IPPF

International Professional Practices Framework

Aanvullende richtlijnen

Praktijkgids

FINANCIËLE DIENSTVERLENING

Auditing Modelrisicomanagement

Instituut van Internal Auditors Nederland

Auditing Modelrisicomanagement

Colofon

Titel

Auditing Modelrisicomanagement

Instituut van
Internal Auditors
Nederland

Inhoudsopgave

Over het IPPF

Het International Professional Practices Framework® (IPPF®) is het conceptuele kader waarin de gezaghebbende richtlijnen die door het IIA worden uitgevaardigd zijn opgenomen. Het IIA is een betrouwbaar, wereldwijd orgaan dat richtlijnen vaststelt en internal auditprofessionals wereldwijd gezaghebbende richtlijnen biedt die in het IPPF zijn opgenomen in de vorm van verplichte richtlijnen en aanbevolen richtlijnen.

Verplichte richtlijnen worden ontwikkeld op basis van een vast due-diligenceproces, dat een periode omvat waarin input kan worden gegeven door belanghebbenden. De verplichte elementen van het IPPF zijn:

- Kernbeginselen van de beroepsuitoefening van internal auditing
- Definitie van internal auditing
- Gedragscode
- *Internationale normen voor de professionele praktijk van internal auditing*.

Over aanvullende richtlijnen

Aanvullende richtlijnen maken deel uit van het IPPF en bieden aanvullende aanbevolen (niet-verplichte) richtlijnen voor het uitvoeren van de internal auditfunctie. De aanvullende richtlijnen ondersteunen de *Standaarden* en zijn daarnaast bedoeld om actuele onderwerpen, evenals sectorspecifieke kwesties, in groter procedureel detail te behandelen dan de *Standaarden* of Implementatierichtlijnen. Aanvullende richtlijnen worden door middel van formele beoordelings- en goedkeuringsprocessen onderschreven door het IIA.

Praktijkgidsen

Praktijkgidsen zijn aanvullende richtlijnen die gedetailleerde stapsgewijze benaderingen bieden, met processen, procedures, tools en programma's, evenals voorbeelden van te leveren prestaties.

Praktijkgidsen zijn bedoeld om internal auditors te ondersteunen. Praktijkgidsen zijn ook beschikbaar ter ondersteuning van:

- Financiële dienstverlening.
- Publieke sector.
- Informatie Technologie (GTAG®).

Ga naar www.globaliia.org/standards-guidance voor een overzicht van gezaghebbende richtlijnen die worden aangeboden door het IIA.

Samenvatting

Banken[1] en andere grote financiële dienstverleners zijn in hoge mate afhankelijk van wiskundige modellen om zakelijke beslissingen te nemen en aan wettelijke vereisten te voldoen. Modellen zijn inherent risicovol omdat ze statistische, economische, financiële of wiskundige theorieën toepassen die vereisen dat er gebruik wordt gemaakt van aannames op basis van gezond verstand teneinde schattingen van reële financiële gebeurtenissen op te leveren. Dit proces kan leiden tot onnauwkeurige of onjuiste resultaten. Bovendien kunnen gedurende de gehele levenscyclus van het **model** fouten worden geïntroduceerd, variërend van fouten in de invoergegevens tot onjuiste berekeningen en onjuiste toepassing van het model en de resultaten ervan.

De toenemende afhankelijkheid van organisaties van kwantitatieve analysemodellen heeft geleid tot meer aandacht in de regelgeving voor effectief **modelrisicomanagement** (MRM). Naarmate het reglementaire toezicht rond modelrisicobeheersing toeneemt, speelt de internal auditfunctie een sleutelrol bij de beoordeling van het MRM-raamwerk van een organisatie.

Deze richtlijn geeft een overzicht van de verantwoordelijkheden van de internal auditfunctie met betrekking tot MRM en beschrijft de methoden en processen die internal auditors kunnen gebruiken om het ontwerp, de implementatie en de werking van het MRM-raamwerk van hun organisatie te beoordelen.[2]

1 Voor de toepassing van deze Praktijkgids verwijst de term "bank" naar banken, bankholdings of andere vennootschappen die door toezichthouders van banken worden beschouwd als de moederonderneming van een bankgroep onder de nationale wetgeving, zoals door de nationale toezichthouder van de entiteit passend worden geacht. De term "organisaties" wordt in de gids gebruikt om te verwijzen naar banken en andere grote organisaties op het gebied van financiële dienstverlening, zoals verzekeringsmaatschappijen.

2 Deze Praktijkgids is een vertaling. Hierdoor wordt met name verwezen naar Amerikaanse (toezichthoudende) instanties. Vanzelfsprekend dient in de Nederlandse situatie te worden aangesloten bij relevante artikelen uit de *Capital Requirements Regulation (CRR)*, de Wet op het financieel toezicht (*Wft*) en Besluit prudentiële regels Wft, technical standards en guidance van de EBA (EBA/RTS/2016/07, EBA RTS/2016/03 en EBA/GL/2017/16) en relevante artikelen van de ECB, zoals in de ECB Guide to internal models en de TRIM Guidance (Targeted Review of Internal Models), voor financiële instellingen die onder ECB toezicht staan. [Toevoeging: IIA Nederland]

Inleiding

Modelrisicomanagement (MRM) is opgenomen in de regelgeving op het gebied van financiële dienstverlening die door toezichthouders over de hele wereld is uitgevaardigd. Verbeterde regels voor kapitaal, liquiditeit en hefboomwerking zijn bedoeld om de negatieve effecten te verzachten die onvoldoende gekapitaliseerde organisaties kunnen hebben op de economie. Als reactie hierop hebben organisaties in de sector financiële dienstverlening hun activiteiten aangepast en blijven zij hun activiteiten aanpassen om aan deze voorschriften te voldoen.

NB: Vetgedrukte termen worden gedefinieerd in de woordenlijst in bijlage B. Deze richtlijnen bevatten een reeks technische termen die in de sector financiële dienstverlening gangbaar zijn. Als een definitie niet in de woordenlijst voorkomt, raadpleeg dan de referenties en aanvullende literatuur in bijlage F.

Omdat modeloutput bepaalde beslissingen van het senior management beïnvloedt en soms zelfs bepaalt, kunnen modelfouten een organisatie aan een aanzienlijk risico blootstellen. Bovendien worden modellen steeds belangrijker, complexer en gevarieerder. Als gevolg hiervan zijn organisaties voor het voorkomen, opsporen en corrigeren van modelfouten afhankelijk van interne controlesystemen. De internal auditfunctie (IAF) speelt een sleutelrol in het verzekeren van het senior management en de raad van bestuur dat het interne controlesysteem binnen het MRM kader op optimale niveaus werkt in het hele proces van risicomodellering en dat de resultaten overal in de organisatie juist worden geïnterpreteerd.

Betekenis voor het bedrijf: belangrijkste risico's

Modelrisico wordt gedefinieerd als "de mogelijkheid van nadelige gevolgen van beslissingen op basis van onjuiste of verkeerd gebruikte modelresultaten of rapporten".[3] Modelrisico doet zich voor om twee belangrijke redenen: (1) fundamentele fouten in de data, de rationale, de hypothese en de methodologieën van het model kunnen leiden tot onnauwkeurige resultaten wanneer deze worden afgezet tegen het doel van het ontwerp en het beoogde zakelijke gebruik, en/of (2) het model of de resultaten ervan kunnen niet correct of onjuist worden gebruikt. Verder verwijst **geaggregeerd modelrisico** naar onderling verbonden risico's tussen modellen die worden veroorzaakt door gedeelde inputs en/of aannames of doordat de output van het ene model input van een ander model is.[4]

De rol van de internal auditfunctie in Modelrisicomanagement

Om de naleving van de voorschriften door een organisatie te beoordelen, moeten internal auditors een goed inzicht hebben in de wetgeving die relevant is voor de organisatie en de rechtsgebieden waarin de organisatie actief is. Internal auditors zijn ook verantwoordelijk om de modelmethodologieën van de organisatie goed genoeg te begrijpen om het modelontwerp en de werking ervan te kunnen beoordelen.

De rol van de internal audit in het MRM-proces bestaat erin de doeltreffendheid van het MRM-raamwerk te beoordelen, met inbegrip van de governance, het beleid, de procedures en de activiteiten die worden uitgevoerd om het risico van modelfouten aan te pakken. Internal auditors zijn ook verantwoordelijk voor het verkrijgen van inzicht in de wijze waarop de modeloutput wordt gebruikt en of die geschikt is voor het vermelde doel van het model. Daarnaast moeten internal auditors inzicht geven in de opzet en effectieve werking van MRM-activiteiten om het management, de raad van bestuur en andere belangrijke belanghebbenden te helpen bij het uitvoeren van hun taken en om te bevestigen dat de organisatie zich houdt aan de richtlijnen van de toezichthouders.

Internal auditors zijn niet verantwoordelijk voor het uitvoeren of herhalen van modelrisico-activiteiten. Om hun verantwoordelijkheden te vervullen dienen internal auditors onafhankelijk te zijn, over relevante vaardigheden te beschikken, hun bevindingen rechtstreeks aan de raad van bestuur te rapporteren en MRM op gepaste wijze in overweging te nemen bij het ontwikkelen en uitvoeren van het auditplan.

3 Board of Governors of the Federal Reserve System (FRS), *Supervisory Guidance on Model Risk Management*. SR 11-7, (Washington, D.C.: FRS, 2011), 4, https://www.federalreserve.gov/supervisionreg/srletters/sr1107.htm.

4 Ibid.

Het proces van Modelrisicomanagement

Het MRM-proces kan worden onderverdeeld in drie activiteitengebieden:

- Bestuur, beleid en beheersingsmaatregelen.
- Ontwikkeling, implementatie en gebruik.
- Initiële en voortdurende validatie[5]

De activiteitengebieden zijn veranderlijk en moeten niet worden beschouwd als gebieden die vaste begin- en eindpunten hebben. Figuur 1 geeft de relatie van elk gebied weer.

Figuur 1: Proces van Modelrisicomanagement

Model Governance, Beleid, en Beheersingsmaatregelen

Effectief governance, beleid en effectieve procedures en beheersingsmaatregelen zijn essentiële onderdelen van een succesvol MRM-raamwerk. Zonder goed toezicht en goede richtlijnen is het moeilijk om ervoor te zorgen dat de processen voor de ontwikkeling, implementatie, validatie en het gebruik van modellen naar behoren functioneren. Uiteindelijk is de raad van bestuur verantwoordelijk voor het toezicht op het MRM-raamwerk. De ontwikkeling en gedetailleerde uitvoering is echter gedelegeerd aan senior management.

Organisaties dienen hun beleid en procedures met betrekking tot het MRM-proces formeel te documenteren. Dit beleid en deze procedures worden gewoonlijk opgesteld door het senior management en goedgekeurd door de raad van bestuur en moeten aan de volgende criteria voldoen:

- Ze dienen het gehele MRM-proces te dekken.
- Ze dienen gedetailleerd beschreven te zijn om de behoefte aan interpretatie te verminderen en een uniforme uitvoering overal in de organisatie te bevorderen.
- Ze dienen documentatiestandaarden voor alle hoofdactiviteiten op de drie activiteiten-gebieden van modelrisicomanagement te geven.
- Ze definiëren MRM-rollen en verantwoordelijkheden binnen de organisatie te definiëren.
- Ze definiëren het modelrisicobeoordelingskader en -proces.
- Vaststellen van beheersingsstandaarden voor modellen.
- Ze dienen de creatie en het onderhoud van een organisatiebrede modelinventarisatie af te dwingen.

