke, bedrijfseigen en/of persoonlijke informatie ontvangen. Vaak gebruiken internal auditors gedurende de gehele opdracht deze informatie (bijv. tijdens het verzamelen van informatie over een te beoordelen activiteit en tijdens het toetsen).

Volgens Standaard 2330 – Documenteren van informatie, moeten internal auditors toereikende, betrouwbare, relevante en nuttige informatie documenteren ter ondersteuning van de resultaten en conclusies van de opdracht. Bij het documenteren van internal auditwerkzaamheden en bevindingen in werkdocumenten en rapporten van de opdracht moeten internal auditors rekening houden met de vertrouwelijkheid van deze informatie. Modellen voor het werkprogramma of werkdocumenten voor de opdracht kunnen een herinnering bevatten voor vertrouwelijkheid. Elektronische versies bevatten vaak geautomatiseerde controlemaatregelen waardoor internal auditors deze herinnering moeten bevestigen voordat ze toegang kunnen krijgen en hun werkdocument kunnen invullen.

Enkele standaarden die van belang zijn voor het plannen en uitvoeren van opdrachten vermelden specifiek het behoedzame gebruik en de bescherming van informatie, zoals beschreven in Regel 3.1. Internal auditors die een assurance-opdracht plannen waarbij partijen buiten de organisatie zijn betrokken, moeten een schriftelijke overeenkomst opstellen over de beperkingen in de verspreiding van de resultaten van de opdracht en in de toegang tot opdrachtdossiers (Standaard 2201.A1). Bij het vrijgeven van de resultaten van een assurance-opdracht aan partijen buiten de organisatie, moeten internal auditors de beperkingen aangegeven voor de verspreiding en het gebruik van de resultaten (Standaard 2410.A3).

Om te voldoen aan de gedragsregels met betrekking tot het vertrouwelijkheidsbeginsel, moeten internal auditors de vastgestelde procedures voor openbaarmaking volgen, waaronder contact opnemen met de juiste afdeling of persoon om toestemming te krijgen alvorens informatie bekend te maken. Internal

auditors kunnen hiertoe schriftelijke toestemming aanvragen en deze toestemming in hun werkdocumenten bewaren.

Tot slot benadrukt Gedragsregel 3.2 dat internal auditors informatie niet mogen gebruiken voor persoonlijk gewin. Zo mogen internal auditors geen voorwetenschap op financieel, strategisch of operationeel gebied van een organisatie gebruiken om daar zelf financieel beter van te worden door het kopen of verkopen van aandelen in de organisatie. Een ander voorbeeld is het zonder toestemming doorspelen van voorwetenschap aan journalisten of via andere media. Ook het gebruikmaken van voorwetenschap om een concurrerend product te ontwikkelen of het verkopen van bedrijfseigen informatie aan een concurrent zijn schendingen van deze vertrouwelijkheidsregel. Daarnaast mogen internal auditors geen misbruik maken van hun recht op toegang tot informatie, zoals toegang tot klantdossiers gebruiken om recente aankopen van een buurman op te zoeken of om de medische dossiers van een beroemdheid te bekijken.

Overwegingen bij het aantonen van naleving

Hoofd van de internal auditfunctie

Het hoofd van de internal auditfunctie kan aantonen dat internal auditing vertrouwelijkheid naleeft door bewijs te overleggen van geïmplementeerde beleidsmaatregelen, processen, procedures en trainingsmaterialen met betrekking tot vertrouwelijkheid (die van toepassing is op de internal auditfunctie en de organisatie). Ook notulen van bijeenkomsten en/of trainingen waar vertrouwelijkheid met leden van de internal auditfunctie is besproken tonen aan dat het hoofd van de internal auditfunctie het in acht nemen van vertrouwelijkheid ondersteunt.

Wat betreft het vrijgeven van resultaten of rapporten van de opdracht of daarmee verband houdende informatie geldt het volgende. Het hoofd van de internal auditfunctie toont naleving van het vertrouwelijkheidsbeginsel en de gedragsregels aan door het documenteren en bewaren van dossiers van bekendmakingen die zijn goedgekeurd door juridische adviseurs, indien van toepassing, en door het senior management en het bestuur. Het hoofd van de internal auditfunctie geeft blijk van toegangsbeheer tot dossiers door internal auditbeleidsmaatregelen en procedures te documenteren en te communiceren, en door mechanismen te implementeren die de toegang beperken en het risico van ontduiking of schending van deze beheersmaatregelen verkleinen.

