Inleiding

Standaard 2600 – Communicatie van de risicoacceptatie

Wanneer het hoofd van de internal auditfunctie meent dat het management een risiconiveau heeft aanvaard dat ontoelaatbaar zou kunnen zijn voor de organisatie, moet het hoofd van de internal auditfunctie dit met het senior management bespreken. Als het hoofd van de internal auditfunctie vaststelt dat deze kwestie niet is opgelost, moet het hoofd van de internal auditfunctie deze kwestie communiceren aan het bestuur.

**Interpretatie:**

De identificatie van een door het management aanvaard risico kan worden waargenomen op grond van een audit- of een adviesopdracht, het controleren van de voortgang van door het management genomen maatregelen als gevolg van eerdere opdrachten, of anderszins. Het oplossen van het risico valt niet onder de verantwoordelijkheid van het hoofd van de internal auditfunctie.

## Herziene *Standaarden* die per 1 januari 2017 van kracht zijn

Implementatierichtlijn 2600

Om Standaard 2600 succesvol te implementeren, moet het hoofd van de internal auditfunctie zich eerst inzicht verschaffen in de visie en tolerantie van de organisatie ten aanzien van diverse typen organisatierisico's. Organisaties verschillen in de mate van risico en typen risico's die zij aanvaardbaar achten. Zo aanvaarden sommige organisaties in hogere mate financiële risico's, bijvoorbeeld om uit te breiden naar een nieuwe markt in een land met een onstabiele regering, of om te investeren in een opwindend nieuw product dat een relatief kleine kans op succes heeft maar een hoog rendement als het een succes wordt. Andere organisaties mijden dergelijke financiële risico's en situaties. Daarnaast verschillen organisaties in de factoren die zij in aanmerking nemen bij het bepalen van het aanvaardbare risiconiveau, zoals de mogelijke impact en waarschijnlijkheid van de risicogebeurtenis en de tijd die het management nodig heeft om een onaanvaardbaar risico te ondervangen.

Indien de organisatie een formeel beleid voor risicomanagement heeft, dat een proces voor risicoaanvaarding kan omvatten, is het belangrijk dat de CAE en de internal auditfunctie hier kennis van hebben.

Conform Standaard 2500 moet de CAE ook een systeem opzetten en onderhouden om toe te zien op de opvolging van de aan het management geapporteerde bevindingen.

Daarnaast is het nuttig als de CAE weet hoe kwesties met een hoger risico gewoonlijk binnen de organisatie gecommuniceerd worden. Mogelijk wordt in bestaand beleid beschreven welke communicatieaanpak de voorkeur heeft. Het risicomanagementbeleid kan bijvoorbeeld richtsnoeren voor de tijdigheid, de hiërarchie van de rapportage en soortgelijke aspecten bevatten.

Overwegingen bij de implementatie

In het kader van het monitoren van de opvolging van bevindingen en de bijbehorende verbeteracties, kan het gebeuren dat de CAE kwesties met een hoog risico observeert die niet tijdig worden opgelost of die een hoger risico inhouden dan de organisatie normaliter zou aanvaarden en dus onaanvaardbaar zijn voor de organisatie.

Het voortdurende monitoringsproces is niet de enige manier waarop een CAE onaanvaardbare risico's identificeert. Een effectieve CAE zet diverse werkwijzen in om op de hoogte te blijven van organisatierisico's. Zo kan de CAE informatie ontvangen van medewerkers van de internal auditfunctie over belangrijke risico's die zij tijdens hun assurance- of adviesopdrachten hebben geïdentificeerd. Of de organisatie hanteert een proces voor risicobeheer (Enterprise Risk Management (ERM)) om belangrijke risico's te identificeren en monitoren; het kan zijn dat de CAE betrokken is bij dit proces. Daarnaast kan de CAE door het opbouwen en onderhouden van een op samenwerking gebaseerd communicatienetwerk met het management op de hoogte komen van een gebied in de organisatie met een opkomend risico. Ook streven CAE's ernaar om op de hoogte te blijven van sectortrends en veranderingen in wet- en regelgeving om zo mogelijke en opkomende risico's beter te kunnen herkennen.

Ongeacht hoe een onaanvaardbaar risico wordt geïdentificeerd, moet de CAE dit risico aan het senior management communiceren indien de CAE vaststelt dat het risico hoger is dan de organisatie normaliter zou aanvaarden en de CAE meent dat het risico niet tot een aanvaardbaar niveau is beperkt. Voorafgaand aan deze rapportage bespreekt de CAE de kwestie meestal met de leden van het management die verantwoordelijk zijn voor het risicogebied om de zorgen duidelijk te maken, inzicht te krijgen in het standpunt van het management en een proces overeen te komen om het risico te ondervangen. Als hierover echter geen overeenstemming wordt bereikt, moet de CAE de kwestie doorverwijzen naar het senior management. Indien het risico ook na een soortgelijke bespreking met het senior management nog steeds niet is ondervangen, moet de CAE de kwestie rapporteren aan het bestuur. Het is dan aan het bestuur om te besluiten hoe men de kwestie samen met het management aanpakt.

