Standaard 2120 – Risicomanagement

De internal-auditfunctie moet de doeltreffendheid van de risicomanagementprocessen evalueren en bijdragen aan het verbeteren daarvan.

**Interpretatie:**

*Om te kunnen vaststellen of de risicomanagementprocessen doelmatig zijn, moet de internal auditor eerst beoordelen in hoeverre:*

* *de organisatorische doelstellingen de missie van de organisatie ondersteunen en daarop aansluiten;*
* *belangrijke risico's worden vastgesteld en beoordeeld;*
* *passende risicobeheermaatregelen worden geselecteerd waarbij risico's worden afgezet tegen de risicobereidheid van de organisatie;*
* *relevante risico-informatie wordt vastgelegd en tijdig wordt verspreid binnen de organisatie, zodat personeel, management en het bestuur hun verantwoordelijkheden kunnen uitoefenen.*

*De internal-auditfunctie kan gedurende diverse opdrachten informatie verzamelen ter onderbouwing van deze evaluatie. Wanneer de resultaten van deze opdrachten in hun onderlinge samenhang worden beschouwd, bieden ze inzicht in de risicomanagementprocessen van de organisatie en de doelmatigheid daarvan.*

*Risicomanagementprocessen worden bewaakt door doorlopende managementactiviteiten, afzonderlijke evaluaties of een combinatie daarvan.*

**2120.A1** – De internal-auditfunctie moet potentiële risico’s aangaande de governance, de operationele activiteiten en de informatiesystemen van de organisatie evalueren op het gebied van:

Implementatierichtlijn 2120

Inleiding

* verwezenlijking van de strategische doelstellingen van organisatie;
* betrouwbaarheid en integriteit van de financiële en operationele informatie;
* doelmatigheid en efficiëntie van de bedrijfsactiviteiten en -programma's;
* bescherming van de activa;
* naleving van wet- en regelgeving, beleidsmaatregelen, procedures en contracten.

**2120.A2** – De internal-auditfunctie moet de kans op het bestaan van fraude en hoe de organisatie frauderisico’s beheert, evalueren.

**2120.C1** – Tijdens adviesopdrachten moeten de internal auditors zich toeleggen op risico’s die binnen de doelstellingen van de opdracht vallen en aandacht hebben voor eventuele andere belangrijke risico's.

**2120.C2** – Internal auditors moeten kennis op het gebied van risico's die zij hebben opgedaan uit adviesopdrachten, verwerken in hun evaluatie van de risicomanagementprocessen van de organisatie.

**2120.C3** – Wanneer interne auditors het management ondersteunen bij het vaststellen en verbeteren van de risicomanagementprocessen, moeten zij zich onthouden van elke managementverantwoordelijkheid voor het daadwerkelijke beheer van risico’s.

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

Om aan deze standaard te voldoen, beginnen het hoofd van de internal auditfunctie (CAE) en internal auditors met het verkrijgen van een duidelijk inzicht in de risicobereidheid, evenals de zakelijke missies en doelstellingen van de organisatie. Het is ook belangrijk om een ​​volledig inzicht te krijgen in de bedrijfsstrategieën van de organisatie en de door het management geïdentificeerde risico's.

Risico's kunnen financieel, operationeel, juridisch of strategisch van aard zijn of betrekking hebben op regelgeving. De definitie van risicomanagement in de woordenlijst van de *Internationale Standaarden voor de Beroepsuitoefening van internal auditing* moet in overweging worden genomen, samen met raamwerken en modellen voor risicomanagement die wereldwijd worden gepubliceerd. Daarnaast kan Implementatierichtlijn 2100 – Aard van het werk, nuttig zijn om de basis te verkrijgen die nodig is om Standaard 2120 te implementeren.

Aangezien deze standaard de internal auditfunctie de taak geeft de effectiviteit van risicomanagementprocessen te beoordelen zullen internal auditors doorgaans inzicht zien te krijgen in de bestaande risicomanagementomgeving van de organisatie en de corrigerende maatregelen ter voorkoming van eerdere risico's. Het is belangrijk om te weten hoe de organisatie risico's identificeert en beoordeelt en hoe zij toezicht houdt op risico's voordat de internal auditors Standaard 2120 gaan implementeren.

In haar risicobeoordeling dient de internal auditfunctie de omvang, complexiteit, levenscyclus, volwassenheid, stakeholderstructuur en juridische en competitieve omgeving van de organisatie in overweging te nemen. Recente veranderingen in de omgeving van de organisatie (bv. nieuwe regelgeving, nieuw managementpersoneel, nieuwe organisatiestructuur, nieuwe processen en nieuwe producten) kunnen nieuwe risico's hebben geïntroduceerd. De CAE kan ook de volwassenheid van de risicomanagementpraktijken van de organisatie beoordelen en bepalen in hoeverre de internal auditfunctie zich zal baseren op de risicobeoordeling van het management.

Ten slotte zou de internal auditfunctie een vast proces moeten hebben voor de planning, auditing en rapportering van kwesties met betrekking tot risicomanagement. Internal auditors zullen het risicomanagement ook beoordelen tijdens assurance- en adviesbeoordelingen met betrekking tot een specifiek gebied of proces.

Overwegingen bij de implementatie

Door de implementatie van Standaard 2120 zal de CAE en de gehele internal auditfunctie uiteindelijk blijk geven van hun inzicht in de risicomanagementprocessen van de organisatie en naar mogelijkheden voor verbetering zoeken. De CAE neemt door middel van gesprekken met senior management en het bestuur de risicobereidheid, risicotolerantie en risicocultuur van de organisatie in overweging. De internal auditfunctie dient het management te waarschuwen voor nieuwe risico's en risico's die niet adequaat worden beperkt en dient aanbevelingen en actieplannen voor een adequate risicoreactie te bieden (bv. accepteren, nastreven, overdragen, beperken of vermijden). Daarnaast dient de internal auditfunctie voldoende informatie te verkrijgen om de effectiviteit van de risicomanagementprocessen van de organisatie te evalueren.