Individuele internal auditors

Gegevens over het bijwonen van trainingen over vertrouwelijkheid moeten worden bewaard, samen met de handtekeningen van internal auditors ter bevestiging van hun inzicht in vertrouwelijkheid en toepasselijke beleidsmaatregelen, procedures en wet- en regelgeving. Ook kunnen functioneringsgesprekken met internal auditors feedback bevatten over de gevolgde beleidsregels en procedures met betrekking tot vertrouwelijkheid en de bekendmaking van informatie.

Internal auditors tonen aan dat ze bij opdrachtdossiers vertrouwelijkheid in acht hebben genomen door beperkingen in de verspreiding van werkdocumenten en rapporten van de opdracht te documenteren en door de toestemming voor alle bekendmakingen en goedgekeurde distributielijsten te bewaren. Een ondertekende verklaring waaruit blijkt dat informatie met betrekking tot de opdracht vertrouwelijk is gehouden, kan bij het werkprogramma worden bewaard.

Als er geen rapporten of onderzoeken zijn van individuele auditors die beleidsmaatregelen, procedures en regels betreffende vertrouwelijkheid hebben geschonden, is het aannemelijk dat de internal auditfunctie als geheel het beginsel naleeft.

Toepasselijkheid en handhaving van de Gedragscode

Deze Gedragscode is van toepassing op zowel entiteiten als individuele personen die internal audits verrichten.

Voor leden van het IIA en bezitters van of kandidaten voor een professioneel IIA-certificaat worden eventuele inbreuken op de gedragscode geëvalueerd en beheerd overeenkomstig de statuten en administratieve richtlijnen van het instituut. Het feit dan een specifieke gedraging niet wordt genoemd in de Gedragsregels houdt niet in dat deze onacceptabel of verwerpelijk is. Derhalve kunnen ook dergelijke gedragingen voor leden, certificaathouders en kandidaten disciplinaire maatregelen tot gevolg hebben.

Over het IIA

The Institute of Internal Auditors (IIA) is de meest erkende pleitbezorger, opleider en leverancier van standaarden en richtlijnen voor en certificeringen van internal auditors. Het IIA, opgericht in 1941, bedient op dit moment meer dan 190.000 leden uit meer dan 170 landen en regio's. Het wereldwijde hoofdkantoor van de vereniging bevindt zich in Lake Mary, Fla. USA. Ga voor meer informatie naar www.globaliia.org.

Over de Implementatierichtlijnen

Implementatierichtlijnen bieden als onderdeel van het International Professional Practices Framework® (IPPF®) van het IIA Aanbevolen (niet-verplichte) richtlijnen voor de internal auditberoepsgroep. Ze zijn bedoeld om zowel internal auditors als internal auditfuncties te ondersteunen bij het verbeteren van hun vermogen om te voldoen aan de *internationale standaarden voor de beroepsuitoefening van internal auditing (Standaarden).*

De Implementatierichtlijnen schetsen overwegingen die van toepassing kunnen zijn en mogelijke maatregelen om de Verplichte richtlijnen van het IIA te implementeren. De Implementatierichtlijnen specificeren geen programma's, processen, procedures of tools.

Andere gezaghebbende richtlijnen van het IIA kunt u vinden op onze website https://globaliia.org/standards-guidance.

Over de Gedragscode van het IIA

De Gedragscode van het IIA omvat twee essentiële componenten:

- Vier beginselen die van belang zijn voor het beroep en de praktijk van internal auditing.
- Gedragsregels voor elk beginsel, die de gedragsnormen omschrijven die worden verwacht van internal auditors.

Het doel van de Gedragscode van het IIA is het bevorderen van een ethische cultuur binnen het geheel van de beroepsgroep van internal audit.

De volledige Gedragscode kunt u vinden op https://globaliia.org/standards-guidance/mandatory-guidance/Pages/Code-of-Ethics.aspx.

Disclaimer

Het IIA publiceert dit document voor informatieve en educatieve doeleinden. Deze richtlijnen zijn niet bedoeld om definitieve oplossingen te geven voor specifieke afzonderlijke gevallen. Het IIA adviseert om altijd onafhankelijk deskundig advies in te winnen dat rechtstreeks betrekking heeft op een specifieke situatie. Het IIA accepteert geen verantwoordelijkheid wanneer iemand alleen op deze richtlijnen afgaat.

Copyright

Februari 2019