De CAE gebruikt oordeelsvorming om te bepalen hoe en hoe snel dergelijke zaken aan wie moeten worden gecommuniceerd. Hij of zij doet dit op basis van de aard en urgentie van de kwestie, de mogelijke impact ervan en de eventuele bestaande procedures. Als bijvoorbeeld wet- of regeling is overtreden, moet dan het hoofd van de juridische afdeling worden geraadpleegd? En moet het risico worden gecommuniceerd in een besloten vergadering met een bestuurslid of in een functieoverschrijdende vergadering die wordt bijgewoond door vele vaktechnische specialisten?

Standaard 2600 is van toepassing op zeer belangrijke risico's die naar het oordeel van de CAE het door de organisatie getolereerde niveau overstijgen. Hierbij valt te denken aan:

* Risico's die de reputatie van de organisatie kunnen schaden.
* Risico's die mensen persoonlijk kunnen schaden.
* Risico's die kunnen leiden tot aanzienlijke boetes door toezichthouders, boetes, restricties op bedrijfsactiviteiten of andere financiële of contractuele sancties.
* Afwijkingen van materieel belang.
* Fraude of andere strafbare feiten.
* Ernstige belemmeringen voor het realiseren van strategische doelstellingen.

Overwegingen bij het aantonen van de naleving

De naleving kan worden aangetoond door de notulen van vergaderingen waarin een kwestie met een belangrijk risico is besproken met het senior management, het bestuur of een risicocommissie. Indien de CAE het onaanvaardbare risico rapporteert in een gesprek onder twee ogen of in een besloten vergadering, kan een memorandum worden opgesteld om de stappen te documenteren die zijn genomen om het management en bestuur op de hoogte te brengen van het risico. Daarnaast kan de naleving indirect blijken uit bepalingen in het beleidshandboek van de internal auditfunctie die de vereisten op grond van Standaard 2600 en voor het rapportageproces van de organisatie uiteenzetten.

Over het IIA

Het *Institute of Internal Auditors* (IIA) is internationaal de meest vooraanstaande beroepsorganisatie van de internal auditors. Het instituut treedt op als belangenbehartiger, houdt zich bezig met educatie en verstrekt standaarden, richtsnoeren en certificeringen. Het IIA werd opgericht in 1941 en heeft inmiddels meer dan 180.000 leden in ruim 170 landen. Het wereldwijde hoofdkantoor van het IIA staat in de Verenigde Staten in Lake Mary, Florida. Ga voor andere informatie naar www.globaliia.org of www.theiia.org.

Over de Implementatierichtlijnen

De Implementatierichtlijnen maken deel uit van het *International Professional Practices Framework*® (IPPF®) van het IIA en bevatten (niet-verplichte) richtsnoeren voor het beroep van internal auditor. Doel van de Implementatierichtlijnen is ondersteuning te bieden aan internal auditors en internal auditfuncties zodat zij beter in staat zijn om de *International Standards for the Professional Practice of Internal Auditing* (Standaarden) na te leven.

De Implementatierichtlijnen ondersteunen internal auditors bij het toepassen van de Standaarden. De Implementatierichtlijnen beschrijven de aanpak, methodieken en overwegingen die de internal auditfunctie moet hanteren, maar gaan niet in detail in op processen of procedures.

Andere gezaghebbende richtlijnen van het IIA kunt u vinden op onze websites: www.globaliia.org/standards-guidance en www.theiia.org/guidance.

Disclaimer

Dit document is door het IIA gepubliceerd voor informatieve en educatieve doeleinden. Deze Richtlijnen hebben niet tot doel definitieve antwoorden te geven op specifieke individuele vragen en zijn derhalve slechts bedoeld als richtsnoer. Het IIA raadt aan om met betrekking tot een specifieke situatie altijd onafhankelijk deskundig advies ter zake in te winnen. Het IIA accepteert geen verantwoordelijkheid voor de gevolgen indien men uitsluitend afgaat op deze Richtlijnen.

Auteursrecht

Copyright® 2016 *The Institute of Internal Auditors.* Toestemming voor reproductie van deze publicatie kunt u per e-mail aanvragen via guidance@theiia.org.