5 Board of Governors of the Federal Reserve System, *Supervisory Guidance on Model Risk Management*, 3-9.

Bij bepaalde modellen kan een organisatie ervoor kiezen om deze activiteiten uit te besteden; bijvoorbeeld wanneer de interne middelen die nodig zijn voor de ondersteuning van de ontwikkeling en/of validatie niet beschikbaar zijn. In deze gevallen dient het management richtlijnen op te stellen voor de integratie van externe middelen en aangekochte producten (bijv. modellen, data, parameters, waarden) in het algemene MRM-raamwerk.

Het management dient de rollen en verantwoordelijkheden vast te leggen van elke partij die betrokken is bij het MRM-proces. Het management kan deze rollen en verantwoordelijkheden documenteren door een schema op te stellen voor opname in het MRM-beleids- en proceduredocument. Het moet ten minste alle niveaus van werknemers omvatten die betrokken zijn bij het proces, de aan hen toegewezen te leveren prestaties en alle vereiste beoordelingen of goedkeuringen. Organisaties kunnen als best practice gebruik maken van het "Three Lines of Defense"[6] model om de rollen en verantwoordelijkheden uit te bouwen. Internal auditors kunnen het management hierbij bijstaan door de gerelateerde gebieden die in hun portefeuille zijn gedocumenteerd, indien aanwezig, te delen.

Voor meer informatie over het ontwikkelen van een assurance map, zie de IIA Practice Guide "Coordination and Reliance: Developing an Assurance Map".

Het "Three Lines of Defense" model is een best-practice-kader dat organisaties kunnen gebruiken om bedrijfsprocessen te structureren. Het model helpt het management om duidelijke rollen en verantwoordelijkheden vast te stellen en internal auditors kunnen het model gebruiken om hiaten of doublures in de risicodekking op te sporen, om informatiebronnen te identificeren die nodig zijn om opdrachten te plannen en het bestaande MRM-raamwerk van een organisatie te helpen ontwikkelen of verbeteren.

De eerste verdedigingslinie is het operationele management. In de context van MRM omvat dit hoofden van afdelingen of functionele gebieden en gebruikers, eigenaars, en ontwikkelaars van modellen. Deze functies hebben in de eerste plaats de verantwoordelijkheid om ervoor te zorgen dat organisaties risico's in modellen identificeren, beoordelen en beperken. Daarnaast is de eerste lijn verantwoordelijk voor de basis van het MRM-proces; de ontwikkeling van modellen; de implementatie en uitvoering van en het toezicht op modelbeheersingsmaatregelen; en onderhoud van modeldocumentatie.

De tweede verdedigingslinie omvat andere taken op het gebied van bedrijfstoezicht, zoals risicobeheersing en compliance. Grote organisaties hebben binnen hun risicobeheersing- of compliance-afdelingen doorgaans modelrisico-units aangewezen. Deze verdedigingslinie kan ook verschillende risicocommissies van de raad van bestuur en het management omvatten. De tweede verdedigingslinie is verantwoordelijk voor:

- Toezicht houden op en adviseren en assisteren van de eerste verdedigingslinie.
- Ondersteuning van beperking van het totale modelrisico door aggregatie en analyse van modelinformatie van verschillende bedrijfsafdelingen.

6 The Institute of Internal Auditors. IIA Position Paper*: The Three Lines of Defense in Effective Risk Management and Control* (Altamonte Springs: The Institute of Internal Auditors, 2013).

- Het uitvoeren van de initiële validatie en van de lopende monitoring en validatie, en ervoor zorgen dat alle vastgestelde problemen worden aangepakt.
- Rapporteren van modelrisico-informatie aan het senior management, de raad van bestuur en de juiste toezichtgroepen.

De internal auditfunctie is de derde verdedigingslinie, die de raad van bestuur en het senior management veelomvattende zekerheid biedt op basis van het hoogste niveau van onafhankelijkheid en objectiviteit binnen de organisatie. In de context van MRM beoordelen internal auditors de toereikendheid van het MRM-raamwerk (governance, beleid, procedures en beheersingsmaatregelen) en geven een oordeel over het totale proces. De internal auditfunctie is onafhankelijk van de andere verdedigingslinies en rapporteert haar resultaten rechtstreeks aan de raad van bestuur of haar gedelegeerden.

Model Ontwikkeling, Implementatie, en Gebruik

Wanneer een hiaat of tekortkoming in de modelportfolio van een organisatie wordt vastgesteld, moet het management beslissen om een nieuw model te bouwen of te kopen. Het management moet formeel documenteren wat het beoogde doel is van het nieuwe model en zijn beslissing om een nieuw model te bouwen of te kopen. Als het management besluit om het model te bouwen, moet het goed geïnformeerde en ervaren ontwikkelaars toewijzen aan het project. Naast het bouwen van het model, moeten ontwikkelaars de juiste data-invoer selecteren om ervoor te zorgen dat de kwaliteit van de resulterende data hoog is.[7]

Ontwikkelaars kunnen veel verschillende soorten data gebruiken:

- De meest fundamentele soort zijn de ruwe data die rechtstreeks van de bron worden afgeleid en op geen enkele manier worden gemanipuleerd.
- Als er hiaten zijn in de ruwe data, kunnen ontwikkelaars deze vullen met kunstmatige datasets die expansiedata worden genoemd. Deze data worden gecreëerd door eenvoudige regels te dupliceren of toe te passen op bestaande datasets in een poging om de ontbrekende data te benaderen.
- Als er geen data beschikbaar zijn, moet de ontwikkelaar gebruik maken van proxy-data, een sterk gecorreleerde dataset die wordt gebruikt om niet-waarneembare of onmeetbare data te benaderen. Zo dient het bruto nationaal product doorgaans als proxy data voor de economische situatie van een land.
- Ten slotte kunnen ontwikkelaars data van andere modellen verkrijgen. Deze worden sub-model data genoemd en hebben betrekking op de output van een model dat gebruikt wordt als input voor een ander model.

Zodra de ontwikkelaars het model hebben gebouwd en de datasets hebben bepaald, moeten ze de functionaliteit van het model testen om er zeker van te zijn dat het naar verwachting presteert. Grondig testen brengt een verscheidenheid van scenario's met zich mee, met inbegrip van extreme situaties, hetgeen ook wel stress

Voor meer informatie over stress testing in organisaties, zie de IIA Practice Guide "Auditing Capital Adequacy and Stress Testing for Banks".

7 Board of Governors of the FRS, *Supervisory Guidance on Model Risk Management*, 5-6.

testing wordt genoemd. Als het model in deze extreme situaties niet naar behoren functioneert, kan het nodig zijn om beperkingen aan het model te stellen en het gebruik ervan te beperken. Organisaties dienen alle beperkingen formeel te documenteren. Nadat het model is getest door ontwikkelaars, moeten zakelijke gebruikers de mogelijkheid hebben om het model te beproeven of te testen en feedback te geven.

Zodra de ontwikkelaars en de zakelijke gebruikers tevreden zijn over de functionaliteit van het model, kan het naar de eerste validatiefase gaan, waarin het model wordt getest door onafhankelijke partijen van binnen of buiten de organisatie. Als het model niet slaagt voor een eerste validatietest, moet het opnieuw door het ontwikkelingsproces. Als het model validatie doorstaat, moet het de implementatiefase ingaan voor productie volgens de IT richtlijnen van de organisatie. Zodra dit is voltooid, is het model beschikbaar voor gebruik door de organisatie.

De lijnorganisatie is gedurende de gehele levensduur van het model verantwoordelijk voor het in stand houden van geschikte processen en beheersingsmaatregelen om modelrisico's te beperken en nauwkeurige resultaten te ondersteunen, afgestemd op het beoogde gebruik van het model. Deze omvatten bijvoorbeeld het toereikend documenteren van het doel, de methodologie, de aannames en de beperkingen van het model. Afhankelijk van de aard van het bedrijf en de **materialiteit** van het model voor de bedrijfsvoering, kan het ook nuttig zijn om afwijkingen van industriestandaarden en de reden voor de verschillen te documenteren.

De lijnorganisatie is ook verantwoordelijk voor het onmiddellijk rapporteren van problemen met modelprestaties aan het juiste managementniveau. Gezien het belang van de outputs van de modellen die het management zal gebruiken in zijn besluitvormingsprocessen en bij het uitvoeren van zijn andere verantwoordelijkheden, moeten modellen met materiële betekenis bovendien voortdurend worden gevalideerd.

Validatie

Validatie is het proces om te controleren of een model functioneert zoals bedoeld. Validatie wordt doorgaans uitgevoerd door een onafhankelijke partij en staat los van de tests die worden uitgevoerd door de ontwikkelaars en zakelijke gebruikers. Er kunnen zich echter gevallen voordoen waarin het onpraktisch is om een derde in te schakelen om te valideren (d.w.z, gezien de omvang en/of aard van het bedrijf) en de ontwikkelaars of zakelijke gebruikers de validatietest moeten uitvoeren[8]. In deze situatie moet een onafhankelijke partij, zoals de internal auditfunctie, de testresultaten beoordelen om de nauwkeurigheid van de validatie te ondersteunen.

De bij het validatieproces betrokken partijen moeten in staat zijn het model effectief te testen. De exacte definitie van effectief testen kan variëren afhankelijk van de verwachtingen van toezichthouders en andere belanghebbenden van een organisatie. De Federal Reserve Board (FRB) en het Office of the Comptroller of the Currency (OCC) geven een algemene definitie van een effectieve test als "kritische analyse door objectieve, geïnformeerde partijen

8 In de Nederlandse wetgeving voor financiële instellingen is opgenomen dat altijd iemand anders dan de ontwikkelaar moet valideren [Toevoeging: IIA Nederland]

die modelbeperkingen en -aannames kunnen identificeren en passende wijzigingen kunnen aanbrengen".[9] Om een model effectief te kunnen testen moet iemand competent en invloedrijk zijn en niet worden beïnvloed door beloningen. Een validator moet met name aan de volgende kwalificaties voldoen:

- Niet betrokken zijn bij het ontwikkelingsproces en er zijn geen financiële vergoedingen verbonden aan het model (bijv. loonsverhogingen, bonussen, promoties, prestatiebeoordelingen).
- Beschikken over diepgaande kennis van het model zelf en de bedrijfstak(ken) waarin het wordt gebruikt.
- Beschikken over een passend bevoegdheidsniveau dat waarborgt dat corrigerende maatregelen worden genomen om eventuele tijdens het validatieproces vastgestelde modelfouten aan te pakken.