Door het strategisch plan, het bedrijfsplan en het beleid van de organisatie te evalueren en met het bestuur en het senior management te spreken, kan de CAE inzicht krijgen zodat hij/zij kan beoordelen of de strategische doelstellingen de missie, visie en risicobereidheid van de organisatie ondersteunen en daarmee in overeenstemming zijn. Interviews met mid-level management kunnen extra inzicht bieden in de overeenstemming van de missie, de doelstellingen en de risicobereidheid van de organisatie op het niveau van de business unit.

Internal auditors zouden grondig moeten onderzoeken hoe de organisatie risico's identificeert en aanpakt en hoe zij vaststelt welke risico's aanvaardbaar zijn. De internal auditfunctie zal doorgaans de verantwoordelijkheden en risico-gerelateerde processen van het bestuur en de belangrijkste risicomanagementrollen beoordelen. Om dit te bereiken kunnen internal auditors recentelijk voltooide risicobeoordelingen en bijbehorende rapporten bekijken, die zijn uitgegeven door senior management, externe auditors, regelgevers en andere bronnen.

Daarnaast voert de internal auditfunctie doorgaans haar eigen risicobeoordelingen uit. Gesprekken met het management en het bestuur en evaluatie van het beleid van de organisatie en notulen van vergaderingen zullen over het algemeen de risicobereidheid van de organisatie laten zien, waardoor de CAE en de internal auditfunctie hun aanbevolen risicoreacties op elkaar kunnen afstemmen. De internal auditfunctie kan overwegen om gebruik te maken van een vast raamwerk voor risicomanagement of beheersing (bv., De raamwerken van The Committee of Sponsoring Organizations van de Treadway Commission of ISO 31000) om te helpen bij het identificeren van risico's. Om op de hoogte te blijven van potentiële blootstellingen aan risico's en kansen kan de internal auditfunctie ook onderzoek doen naar nieuwe ontwikkelingen en trends die verband houden met de bedrijfstak van de organisatie, evenals processen die kunnen worden gebruikt om dergelijke risico's en kansen te monitoren, beoordelen en erop te reageren.

Door deze stappen te nemen, kunnen internal auditors zelfstandig gap-analyses uitvoeren om te bepalen of belangrijke risico's adequaat worden geïdentificeerd en beoordeeld en de internal auditfunctie zal in de gelegenheid worden gesteld om het risicobeoordelingsproces van het management te evalueren. Bij de beoordeling van het risicomanagementproces is het belangrijk dat internal auditors de risico's en de gekozen corresponderende reacties identificeren en bespreken. Het management kan er bijvoorbeeld voor kiezen om risico te accepteren en de CAE dient te bepalen of het besluit juist is, in overeenstemming met de risicobereidheid of risicomanagementstrategie van de organisatie. Indien de CAE concludeert dat het management een risiconiveau heeft aanvaard dat ontoelaatbaar zou kunnen zijn voor de organisatie, moet de CAE de zaak nader bespreken met het senior management en zal de CAE de kwestie eventueel moeten communiceren aan het bestuur in overeenstemming met Standaard 2600 – Communicatie van de risicoacceptatie. In gevallen waarin het management ervoor kiest om een ​​risicobeperkende strategie te volgen in reactie op geïdentificeerde risico's, kan de internal auditfunctie de toereikendheid en tijdigheid van genomen herstelmaatregelen evalueren, indien nodig. Dit kan worden bereikt door de ontwerpen voor beheersing te beoordelen en de beheersingsmaatregelen en de bewakingsprocedures te toetsen.

Om te beoordelen of relevante risico-informatie is vastgelegd en tijdig wordt gecommuniceerd in de hele organisatie, kunnen internal auditors het personeel op verschillende niveaus interviewen en vaststellen of de doelstellingen, de belangrijke risico's en de risicobereidheid van de organisatie voldoende duidelijk zijn gemaakt en worden begrepen in de hele organisatie. De internal auditfunctie beoordeelt doorgaans ook de toereikendheid en tijdigheid van de rapportage van de resultaten van het risicomanagement door het management. De internal auditfunctie kan notulen van het bestuur inzien om te bepalen of de belangrijkste risico's tijdig aan het bestuur zijn meegedeeld en of het bestuur optreedt om ervoor te zorgen dat het management adequaat reageert.

Ten slotte moet de internal auditfunctie de nodige maatregelen treffen om ervoor te zorgen dat zij haar eigen risico's, zoals auditfouten, valse assurance en reputatierisico's, beheerst. Ook alle corrigerende maatregelen dienen te worden gecontroleerd.

Overwegingen bij het aantonen van de naleving

Documenten die naleving van Standaard 2120 kunnen aantonen zijn onder andere het internal auditcharter, dat de rollen en verantwoordelijkheden van de internal auditfunctie met betrekking tot risicomanagement documenteert, en het internal auditplan. Daarnaast kan naleving worden aangetoond door notulen van vergaderingen waarin de elementen van de standaard — zoals de aanbevelingen voor risicobeheersing van de internal auditfunctie — zijn besproken door de CAE, het bestuur en het senior management of vergaderingen van de internal auditfunctie met relevante commissies, task forces en de belangrijkste leden van het senior management.

Risicobeoordelingen uitgevoerd door de internal auditfunctie en actieplannen voor het aanpakken van risico's laten over het algemeen respectievelijk de beoordeling en de verbetering van risicomanagementprocessen zien.

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.