De International Association of Insurance Supervisors schrijft in Standaard nr. 2.2.7 voor dat voordat modellen die bedoeld zijn voor het toetsingsvermogen in gebruik worden genomen, dienen drie tests te worden uitgevoerd. Deze drie tests zijn een goed startpunt voor elk modelvalidatieprogramma:

1. Met behulp van een statistische kwaliteitstoets wordt de kwantitatieve basismethodologie van het interne model beoordeeld. Als onderdeel van dit testproces moet de gebruiker van het model de geschiktheid van de methodologie kunnen aantonen, met inbegrip van de keuze van de input en parameters van het model, en moet hij of zij de aannames die aan het model ten grondslag liggen kunnen rechtvaardigen.
2. Een kalibratietest toont aan dat het voorgeschreven toetsingsvermogen zoals bepaald door het interne model voldoet aan de modelleercriteria die door de toezichthouder zijn gespecificeerd.
3. Een gebruikstest bevestigt dat het interne model en zijn methodologieën en resultaten volledig zijn ingebed in de risicostrategie en operationele processen van de gebruiker van het model. De standaard stelt ook dat de raad van bestuur en het senior management de algehele verantwoordelijkheid moeten hebben om ervoor te zorgen dat er adequate governance en beheersingsmaatregelen zijn met betrekking tot de constructie en het gebruik van interne modellen.[10]

Monitoring en hervalidatie

Initiële modelvalidatie vindt normaliter plaats voordat een model voor gebruik beschikbaar wordt gesteld, en permanente monitoring en validatie worden voortgezet gedurende de gehele levensduur van het model. Wanneer een organisatie vertrouwt op talrijke modellen, kan het management gebruik maken van een modelrisicobeoordeling om de frequentie te bepalen waarmee monitoring en hervalidatie moeten worden uitgevoerd.

9 Board of Governors of the Federal Reserve System, *Supervisory Guidance on Model Risk Management*, 4.

10 Solvency and Actuarial Issues Subcommittee, "Standard nr. 2.2.7: IAIS Standard on the Use of Internal Models for Regulatory Purposes," (Basel: International Association of Insurance Supervisors, 2008), 5, https://www.iaisweb.org/file/34143/16-standard-no-227-on-the-use-of-internal-models-for-regulatory-capital-purposes.

Een modelrisicobeoordeling houdt het volgende in:

- Vaststelling van de belangrijkste risicofactoren die aan elk model verbonden zijn. Risicofactoren omvatten de complexiteit van het model, de materialiteit van de output van het model, het soort modelberekeningen (handmatig versus geautomatiseerd), etc.
- Beoordeling van het **inherente risico** van elk model op basis van de geïdentificeerde factoren.
- Vaststellen of de activiteiten op het gebied van monitoring en voortdurende validatie van het model wat frequentie (schema) en aard betreft in overeenstemming zijn met het inherente risico van elk model.
- Beoordelen of de frequentie wat betreft monitoring en voortdurende validatie van het model in overeenstemming zijn met de totale **risicobereidheid** van de organisatie.

Personen die modellen valideren dienen modellen die van materieel belang zijn regelmatig te controleren om de functionaliteit op hoog niveau te beoordelen en vast te stellen of de historische validatieactiviteiten nog steeds voldoende zijn. Als het model niet goed werkt, moet het worden aangepast en opnieuw worden gevalideerd. Indien het model naar behoren functioneert, maar de historische validatieactiviteiten door regelgevers of een andere relevante partij ontoereikend worden geacht, dienen validators een volledige of gedeeltelijke hervalidatie uit te voeren.

Organisaties dienen te voorkomen dat modellen van materiële betekenis gedurende langere perioden niet worden gehervalideerd. Sommige toezichthoudende instanties[11] en andere belangrijke belanghebbenden kunnen verwachten dat de validatie met bepaalde tussenpozen plaatsvindt. De FRB en de OCC bevelen bijvoorbeeld aan om modellen met een materiële significantie routinematig volledig te hervalideren, ongeacht de resultaten van regelmatige monitoringactiviteiten.[12]

11 Voor de Nederlandse situatie zijn dit ECB en/of DNB [Toevoeging: IIA Nederland]

12 Solvency and Actuarial Issues Subcommittee, "Standard nr. 2.2.7: IAIS Standard on the Use of Internal Models for Regulatory Purposes," (Basel: International Association of Insurance Supervisors, 2008), 5, https://www.iaisweb.org/file/34143/16-standard-no-227-on-the-use-of-internal-models-for-regulatory-capital-purposes

Auditing Modelrisicomanagement

De opdracht plannen

IIA Standaard 2200 – Planning van de opdracht
IIA Standaard 2201 – Overwegingen bij de planning

Voor meer informatie verwijzen we u naar de IIA Practice Guide "Engagement Planning: Establishing Objectives and Scope".

Bij het plannen van een beoordeling van het MRM-raamwerk van een organisatie, moeten internal auditors het beleid, de processen en de tools identificeren die worden gebruikt om de risico's te beheersen en de omgeving met betrekking tot modellen te beheren. Vervolgens moeten internal auditors bepalen of het MRM-raamwerk is opgenomen als onderdeel van de uniforme en samenhangende, organisatiebrede governancestructuur.

Planning van de opdracht omvat over het algemeen de volgende stappen:

- De context en het doel van de opdracht begrijpen.
- Informatie verzamelen om het gebied of proces dat beoordeeld wordt te begrijpen.
- Een voorlopige risicobeoordeling uitvoeren.
- Opdrachtdoelstellingen formuleren.
- Reikwijdte van de opdracht vaststellen.
- Middelen toewijzen.
- Het plan documenteren.

De volgende secties van deze gids helpen de internal auditor bij het plannen en uitvoeren van een beoordeling van het MRM-raamwerk van de organisatie.

De context en het doel van de opdracht begrijpen
IIA Standaard 2201 – Overwegingen bij de planning

Bij de planning van de auditopdracht moeten de internal auditors rekening houden met de volgende elementen:

- Modellen gebruikt door de organisatie.
- Grootte en verfijning van de organisatie en haar MRM-raamwerk.
- De eisen/verwachtingen op het gebied van MRM-regelgeving die relevant zijn voor de organisatie en de rechtsgebieden waarin zij opereert.
- Robuustheid van MRM-rollen, -verantwoordelijkheden en -activiteiten in de hele organisatie.
- Resultaten van modelbewakings-en-validatieactiviteiten en andere modeltoezichtactiviteiten die in de hele organisatie zijn uitgevoerd.

Bij het ontwikkelen van het individuele auditplan verzamelen internal auditors informatie met behulp van procedures zoals het bestuderen van eerdere beoordelingen (bijv., risicobeoordelingen, verslagen van leveranciers van assurance- en adviesdiensten), het begrijpen en in kaart brengen van processtromen en -controles, en het interviewen van relevante belanghebbenden. Omdat MRM een organisatiebrede activiteit is, kan nieuw verkregen

informatie van invloed zijn op de doelstellingen, de reikwijdte, het werkprogramma en de analysemethoden van de opdracht. De informatie die tijdens de planning wordt verzameld, moet derhalve goed worden gedocumenteerd, onmiddellijk worden bijgewerkt en tijdens de hele duur van de audit in aanmerking worden genomen. De informatie kan ook nuttig zijn bij de langetermijnplanning van de CAE voor toekomstige opdrachten.

Informatie verzamelen om het te beoordelen gebied of proces te begrijpen
IIA Standaard 2201 – Overwegingen bij de planning

Zodra internal auditors de afdelingen, functies en rollen in de organisatie hebben geïdentificeerd die relevant zijn voor MRM, dienen zij relevante documentatie te verzamelen ter ondersteuning van de voorlopige risicobeoordeling. De volgende elementen kunnen helpen bij het identificeren van de risico's waarmee de organisatie wordt geconfronteerd en de strategieën die worden gebruikt om deze risico's te beheersen in termen van het MRM-raamwerk:

- Charters, beleidsregels en andere informatie over het mandaat voor de bestuursentiteiten die verantwoordelijk zijn voor het vaststellen van het MRM-raamwerk.
- MRM-beleidsregels, -richtlijnen en -standaarden.
- Beoordeling van modelrisico en -beheersingsmaatregelen door het management.
- Het modelinventarisatie- en risicobeoordelingsproces en de resultaten van de organisatie.
- Alle documenten en alle medewerkers die kunnen helpen inzicht te krijgen in de gebruikte modellen.
- Documentatie van alle fasen van de modelontwikkelings- en validatieprocessen.
- Modelvalidatierapporten.
- Resultaten van modellering voor krediet-, markt-, liquiditeits-, kapitaal-, financiële rapportage- en operationele doeleinden.
- Documentatie van het proces voor het ontwerpen en uitvoeren van normale en stress-scenario's.
- Verslagen met de resultaten van stresstests.
- Resultaten van eerdere onderzoeken van het MRM kader en de individuele modellen die in de organisatie worden gebruikt door regelgevende instanties

Voorlopige risicobeoordeling uitvoeren
IIA Standaard 2210.A1 – Internal auditors moeten een voorlopige evaluatie maken van de risico's die van belang zijn voor de te onderzoeken activiteit.

Omdat één enkele interne auditopdracht niet alle risico's kan dekken, beoordelen internal auditors het belang van de risico's die zijn geïdentificeerd door het management, de validators, de toezichthouders en het belang van de risico's die tijdens eerdere interne auditopdrachten zijn geïdentificeerd. Drie primaire bronnen dragen bij aan het modelrisico:

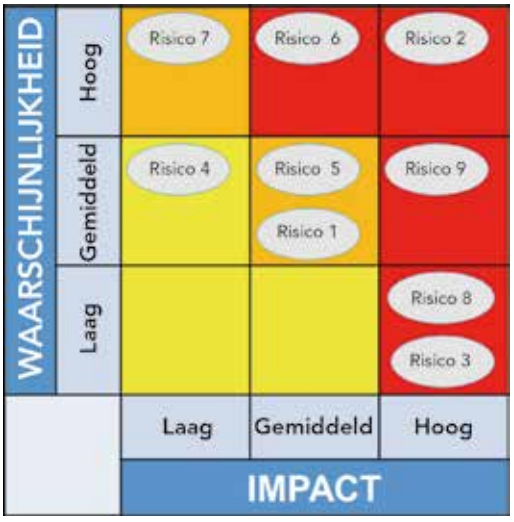
1. Fundamentele fouten kunnen onnauwkeurige output opleveren ten opzichte van het doel van het ontwerp en het beoogde zakelijke gebruik.
2. Onjuist of oneigenlijk gebruik.
3. Onnauwkeurige of beschadigde data voor de input.

Internal auditors dienen alle significante modellen van de organisatie voor deze risicobronnen te onderzoeken en te bepalen welke specifieke risico's relevant zijn voor de modellen die in de audit zijn inbegrepen. Internal auditors willen wellicht modelontwikkelaars, validators, risicomanagers en ander relevant personeel interviewen die wellicht over technische kennis beschikken die kan helpen bij het identificeren van risico's die zijn toegesneden op een specifiek model of een specifieke groep modellen. Zoals eerder vermeld, kunnen internal auditors de beoordelingen van het management van de inherente risico's van de modellen verkrijgen en deze informatie ook opnemen in hun risicobeoordeling op het niveau van hun opdrachten.

Een effectieve manier om een risicobeoordeling op opdrachtniveau uit te voeren en te documenteren is het opstellen van een risicomatrix met een overzicht van de relevante risico's en de matrix vervolgens uit te breiden met maatregelen die van belang zijn. Met behulp van een spreadsheet of een vergelijkbaar document kan, met of zonder een auditsoftwareprogramma, een MRM-risicomatrix worden gecreëerd. De indeling van de matrix kan variëren, maar omvat gewoonlijk een rij voor elk risico en een kolom voor elke risicomaatstaf, zoals impact en waarschijnlijkheid.

Het beoordelen van de waarschijnlijkheid is relatief eenvoudig; de factoren waarmee rekening moet worden gehouden zijn onder meer eerdere risico-incidenten, data over risico-incidenten uit proxy-bronnen, de complexiteit van het model en het aantal mensen dat bij het proces betrokken is. Het beoordelen van de impact is vaak gecompliceerder omdat zowel kwantitatieve als kwalitatieve factoren een rol spelen. Internal auditors dienen niet alleen rekening te houden met de financiële en operationele impact van de MRM-risico's en de impact van de regelgeving met betrekking daartoe, maar ook de niet-financiële impact, zoals schade aan de reputatie van de organisatie of relaties met klanten of leveranciers. Zo kan een fout in een datastream voor een upstream-model materiële gevolgen hebben voor downstream-modellen, afhankelijk van de manier waarop de outputs van het upstream-model worden gebruikt. Sommige risico's kunnen op zichzelf onbeduidend lijken, maar moeten worden gezien in de context van het MRM-programma van de organisatie.

De risicoscores uit de MRM-risicomatrix kunnen dan worden weergegeven in een basisgrafiek, zoals een heatmap. Door de impact van elk risico op de ene as en de waarschijnlijkheid ervan op de andere as in kaart te brengen, geven de internal auditors een duidelijk beeld van het algemene belang van het risico of de prioriteit. De gecombineerde betekenis van effect en waarschijnlijkheid wordt doorgaans aangegeven met behulp van een kleurensysteem: rood geeft de hoogste prioriteit aan, oranje geeft risico's aan die belangrijk genoeg zijn om in overweging te worden genomen, en geel geeft risico's aan die niet significant zijn, zoals aangegeven in Figuur 2. De heatmap moet worden opgenomen in de workpapers van de opdracht, omdat deze de beslissingen van internal auditors over de significantie van risico's ondersteunt.



Figuur 2: Heatmap

Een beperking van heatmaps is dat impact en waarschijnlijkheid even belangrijk lijken te zijn. Hoewel impact en waarschijnlijkheid in sommige gevallen even belangrijk kunnen zijn, heeft impact gewoonlijk een hoger prioriteit dan waarschijnlijkheid. Zo moet in de meeste gevallen aan een risico met een hoge impact en een lage waarschijnlijkheid (H, L) een hogere prioriteit worden gegeven dan aan een risico met een lage impact, ook al is de waarschijnlijkheid dat het risico zich voordoet groot (L, H).

Een bijkomende beperking van heatmaps is dat slechts twee maatstaven tegelijk kunnen worden bekeken (in dit geval de impact en de waarschijnlijkheid). Het kan wenselijk of noodzakelijk zijn om bij het bepalen van de significantie van het risico ook rekening te houden met maatstaven als snelheid, kwetsbaarheid, volatiliteit, onderlinge afhankelijkheid en/of correlatie.

Internal auditors kunnen op basis van de ingevulde heatmap eenvoudig de risico's visualiseren die significant zijn wanneer er geen beheersingsmaatregelen zijn. Nadat de internal auditors de significante inherente risico's hebben geïdentificeerd, moeten zij bepalen welke controles er eventueel zijn om deze risico's te beperken. Dit stelt internal auditors in staat om de restrisiconiveaus te beoordelen en de risico's te kiezen die in de opdracht worden meegenomen voor verdere toetsing.

De risico- en controlematrix dienen net als de heatmap te worden opgenomen in de workpapers van de opdracht. De informatie uit de matrix wordt vervolgens verwerkt in de voorlopige risicobeoordeling die wordt gebruikt om de doelstellingen en reikwijdte van de opdracht vast te stellen. De IIA Practice Guide "Engagement Planning: Establishing Objectives and Scope" biedt gedetailleerde informatie over het voortbouwen op de risicobeoordeling om de doelstellingen en reikwijdte van de opdracht te ontwikkelen. Daarnaast ondersteunen de heatmap en de risico- en controlematrix de resultaten en conclusies van de opdracht, in overeenstemming met Standaard 2330 - Documenteren van de informatie.

Doelstellingen van de opdracht formuleren

IIA Standaard 2210 – Doelstellingen van de opdracht

Het doel van een MRM-assuranceopdracht is doorgaans om onafhankelijke zekerheid te verschaffen over de governance, de beleidsmaatregelen, de processen en de belangrijkste beheersingsmaatregelen die de implementatie, de uitvoering en het toezicht op het MRM-raamwerk van een organisatie ondersteunen.

Doelstellingen van assurance-opdrachten

- Behandel risico's voor de bedrijfsdoelstellingen van het gebied of proces die als significant zijn beoordeeld tijdens de voorlopige risicobeoordeling (Standaard 2210. A1).
- Houd rekening met de kans op significante fouten, fraude, niet-naleving en andere risico's (Standaard 2210.A2).
- Stel geschikte beoordelingscriteria vast (Standaard 2210. A3).

Bij het formuleren van de doelstellingen van de opdracht moeten de internal auditors de criteria identificeren die zullen worden gebruikt om te beoordelen of de doelstellingen met betrekking tot MRM zijn behaald. Volgens Standaard 2210.A3 mogen internal auditors gebruik maken van de volgende bronnen van criteria:

- Intern (bijv. de beleidsmaatregelen en procedures van de organisatie);
- Extern (bijv. wet- en regelgeving die wordt opgelegd door wettelijke instanties);
- Toonaangevende praktijken (bijv. industriële en professionele richtlijnen).

Uiteindelijk dient de beoordeling te bepalen of het MRM-raamwerk functioneert in overeenstemming met de verwachtingen van toezichthouders en de raad van bestuur en zoals beschreven in goedgekeurde beleidsmaatregelen en procedures.

Vaststellen van de reikwijdte van de opdracht
IIA Standaard 2220 – Reikwijdte van de opdracht

Internal auditors dienen te overwegen de volgende elementen op te nemen bij de vaststelling van de reikwijdte van een opdracht ter beoordeling van modelrisicomanagement:

1. Toereikendheid van de beleidsmaatregelen, procedures en activiteiten ter ondersteuning van de modellen en het MRM-raamwerk, inclusief afstemming op de risicobereidheid van de organisatie, de verwachtingen van belanghebbenden en de standaarden in de bedrijfstak.
2. Governance uitgevoerd met betrekking tot de beleidsmaatregelen, procedures en activiteiten die de modellen en het MRM-raamwerk ondersteunen.
3. Opname van het volgende in het MRM-raamwerk:
    - Gedefinieerde rollen en verantwoordelijkheden voor elk van de drie verdedigingslinies en bestuurslichamen.
    - Definities van een model, model risicobereidheid en materialiteit.
    - Een inventarisatie van de modellen, criteria voor de risicoclassificatie en risicobeoordelingsproces.
    - Verwachtingen met betrekking tot modelbeheersingsmaatregelen, met inbegrip van input- en resultaatcontroles, nauwkeurigheid van de data en beheersingsmaatregelen voor het afsluiten, beveiliging en doorvoeren van wijzigingen.
    - Rapportagevereisten voor de aanwezigheid van modelrisico's.
    - Een risicogebaseerd modelbeoordelingsplan waarin onafhankelijke beoordelingen en tests zijn opgenomen, met inbegrip van standaarden voor de definitie en goedkeuring van het plan.
    - Modelvalidatiestandaarden met inbegrip van de dekking van: conceptuele soliditeit, data, IT-infrastructuur, documentatie, processen en beheersingsmaatregelen, en modelbeperkingen.
    - Processen voor het classificeren, escaleren en volgen van bevindingen die voortvloeien uit modelvalidatieactiviteiten.
4. Effectieve werking van model-risicobeheersingsactiviteiten.

Internal auditors dienen deze elementen aan te passen aan hun unieke organisatie; al deze zaken dienen echter in enige vorm aanwezig zijn.

Toekenning van middelen
IIA Standaard 2230 – Toekenning van middelen aan de opdracht

In IIA Standaard 2230 – Toekenning van middelen aan de opdracht staat: "Internal auditors moeten bepalen wat passende en voldoende middelen zijn om de doelstellingen van de

opdracht te bereiken, gebaseerd op een evaluatie van de aard en de complexiteit van elke opdracht, de gestelde tijdslimieten en de beschikbare middelen." Bovendien moeten internal auditors volgens IIA-standaard 1100 – Onafhankelijkheid en objectiviteit objectief zijn bij het uitvoeren van hun werkzaamheden en dient de internal auditfunctie onafhankelijk te zijn, d.w.z. "vrij zijn van omstandigheden die een bedreiging vormen voor het vermogen van de internal auditfunctie om haar verantwoordelijkheden op het gebied van internal audit uit te voeren". Standaard 1130.A1 vereist dat internal auditors "afzien van het beoordelen van specifieke operationele activiteiten waarvoor zij in het verleden verantwoordelijk waren." Om onafhankelijk te zijn, mogen internal auditors niet betrokken zijn bij de ontwikkeling, implementatie of het gebruik van de modellen (of het MRM-raamwerk) die worden beoordeeld. Internal auditors kunnen echter wel bij het validatieproces worden betrokken. Indien deze situatie zich voordoet, dienen de internal auditors die de validatiewerkzaamheden hebben uitgevoerd geen deel uit te maken van het MRM-auditteam.

Internal auditors die leiding geven aan een beoordeling van een MRM-raamwerk moeten niet alleen beschikken over een duidelijk inzicht in de wettelijke vereisten waaraan de organisatie is onderworpen, maar ook over vaardigheden en gespecialiseerde kennis. Dit zou zowel modelleerconcepten moeten omvatten als het gebruik ervan in de relevante bedrijfstakken. Alle internal auditors in het modelrisicoteam moeten algemene vaardigheden bezitten voor het beoordelen van modelrisico's, maar hoeven geen modelrisicodeskundigen te zijn.

De toezichthouder van de opdracht dient ervoor te zorgen dat op elk gebied van de opdracht het juiste personeel wordt ingezet. In IIA Standaard 1210 – Vakbekwaamheid staat: "Internal auditors moeten beschikken over kennis, vaardigheden en andere bekwaamheden, die benodigd zijn voor de uitvoering van hun individuele verantwoordelijkheid. De internal auditfunctie als geheel moet kennis, vaardigheden en overige competenties, die benodigd zijn om haar verantwoordelijkheden uit te voeren, bezitten of verkrijgen." Om deze standaarden te handhaven, moeten meer ervaren internal auditors met diepgaande kennis van business en modellering aan het validatiegebied worden toegewezen. Daarnaast moeten internal auditors die vaardigheden in de business, modellering en informatietechnologie hebben de ontwikkeling, uitvoering en het gebruiksgebied testen. De overige gebieden van het auditplan kunnen worden getoetst door minder ervaren medewerkers met een grondige kennis van basisauditconcepten en een goede praktijkkennis van de business.

Het **hoofd van de internal auditfunctie** (Chief Audit Executive, CAE) kan op regelmatige basis een verschillenanalyse uitvoeren om de kwalificaties en competenties van internal auditors onder het personeel te beoordelen en om te bepalen of de internal auditfunctie als geheel over de juiste kwalificaties en competenties beschikt. Indien de internal auditfunctie niet over voldoende en passende vaardigheden beschikt, vereist standaard 1210.A1 dat de CAE deskundig advies en bijstand inhuurt om de gehele auditopdracht of een gedeelte ervan uit te voeren. Opties zijn toezicht, opleiding en uitbesteding.

Indien de CAE lacunes constateert in de kennis van MRM bij de internal auditfunctie, kan het zinvol zijn om modelrisicotraining te bieden. Dit kan worden bereikt door trainingen te laten ontwikkelen door interne experts of door externe trainers in te huren. Als er te grote kennislacunes zijn, er te weinig tijd is om training te geven of training te duur is, dan moet de auditopdracht worden uitbesteed. Implementatiegids 2230 – Toekenning van middelen aan de opdracht biedt aanvullende richtlijnen voor het gebruik van derden.

Bij het kiezen van een externe partner met wie wordt samengewerkt aan modelrisico-audits, moet de CAE ervoor zorgen dat een gekwalificeerde, competente, bekwame en objectieve auditdeskundige wordt ingehuurd. Na selectie moeten alle overeengekomen diensten formeel worden gedocumenteerd. In Standaard 2050 – Coördinatie en afhankelijkheid wordt opgemerkt: "Ook ingeval op het werk van externe partijen wordt vertrouwd, blijft het hoofd van de internal auditfunctie te allen tijde verantwoordelijk. Het hoofd van de internal auditfunctie moet zorgen voor adequate ondersteuning voor de conclusies en adviezen die worden geformuleerd door de internal auditfunctie." Zelfs als het testen samen met een ingehuurde derde wordt gedaan, dient het werkproduct van de deskundige derhalve te worden beoordeeld met behulp van confirmerende procedures na voltooiing van de opdracht. De CAE en de internal auditors die het werk van de deskundige zouden kunnen beoordelen, moeten dus inzicht hebben in de MRM-concepten en de verantwoordelijkheden van de auditor. Bij het inhuren van een deskundige kan de CAE of de gedelegeerde toezichthouder bij de opdracht gebruik maken van het diagram "Beoordelen van een deskundige" in Bijlage C.

Het plan documenteren
IIA Standaard 2240 – Werkprogramma van de opdracht

Tijdens de planning documenteren internal auditors informatie in het dossier van de audit. Deze informatie wordt onderdeel van het werkprogramma van de audit, dat moet worden opgesteld om de opdrachtdoelstellingen te bereiken, zoals vereist door Standaard 2240 - Werkprogramma van de opdracht.

Het proces van het vaststellen van de doelstellingen en de reikwijdte van de opdracht kan leiden tot de productie van de volgende werkdocumenten of een deel ervan:

- Proceskaarten.
- Inventarisatie van de modellen.
- Samenvatting van interviews.
- Voorlopige risicobeoordeling (bijv., risico- en controlematrix en heatmap).
- Redenen voor beslissingen over welke risico's in de opdracht moeten worden opgenomen.
- Criteria die zullen worden gebruikt voor de evaluatie van het gebied of het proces dat beoordeeld wordt.

Zie de IIA Practice Guide "Engagement Planning: Establishing Objectives and Scope" voor meer informatie over het plannen en het vaststellen van de reikwijdte van een opdracht.

Modelrisicomanagement testen en evalueren

IIA Standaard 2300 – Uitvoering van de opdracht
IIA Standaard 2320 - Analyse en evaluatie

Testen van governance en toezicht
Internal auditors moeten tests ontwerpen om te bevestigen dat het senior management en de raad van bestuur primair verantwoordelijk zijn voor de vaststelling en handhaving van het MRM-raamwerk. De notulen van de raad van bestuur moeten worden bestudeerd om te bevestigen dat de raad van bestuur actief betrokken is bij het MRM-proces. Daarnaast dienen internal

auditors bewijs te verzamelen dat alle aspecten van het MRM-proces aan de juiste partijen zijn toegewezen en naar behoren worden uitgevoerd. Bij het beoordelen van de geschiktheid van toegewezen verantwoordelijkheden kunnen internal auditors verwijzen naar het "Three Lines of Defense" model van het IIA.[13] Bijlage D geeft meer informatie.

Evalueren van gedocumenteerde MRM-procedures

Internal auditors dienen te bevestigen dat de MRM-procedures van de organisatie een goede bedrijfsvoering bevorderen en in overeenstemming zijn met de wettelijke vereisten. Internal auditors zouden bijvoorbeeld bewijs moeten verzamelen dat de raad van bestuur of haar gedelegeerden jaarlijks de procedures controleert en goedkeurt. Daarnaast moeten internal auditors bewijzen verzamelen dat er protocollen van kracht zijn om tijdige procedurele updates in gang te zetten met betrekking tot wijzigingen in producten, regelgeving, organisatiestructuur (acquisities) en soortgelijke gebeurtenissen. Ten slotte dienen internal auditors na te gaan of de procedures het gehele MRM-proces in detail bestrijken en de rollen en verantwoordelijkheden van alle betrokken partijen omvatten.

Een inventarisatie van modellen bijhouden

Het management is verantwoordelijk voor het samenstellen van een volledige en nauwkeurige inventarisatie van modellen, waarin alle modellen zijn opgenomen die in ontwikkeling zijn, in gebruik zijn of recent zijn ingetrokken. Internal auditors dienen het bestaan van de inventarisatie te bevestigen en te valideren dat er adequate controlemechanismen zijn voor het bevestigen van de volledigheid en nauwkeurigheid ervan. Daarnaast dienen internal auditors te beoordelen of het niveau van gedetailleerdheid van de inventarisatie redelijk is, gezien de complexiteit van de modellen van de organisatie en de mate waarin er gebruik van wordt gemaakt. Tot slot kunnen internal auditors informatie uit de inventarisatie van modellen gebruiken om vast te stellen in hoeverre medewerkers zich houden aan het MRM-beleid en de MRM-procedures van de organisatie. Bijlage D geeft meer informatie.

Het validatieproces testen

Om zich een mening te vormen over het validatieproces, dienen internal auditors de geschiktheid en volledigheid van de door validators gebruikte risicobeoordelingsmethode te evalueren. Met betrekking tot de risicobeoordelingsmethode dienen de volgende vragen te worden gesteld:

- Is de methode duidelijk gedefinieerd?
- Is de methode gedocumenteerd?
- Wordt de methode gebruikt?
- Wordt in de methode rekening gehouden met alle relevante kenmerken die van invloed zijn op het niveau van het risico?
- Hoe vaak wordt de risicobeoordeling uitgevoerd?
- Welke trigger-events zouden leiden tot een verandering in het risiconiveau van een model?

Zodra de methode is beoordeeld, moeten internal auditors de geschiktheid van de individuele modelrisicoclassificaties die uit de risicobeoordeling naar voren komen, evalueren. Bij grote

13 The Institute of Internal Auditors. De IIA Position Paper*: The Three Lines of Defense in Effective Risk Management and Control*, 2-6.

inventarissen van modellen kan een steekproef worden gebruikt. Internal auditors moeten bepalen of de controleactiviteiten voor elk risiconiveau (validatiefrequentie, etc.) geschikt zijn en zouden ervoor moeten zorgen dat de modellen niet opzettelijk "te laag geclassificeerd" worden om aan aanvullend onderzoek te ontsnappen.

Internal auditors moeten tests op hoog niveau uitvoeren om te bevestigen dat het validatieproces alomvattend is en dat de validators alle belangrijke risicogebieden beoordelen. Validatieprogramma's waarbij een steekproef van modellen wordt gebruikt, dienen diepgaand te worden getest. Dergelijke tests moeten bevestigen dat de validators de conceptuele deugdelijkheid van de modellen, met inbegrip van hun inputs, verwerking en rapportagecomponenten, hebben beoordeeld. Internal auditors moeten ook bevestigen dat de validators voldoen aan de criteria voor een effectieve test, hetgeen kan worden gedefinieerd als een "kritische analyse door objectieve, geïnformeerde partijen die modelbeperkingen en -aannames kunnen identificeren en passende wijzigingen kunnen aanbrengen".[14]

Internal auditors moeten nagaan of het niveau van de verrichte validatieactiviteiten in verhouding stond tot het risico van het model. De validator had bijvoorbeeld de lopende monitoringactiviteiten van het model moeten beoordelen en de resultaten moeten analyseren om te garanderen dat de output van het model representatief is voor de werkelijke resultaten. Internal auditors moeten bevestigen dat alle tekortkomingen of beperkingen die tijdens het validatieproces zijn vastgesteld, zijn geregistreerd, gecontroleerd en aangepakt. Als laatste stap dienen de internal auditors na te gaan of de kwaliteit van de data van het model is gevalideerd. Dit ondersteunt de conformiteit van de internal auditfunctie met de IIA Standaard 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:... betrouwbaarheid en integriteit van de financiële en de operationele informatie." Bijlage D biedt aanvullende informatie.

Testen van ontwikkeling, implementatie en gebruik van toetsingsmodellen

Internal auditors moeten analytische procedures toepassen op een steekproef van modellen om de ontwikkeling, implementatie en het gebruik van modellen grondig te testen. In de publicatie AS 2305 van de Public Company Accounting Oversight Board uit 2002 staat het volgende: *Essentiële analytische procedures*, "Analytische procedures vormen een belangrijk onderdeel van het auditproces en bestaan uit evaluaties van financiële informatie op basis van een onderzoek naar plausibele relaties tussen zowel financiële als niet-financiële data. Analytische procedures variëren van eenvoudige vergelijkingen tot het gebruik van complexe modellen die vele relaties en data-elementen omvatten. De IIA Implementatiegids 2320 – Analyse en evaluatie geeft meer informatie over de analysemethoden van de internal audit.

Internal auditors moeten bevestiging krijgen dat de ontwikkelaars die de modellen hebben gemaakt en de tests hebben uitgevoerd, over voldoende, relevante vaardigheden beschikten en dat alle uiteindelijke modelleringsbeslissingen naar behoren werden onderbouwd. Gedetailleerde documentatie van het gehele proces moet voorhanden zijn voor de beoordeling door de internal audit. Internal auditors moeten bewijzen verzamelen om te bevestigen dat ontwikkelaars de vereiste goedkeuringen hebben verkregen voorafgaand aan de implementatie. Bijlage D geeft meer informatie.

14 Board of Governors of the Federal Reserve System, *Supervisory Guidance on Model Risk Management*, 4.

Modeldata

Het MRM-raamwerk van een organisatie dient controlestandaarden voor modellen vast te stellen, met inbegrip van controles van data-invoer. Internal auditors moeten testen uitvoeren om te bevestigen dat controles van de input van data worden beoordeeld tijdens modelvalidatie en kunnen ook de kwaliteit van de ingevoerde data controleren. Er moeten beheersmaatregelen bestaan om ervoor te zorgen dat de data volledig, juist, tijdig en correct geïnterpreteerd zijn. Wanneer gebruik wordt gemaakt van proxy-data, dienen internal auditors de geschiktheid te beoordelen van de methode die is gebruikt om de data te ontwikkelen. Als het model data van een ander model gebruikt, moeten internal auditors de bestaande controles beoordelen om de nauwkeurigheid van de berekeningen en output van het submodel te waarborgen.

Gebruik van derden bij ontwikkeling en/of validatie

Om het effectieve voortdurende gebruik en de levensvatbaarheid van tools van derden te ondersteunen, dient de organisatie resultaten te verkrijgen van de voortdurende monitoring van elke leverancier en details van alle wijzigingen aan modellen, en dient zij haar eigen voortdurende monitoring uit te voeren met behulp van inputs van de organisatie. Bovendien moet de organisatie beschikken over een noodplan om onderbreking van haar activiteiten te voorkomen indien de leverancier niet in staat is het model te ondersteunen, voortdurende monitoring uit te oefenen of wijzigingen aan te brengen.

Internal auditors moeten bevestigen dat de leverancier de geldende overeenkomsten inzake dienstverleningsniveau nakomt. Indien een leverancier niet meer in staat is zijn verplichtingen na te komen, dienen internal auditors na te gaan of het management het noodplan tijdig en volledig volgens de gedocumenteerde procedures heeft uitgevoerd. Indien een externe partij wordt ingehuurd om een validatie uit te voeren, dienen internal auditors te bevestigen dat de partij voldoet aan de effectieve toetsingscriteria. Bijlage D geeft meer informatie.

De resultaten van de opdracht rapporteren

IIA Standaard 2330 – Documenteren van de informatie
IIA Standaard 2410 – Kenmerken van de communicatie
IIA Standaard 2440 – Distributie van de resultaten

Na voltooiing van grondige testen, analyses en evaluaties, zullen de internal auditors "voldoende, betrouwbare, relevante en nuttige informatie ter ondersteuning van de conclusies en resultaten van de opdracht" hebben gedocumenteerd, in overeenstemming met Standaard 2330 – Documenteren van de informatie. Internal auditors dienen voor alle MRM-opdrachten hun standaardprocedures voor rapportage te volgen. Bij de verspreiding van de resultaten moet echter een schriftelijk rapport worden opgesteld en moet de raad van bestuur een afschrift ontvangen. Indien er tijdens een opdracht geen materiële zwaktes werden vastgesteld en de beoordeling bevredigend was, is het doorgaans aanvaardbaar om een samenvattend verslag voor te leggen aan de raad van bestuur of haar gedelegeerden. Internal auditors dienen er echter nota van te nemen dat, om te voldoen aan IIA Standaard 2410 – Kenmerken van de communicatie en Standaard 2410.A1, de uiteindelijke communicatie van de resultaten van de opdracht de doelstellingen, reikwijdte, resultaten, toepasselijke conclusies, aanbevelingen en/of actieplannen van de opdracht moet omvatten. Meer informatie kan worden gevonden in de IIA Practice Guide "Audit Reports: Communicating Assurance Engagement Results".

Bijlage A.
Gerelateerde standaarden en richtlijnen van IIA

Zie de *Standaarden* voor de volledige verklaring. Om u te helpen bij de implementatie van de *Standaarden*, beveelt het IIA aan dat internal auditors de respectieve Implementatiegids van elke standaard raadplegen.

Gerelateerde standaarden van IIA
Standaard 1100 - Onafhankelijkheid en objectiviteit
Standaard 1210 - Vakbekwaamheid
Standaard 2060 –Rapportering aan het senior management en de raad van bestuur
Standaard 2200 – Planning van de opdracht
Standaard 2201 – Overwegingen bij de planning
Standaard 2210 – Doelstellingen van de opdracht
Standaard 2220 – Reikwijdte van de opdracht
Standaard 2230 – Toekenning van middelen aan de opdracht
Standaard 2240 – Werkprogramma van de opdracht
Standaard 2300 – Uitvoering van de opdracht
Standaard 2320 – Analyse en evaluatie
Standaard 2330 – Documenteren van de informatie
Standaard 2410 – Kenmerken van de communicatie
Standaard 2440 – Distributie van de resultaten
Gerelateerde richtlijnen van IIA
Practice Guide "Audit Reports: Communicating Assurance Engagement Results", 2016 Guide: Audit Reports: Communicating Assurance Engagement Results
Practice Guide "Auditing Capital Adequacy and Stress Testing for Banks", 2018.
Practice Guide "Auditing Liquidity Risk: An Overview", 2018.
Practice Guide "Engagement Planning: Establishing Objectives and Scope", 2017.
Practice Guide "Internal Audit and the Second Line of Defense", 2016.
IIA Position Paper: *The Three Lines of Defense in Effective Risk Management and Control, 2013.*

Bijlage B. Woordenlijst

De met een sterretje (*) aangeduide termen zijn ontleend aan de "Woordenlijst" van The IIA's *International Professional Practices Framework®* (*IPPF®*), uitgave 2017. Tenzij anders vermeld, zijn de overige definities overgenomen uit de Federal Reserve, SR 11-7: Guidance on Model Risk Management, 2011.

Geaggregeerd modelrisico – Onderling verbonden modelrisico veroorzaakt door gedeelde inputs en aannames of omdat de output van het ene model de input van een ander model vormt.

Hoofd van de internal auditfunctie (Chief Audit Executive) * – Beschrijft de rol van een persoon in een senior functie binnen de organisatie, met verantwoordelijkheid voor het effectieve beheer van de internal auditfunctie overeenkomstig het internal auditcharter en de verplichte aspecten van het internationale raamwerk voor de beroepsuitoefening. Het hoofd van de internal auditfunctie of de overige medewerkers die rapporteren aan het hoofd van de internal auditfunctie, beschikken over passende professionele certificaten en kwalificaties. De specifieke functienaam en/of de verantwoordelijkheden van het hoofd van de internal auditfunctie kunnen per organisatie verschillen.

Inherent risico – Het risico voordat de kwaliteit van de interne beheersingsmaatregelen wordt bekeken.[15]

Materialiteit – Wat zou van materieel belang zijn voor de redelijke belegger bij het nemen van een beslissing over belegging in de effecten van het bedrijf. Gewoonlijk is dit 5 procent van het nettoresultaat voor belastingen van de onderneming, maar dit kan anders zijn wanneer de onderneming verlies lijdt of een laag winstniveau heeft; zowel kwantitatieve als kwalitatieve aspecten moeten in aanmerking worden genomen[16].

Model – Kwantitatieve methode, systeem of benadering waarbij statistische, economische, financiële of wiskundige theorieën, technieken en aannames worden toegepast om input-data te verwerken tot kwantitatieve schattingen. Een model bestaat uit drie componenten: een informatie-inputcomponent, die veronderstellingen en data aan het model levert; een verwerkingscomponent, die inputs in ramingen omzet; en een rapportagecomponent, die de ramingen vertaalt naar nuttige bedrijfsinformatie.

15 Norman Marks, *Sarbanes-Oxley Section 404: A Guide for Management by Internal Controls Practitioners*, (Altamonte Springs: The Institute of Internal Auditors, 2008), https://na.theiia.org/standards-guidance/Public%20Documents/Sarbanes-Oxley_Section_404_--_A_Guide_for_Management_2nd_edition_1_08.pdf

16 Ibid.

Modelcriteria – Verzameling definities die wordt gebruikt om het management te helpen bepalen welke instrumenten of processen als modellen worden beschouwd.

Modelrisico – De mogelijkheid van nadelige gevolgen van beslissingen op basis van onjuiste of verkeerd gebruikte modeloutputs of rapporten. Modelrisico treedt voornamelijk op om drie redenen:

1. Fundamentele fouten kunnen onnauwkeurige output opleveren ten opzichte van het doel van het ontwerp en het beoogde zakelijke gebruik.
2. Onjuist of oneigenlijk gebruik.
3. Onnauwkeurige of beschadigde data voor de input.

Modelrisicomanagement (MRM) – Het proces van het bouwen van modellen, het classificeren van hun risico's en het beheren van deze risico's.

Risicobereidheid* – Het risiconiveau dat een organisatie bereid is te accepteren.

Bijlage C.
Diagram: Een deskundige beoordelen

Bijlage D. Modelrisicomanagement testen en evalueren

Gezien de rol van de internal auditfunctie bij het verschaffen van onafhankelijke assurance dat de organisatie risico's beheerst op een manier die in overeenstemming is met de wettelijke vereisten en het bereiken van hun doelstellingen, vormen de onderstaande tabellen een kader voor het uitvoeren van een beoordeling van het MRM-raamwerk. De internal auditor moet mogelijk controles op maat maken of creëren voor unieke gebieden van het specifieke kader, beleid en procedures van een organisatie. Het kan ook nodig zijn dat de internal auditor verwijst naar werkprogramma's voor verwante gebieden (d.w.z, stresstests, liquiditeitsrisicobeheersing, krediet-/markt-/operationele risicobeheersing) om een volledig ontwikkelde MRM-opdracht te ontwikkelen, met name indien de opdracht wordt opgesplitst in segmenten zoals vermeld in deze gids.

Governance en Toezicht	Parafen/ Datum	WP Ref
Mededelingen		
• Rollen en verantwoordelijkheden van MRM zijn gecommuniceerd. • De organisatorische mededelingen met betrekking tot MRM zijn juist.		
Training		
• Medewerkers zijn getraind in het MRM-proces. • De trainingsdocumenten zijn nauwkeurig. • Alle medewerkers voor wie dit vereist is hebben de training afgerond.		
Rollen en verantwoordelijkheden		
• De rollen en verantwoordelijkheden voor compliance zijn in overeenstemming met het Three Lines of Defense model. • De rollen en verantwoordelijkheden omvatten een gedetailleerde beschrijving van wie elk proces uitvoert, de verwachte resultaten en de timing van de vereiste goedkeuringen.		
Raad van Bestuur en Senior Management		
• Uit de bestudering van de notulen van de raad van bestuur blijkt de actieve betrokkenheid van de raad van bestuur bij het MRM-proces, waarbij ook de risicotolerantie van de organisatie in aanmerking wordt genomen. • De raad van bestuur beoordeelt het modelrisico voor de organisatie afzonderlijk en in totaal. • In de loop van het jaar heeft de raad van bestuur alle vereiste MRM-rapporteringen ontvangen. • De raad van bestuur dient jaarlijks het beleid en de procedures te beoordelen en goed te keuren. Een kopie van de meest recente goedkeuring is verkregen.		

Beleid en procedures	Parafen/ Datum	WP Ref
Volledigheid en nauwkeurigheid		
• Het beleid en de procedures zijn actueel en procedurele wijzigingen worden er tijdig in verwerkt. De door de raad van bestuur tijdens het laatste onderzoek gevraagde updates zijn op de juiste wijze doorgevoerd. • Het beleid en de procedures bestrijken het gehele MRM-proces tot in detail. Er zijn specifieke gebieden van belang in opgenomen: - Documentatiestandaarden. - Criteria voor het definiëren van een model. - Model- en modelrisico-definities. - Risicobereidheidsverklaring. - Materialiteitsverklaring. - Overzicht governance. - Beheersingsmaatregelen. - Ontwikkelingsstandaarden. - Richtlijnen voor implementatie en gebruik. - Validatie en voortdurende monitoring. - Risicobeoordelingsmethode. - Overwegingen in verband met data. - Verandermanagement. - Processen/criteria voor classificatie, escalatie en het volgen van modelkwesties. • Alle relevante voorschriften zijn opgenomen in het beleid en de procedures (bijv., SR 11-07/OCC 2011-12, Basel III, Solvency II, SR 15-18).		

Ontwikkeling, Implementatie, en Gebruik	Parafen/ Datum	WP Ref
Toewijzing ontwikkelaars		
• De verschillende vaardigheden van alle ontwikkelaars die zijn aangewezen om het model te bouwen zijn in het geheel genomen geschikt wat betreft educatieve achtergrond, ervaring en/of technische kennis.		
Algemene documentatie		
• De beslissing om het model te bouwen of te kopen was duidelijk gedocumenteerd. • Het doel van het model was gedocumenteerd. • Alle vereiste beoordelingen en goedkeuringen zijn uitgevoerd.		
Geschiktheid van het model		
• De technische ontwikkelingsdocumentatie is gedetailleerd genoeg voor derden om te begrijpen hoe het model is opgebouwd. • Voordat over de definitieve versie van het model werd beslist, werden alternatieve theorieën onderzocht. • De onderbouwing van alle aannames en ramingen is gedocumenteerd en lijkt redelijk. • De behandeling van en de beheersingsmaatregelen met betrekking tot de data die gebruikt zijn om het model te ontwikkelen zijn gedocumenteerd. • Voor modellen die bij een leverancier zijn gekocht, zijn gedetailleerde specificaties verkregen en beoordeeld en ondersteuning voor aanpassingen van het model is beschikbaar.		

Ontwikkeling, Implementatie, en Gebruik	Parafen/ Datum	WP Ref
Testen ontwikkelaar en eindgebruiker		
• De ontwikkelaars hebben het model aan gedetailleerde tests onderworpen om er zeker van te zijn dat het goed functioneerde. • De ontwikkelaars hebben de inputdata van het model getest op nauwkeurigheid en volledigheid. • Alle beperkingen die tijdens het testen werden vastgesteld, zijn gedocumenteerd. • Alle fouten die tijdens het testen werden geconstateerd, werden geregistreerd en gecorrigeerd. • Indien de eindgebruikers in de gelegenheid werden gesteld het model te testen, werden alle relevante opmerkingen beoordeeld en waar nodig in aanmerking genomen. • Indien het model was geïmplementeerd voordat de tests waren voltooid, was het juiste bevoegdheidsniveau bij het besluit betrokken.		
Modelwijzigingen		
• Wijzigingen van het model werden vastgelegd en gedocumenteerd in overeenstemming met het beleid en de procedures. • Alle wijzigingen werden beoordeeld en goedgekeurd.		
Implementatie		
• De gebruikte modelcode was dezelfde als de code die werd getest en gevalideerd. • De geïmplementeerde versie van het model bevat de goedgekeurde aannames. • Het model en zijn in- en outputs werden geïmplementeerd in een toegangsgecontroleerde, corporate IT-infrastructuur.		
Toegangsmaatregelen		
• De werkende versie van het model is niet lokaal op afzonderlijke computers opgeslagen. • Internal auditors hebben een lijst van gebruikers met toegang tot het model verkregen en hebben informatie ingewonnen over degenen die voor hun werkzaamheden duidelijk behoefte hebben om toegang te krijgen tot het model en zij die dat niet hebben. • Internal auditors hebben een lijst van werknemers vergeleken met een lijst van gebruikers met toegang tot het model en hebben informatie ingewonnen over niet-werknemers of uit dienst getreden werknemers.		
Inputcontroles		
• Internal auditors hebben een import van data in het model door de eindgebruiker waargenomen en hebben van toepassing zijnde controles op nauwkeurigheid beoordeeld. • Alle datumvelden hebben een consistente opmaak (mm/dd/jj, jjjj/mm/dd, dd/mm/jjjj, etc.). • De data met betrekking tot upstream- en downstream-modellen zijn nauwkeurig doorgegeven. • Indien het model indicatoren heeft om een gebruiker te informeren wanneer onjuiste informatie is ingevoerd, hebben internal auditors de functionaliteit van de indicatoren getest door de eindgebruiker te vragen onjuiste data in te voeren. • Data afkomstig van verschillende bronnen worden gescheiden en geëtiketteerd. • Internal auditors hebben één reeks geïmporteerde data teruggevoerd naar het bronbestand om de nauwkeurigheid en volledigheid ervan te bevestigen.		

Ontwikkeling, Implementatie, en Gebruik	Parafen/ Datum	WP Ref
Controlemechanismen berekening		
• Alle cellen of velden waarvoor geen input van data nodig is, zijn vergrendeld en beveiligd. • Waar mogelijk is cross-footing toegepast. Internal auditors hebben herberekeningen uitgevoerd om de nauwkeurigheid te verifiëren. • Internal auditors hebben onafhankelijk de berekeningen van het model uitgevoerd om de nauwkeurigheid te verifiëren. • Waarden voor formules worden ontleend aan data-waarde-invoervellen (best practice), niet hard gecodeerd in formules. • Bij gebruik van draaitabellen is de vastlegging van alle relevante datasets gewaarborgd.		
Beoordeling output door het management		
• Het management voert een variantieanalyse uit van de feitelijke modeloutput ten opzichte van andere bekende waarden (bijv. voorgaande perioden, begrotingen, prognoses).		

Validatie	Parafen/ Datum	WP Ref
Beleid en procedures		
• In de sjablonen en richtlijnen met betrekking tot de standaard validatieprocedures van de organisatie zijn vereisten opgenomen dat de validators alle belangrijke risicogebieden moeten testen. • De organisatie heeft een frequentie vastgesteld voor validatie- en voortdurende monitoringactiviteiten. • Modellen moeten vóór de implementatie gevalideerd worden. • Er zijn gedetailleerde instructies opgesteld voor de reikwijdte en de prioriteitsbepaling van validatietests. • De risicoclassificaties van modellen worden gebruikt om de reikwijdte en prioriteitsbepaling van validatietesten te bepalen. • Bevestig dat alle geïdentificeerde modelproblemen moeten worden gedocumenteerd en gevolgd. • Het beleid en de procedures vereisen dat modellen worden getest en geanalyseerd. • Er zijn targets en acceptabele afwijkingen voor de modelnauwkeurigheid vastgesteld. • Er zijn procedures voor het beoordelen en aanpakken van onaanvaardbare afwijkingen.		
Algemeen		
• Validatie- en tijdschema's worden ter goedkeuring voorgelegd aan de betreffende partijen. • Modellen worden gevalideerd, of ze nu intern zijn gebouwd of bij een leverancier zijn gekocht. • De validatiedocumentatie is gedetailleerd genoeg voor derden om inzicht te krijgen in de uitgevoerde werkzaamheden. • De validatierapportage aan het management is accuraat en volledig. • Validators beschikken over de criteria die nodig zijn voor een doeltreffende test (d.w.z, stimulansen, competentie en invloed).		
Conceptuele deugdelijkheid		
• De validator voerde onafhankelijke tests uit om de keuze van de ontwikkelaar van theorieën, aannames, inputs, databronnen, etc. te evalueren. • De validatie omvatte gevoeligheidsanalyses en stresstests waar nodig. • De modeluitsplitsingen en/of -beperkingen die bij de validatie werden vastgesteld, zijn geregistreerd, gemonitord en gecorrigeerd of beperkt door aanvullende beheersingsmaatregelen.		

Validatie	Parafen/ Datum	WP Ref
Voortdurende monitoring		
• De modellen worden jaarlijks geëvalueerd. • Volledige of gedeeltelijke hervalidaties werden uitgevoerd indien aangegeven door de laatste jaarlijkse beoordelingsresultaten. • Modellen worden routinematig volledig gevalideerd, ongeacht de resultaten van de jaarlijkse beoordeling. • De validator(s) heeft/hebben alle overschrijdingen gecontroleerd en de juiste informatie over de overschrijdingen is geregistreerd, goedgekeurd en ondersteund. • De validator(s) vergeleek (vergeleken) de modeloutputs met alternatieve data of modellen en onderzocht(en) eventuele discrepanties (bijv. benchmarking).		
Resultatenanalyse		
• De validator(s) voerde (voerden) resultatenanalyses uit om modeloutputs te vergelijken met werkelijke resultaten (bijv. parallelle resultatenanalyse en back-testing). • Discrepanties werden onderzocht en waar nodig aangepakt.		
Datakwaliteit		
• Het management documenteerde de verwachtingen rond datakwaliteit en de validator(s) vergeleek (vergeleken) de datakwaliteitsverwachtingen met modeldata. • De validatie(s) beoordeelde(n) controlemechanismen met betrekking tot de validiteit, volledigheid, nauwkeurigheid, geschiktheid en integriteit van de data. Fouten die met behulp van de controlemechanismen werden ontdekt, werden naar behoren aangepakt. • De validator(s) heeft (hebben) het bestaande proces voor het vernieuwen en bijwerken van de data beoordeeld. • Instructies met betrekking tot datastromen, -aggregaties en -transformaties werden gedocumenteerd en beoordeeld door de validator(s). • De resultaten van elke data-aggregatiestap en transformatiestap werden gedocumenteerd. De internal auditors herhaalden de data-aggregaties en -transformaties en vergeleken elke stap met de resultaten van het bedrijf.		

Modelinventarisatie	Parafen/ Datum	WP Ref
Beleid en procedures		
• Het MRM-beleid en de MRM-procedures vereisen dat een modelinventarisatie wordt bijgehouden. • De modelinventarisatie gaat vergezeld van richtlijnen of een sjabloon. • Er zijn criteria vastgesteld om het management te helpen onderscheid te maken tussen modellen en tools of processen. • Er zijn criteria vastgesteld om elk model te beoordelen op zijn risico en/ of materialiteit.		

Modelinventarisatie	Parafen/ Datum	WP Ref
Volledigheid en nauwkeurigheid		
• De modellen die geselecteerd zijn voor validatie- en ontwikkelings-, implementatie- en gebruikstesten zijn opgenomen in de modelinventarisatie en hun informatie is nauwkeurig vastgelegd. • Indien het management de volledigheid van de modelinventarisatie moet certificeren, blijkt uit een steekproef van business lines dat alle vereiste partijen hun certificeringen hebben ingediend. • Indien het management beschikt over een mappingproces om de volledigheid van de inventarisatie te verzekeren, hebben de internal auditors een kopie ontvangen en deze op redelijkheid gecontroleerd (bijv. mapping van modellen naar posten van de jaarrekening). • De modelinventarisatie heeft geen blanco velden. • De modelinventarisatie is goed beveiligd, zodat alleen goedgekeurde personen updates kunnen uitvoeren.		
Modelclassificatie		
• De modellen die geselecteerd zijn voor validatie- en ontwikkelings-, implementatie- en gebruikstesten voldoen aan de criteria van de organisatie om als model geclassificeerd te worden. • Tools of processen die niet tot het model behoren zijn niet opgenomen in de modelinventarisatie. • Een steekproef van tools of processen die niet tot het model behoren blijkt op de juiste wijze te zijn geclassificeerd, gebaseerd op de modelcriteria van de organisatie. • Modellen voor deskundige beoordelingen zijn nauwkeurig geclassificeerd en gedocumenteerd, op basis van hun unieke aspecten met betrekking tot validatie, governance en monitoring van modellen die op adviezen van deskundigen zijn gebaseerd.		
Modelratings		
• Internal auditors hebben de door het management vastgestelde criteria voor modelratings gebruikt om de ratings van de modelinventarisatie onafhankelijk te beoordelen. • Bij afwijking van de modelrating (indien van toepassing) zijn de juiste procedures voor ondersteuning en goedkeuring gevolgd. • Indien de inventarisatie een groot aantal modellen met een lage rating bevat, wordt het geaggregeerde risico daarvan beoordeeld.		
Validatie		
• Alle modellen in de inventarisatie werden vóór de implementatie gevalideerd, tenzij anderszins naar behoren goedgekeurd voor implementatie, tijdig gevolgd door validatie. • Uit een steekproef van modellen die de initiële validatie niet hebben doorstaan blijkt dat fouten zijn geregistreerd en gecorrigeerd. • Op basis van de gegevens in de modelinventarisatie met betrekking tot het niveau van de uitgevoerde validatie blijken voor modellen met vergelijkbare classificaties passende niveaus van validatiewerkzaamheden te worden uitgevoerd. • Wijzigingen van modellen werden goedgekeurd en gevalideerd.		
Voortdurende monitoring		
• Alle modellen in de inventarisatie zijn het afgelopen jaar gevalideerd of gemonitord in het kader van het jaarlijkse evaluatieproces. • De meest recente validatiedatum of het meest recente monitoringschema van elk model is in overeenstemming met de timing die door de organisatie is goedgekeurd.		

Bijlage E.
Overzicht van de belangrijkste voorschriften

Verordening van de Europese Unie, Solvabiliteit II richtlijn.

In deze op drie pijlers gebaseerde richtlijn zijn de kapitaalvereisten (Solvabiliteitscriterium, SCR) voor verzekeraars in de Europese Unie vastgesteld, dat wil zeggen kapitaalniveaus die hen in staat stellen de ergste verwachte verliezen in een bepaald jaar op te vangen met een betrouwbaarheidsniveau van 99,5 procent. Onder de eerste pijler kunnen organisaties een standaardmodel, een volledig intern model of gedeeltelijk intern model, gebruiken om hun SCR te bepalen. De tweede pijler vereist dat een organisatie haar "beoordeling van eigen risico en solvabiliteit" afrondt, hetgeen ervoor zorgt dat het SCR die in de eerste pijler is gemodelleerd redelijk is. In de derde pijler worden de rapportageverplichtingen aan zowel de toezichthoudende instanties als het publiek verzwaard.

Indien een organisatie gebruik wenst te maken van een geheel of gedeeltelijk intern model voor de raming van haar SCR, dient zij een aanvraag in te dienen bij de Prudential Regulation Authority (PRA). De organisatie moet bij de aanvraag een modelwijzigingsbeleid ter beoordeling en goedkeuring voorleggen. De organisatie moet binnen het veranderbeleid criteria vaststellen voor het definiëren van grote en kleine modelwijzigingen. Als de PRA het model en het veranderbeleid accepteert, kan de organisatie het interne model gaan gebruiken. In de toekomst moet de organisatie de uitdrukkelijke goedkeuring van de PRA verkrijgen alvorens beleidsupdates of belangrijke modelwijzigingen uit te voeren.

Richtlijn IV kapitaalvereisten (Richtlijn 2013/36/EU).

Artikel 3 – Definities: 1. Voor de toepassing van deze Richtlijn gelden de volgende definities: [...] (11) "modelrisico": het potentiële verlies dat een instelling kan lijden als gevolg van besluiten die hoofdzakelijk op de output van de interne modellen zouden kunnen worden gebaseerd en dat te wijten is aan fouten in de ontwikkeling, implementering of aanwending van dergelijke modellen.

Artikel 85 – Operationeel risico: 1. De bevoegde autoriteiten zorgen ervoor dat instellingen beleidslijnen en procedures toepassen om de blootstelling aan operationeel risico, met inbegrip van modelrisico, te beoordelen en te beheren en zelden voorkomende, zeer ernstige gebeurtenissen af te dekken. De instellingen geven aan wat voor de toepassing van deze beleidslijnen en procedures onder operationeel risico moet worden verstaan.

Basel Comité voor bankentoezicht, Basel III.

Basel III stelt voor de banksector wereldwijd te versterken door middel van kapitaalhervormingen, liquiditeitshervormingen en algemene verbeteringen van het financiële stelsel. Er is sprake van een geleidelijke invoering en elk land dat Basel III wil aannemen, is verantwoordelijk voor het doorvoeren van de hervormingen in zijn nationale wet- en regelgeving.

Basel III stelt een verhoging voor van de kwaliteit en kwantiteit van het door organisaties aangehouden kapitaal. Dit wordt bereikt door strengere regels voor de tiering van kapitaal en strengere kapitaaleisen. Daarnaast is in het voorstel een maximale leverage ratio van 3 procent vastgelegd om te voorkomen dat organisaties een te hoge leverage hebben. Het voorstel introduceert ook een liquiditeitsdekkingsratio van 30 dagen om ervoor te zorgen dat organisaties voldoende liquiditeit behouden om bestand te zijn tegen een gestresst financieringsscenario. Voor de berekening van deze ratio moet de verwachte uitstroom van kasmiddelen in het stressscenario worden gemodelleerd.

Een andere ratio die door Basel III wordt voorgesteld, is de netto stabiele financieringsratio. Het drijft financiering naar stabiele bronnen door de beschikbare stabiele financiering van de organisatie te vergelijken met haar vereiste stabiele financiering; beide moeten worden gemodelleerd. Tot slot zijn in Basel III richtlijnen opgenomen voor het beheren van risico's. Organisaties zullen met name modellen moeten gebruiken voor het inschatten van hun tegenpartijrisico, namelijk het risico dat een organisatie haar uitstaande schulden niet op de vervaldag betaalt.

FRB Letter SR 11-7/Bulletin OCC 2011-12

SR 11-7/OCC 2011-12 is een samenwerking tussen de FRB en het Office of the Comptroller of the Currency om een leidraad voor MRM te bieden aan organisaties gedurende de gehele levenscyclus van het model. Het vereist dat organisaties over gedocumenteerd(e) beleid, procedures en beheersingsmaatregelen rond het MRM-proces beschikken. Daarnaast moeten modellen worden ontwikkeld door gekwalificeerd personeel, en moeten deze worden gevalideerd door een onafhankelijke derde en na de implementatie voortdurend worden gecontroleerd. Tot slot legt het de eindverantwoordelijkheid voor het MRM-proces bij de raad van bestuur. In deze richtlijn worden de specifieke eisen van SR 11-7/OCC 2011-12 in detail verkend.

FRB Letter SR 15-18

In SR 15-18 geeft de FRB richtlijnen voor de verwachtingen ten aanzien van kapitaalplanning en toezicht van ondernemingen die vallen binnen het kader van het Large Institution Supervision Coordinating Committee en andere grote en complexe ondernemingen. In deze richtlijnen vereist de FRB dat het senior management het kapitaalplanningsproces van een organisatie ontwerpt en beheert. Bovendien wordt van het senior management verwacht dat zij een goed inzicht heeft in de modellen voor de kapitaalplanning van de instelling, alsmede in alle daarmee verband houdende overlays (d.w.z, overrides), beperkingen en uitgangsposities. Voorts dient het senior management te worden betrokken bij de daarmee verband houdende stresstests en gevoeligheidsanalyses. Van het senior management wordt verwacht dat het elk kwartaal het gehele kapitaalplanningsproces opnieuw bekijkt. De resultaten moeten worden gerapporteerd aan de raad van bestuur, zodat deze een definitieve beslissing kan nemen over de kapitaaltoereikendheid van de organisatie.

Om te voldoen aan SR 15-18 zijn organisaties ook verplicht om stress-scenario's te ontwikkelen en te documenteren die gelijk zijn aan een door de FRB opgesteld zeer ongunstig toezichtscenario of dit overtreffen. Het effect van de stressoren op het kapitaalniveau van de organisatie wordt geprojecteerd aan de hand van modellen of andere schattingsmethoden. Om ervoor te zorgen

dat de instelling voldoende gekapitaliseerd is, worden de resultaten vergeleken met de post-stress kapitaaldoelstellingen die zijn vastgelegd binnen het kapitaalbeleid van de organisatie.

Op grond van SR 15-18 dienen instellingen te beschikken over een sterk risicobeheersingproces en een intern controlekader ter ondersteuning van hun kapitaalplanningsproces. Het interne controlekader moet bestaan uit een modelinventarisatie, het bijhouden van gedetailleerde modeldocumentatie en een onafhankelijk modelvalidatieproces. Internal auditors moeten een algemene evaluatie van het kapitaalplanningsproces uitvoeren en de resultaten rapporteren aan de raad van bestuur.

IAIS Standaard 2.2.7

Deze standaard schrijft drie tests voor om modellen te valideren die gebruikt worden bij het bepalen van de wettelijk vereiste kapitaalniveaus. Instellingen zijn verplicht de resultaten van deze tests aan de toezichthouder voor te leggen voordat het gebruik van interne modellen wordt goedgekeurd. Deze tests worden vermeld in de tekst van deze gids en worden hier opgesomd:

1. Met behulp van een statistische kwaliteitstoets wordt de kwantitatieve basismethodologie van het interne model beoordeeld. Als onderdeel van dit testproces moet de gebruiker van het model de geschiktheid van de methodologie kunnen aantonen, met inbegrip van de keuze van de input en parameters van het model, en moet hij of zij de aannames die aan het model ten grondslag liggen kunnen rechtvaardigen.
2. Een kalibratietest toont aan dat het voorgeschreven toetsingsvermogen zoals bepaald door het interne model voldoet aan de modelleercriteria die door de toezichthouder zijn gespecificeerd.
3. Een gebruikstest bevestigt dat het interne model en zijn methodologieën en resultaten volledig zijn ingebed in de risicostrategie en operationele processen van de gebruiker van het model. De standaard stelt ook dat de raad van bestuur en het senior management de algehele verantwoordelijkheid moeten hebben om ervoor te zorgen dat er adequate governance en beheersingsmaatregelen zijn met betrekking tot de constructie en het gebruik van interne modellen.

In de IAIS-richtlijn inzake het risicobeheer voor kapitaal- en solvabiliteitsdoeleinden van ondernemingen worden richtlijnen gegeven voor de kwesties die moeten worden onderzocht in de context van een intern model dat wordt gebruikt voor de beoordeling van het eigen risico en de solvabiliteit van een verzekeraar, maar niet voor wettelijke kapitaalvereisten.

Targeted Review of Internal Models (TRIM) Guide, ECB[17]

De TRIM guide, door de ECB gepubliceerd in februari 2017, geeft een interpretatie van het bestaande wettelijke kader (CRR, CRD IV, ECB guidance en overig) ten aanzien van interne modellen voor kredietrisico, marktrisico en tegenpartijrisico en ten aanzien van model governance in het algemeen. Artikel 7 van de TRIM guide geeft het volgende aan: "Een instelling moet een kader/ raamwerk voor modelrisicomanagement hebben dat

17 Toevoeging: IIA Nederland

haar in staat stelt om het modelrisico te identificeren, te begrijpen en te beheersen met betrekking tot interne modellen binnen de groep (van instellingen wordt verwacht om een effectief modelrisicomanagement kader/ raamwerk te hebben voor alle modellen)." TRIM is een doorlopend project dat verder aangepast wordt op basis van ontvangen feedback door onder (ECB) toezicht staande instellingen, on-site ECB onderzoeken, peer group analyses en ontwikkelingen in wet- en regelgeving. De verwachting is dat TRIM wordt afgerond in 2019.

Bijlage F.
Verwijzingen en aanvullende literatuur

Basel Committee on Banking Supervision. *Basel III: The liquidity coverage ratio and liquidity risk monitoring tools*. Basel, Switzerland: Bank for International Settlements, January 2013. bis.org/publ/bcbs238.pdf.

Basel Committee on Banking Supervision. *Basel III: The net stable funding ratio*. Basel, Switzerland: Bank for International Settlements, 2014. www.bis.org/bcbs/publ/d295.pdf

Board of Governors of the Federal Reserve System. SR Letter 11-7 attachment: *Supervisory Guidance on Model Risk Management*. Washington, D.C.: FRS, 2011. https://www.federalreserve.gov/supervisionreg/srletters/sr1107a1.pdf.

Board of Governors of the Federal Reserve System. SR 15-18 attachment: *Federal Reserve Supervisory Assessment of Capital Planning and Positions for LISCC Firms and Large and Complex Firms*. Washington, D.C.: FRS, 2015. https://www.federalreserve.gov/supervisionreg/srletters/sr1518_PW.pdf.

European Parliament and the Council of the European Union. "Directive 2013/36/EU of the European Parliament and of the Council of 26 June 2013," *Office Journal of the European Union*. Document 32013L0036. Luxemburg: Publications Office of the European Union, 2013. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:176:0338:0436:En:PDF

Marks, Norman. *Sarbanes-Oxley Section 404: A Guide for Management by Internal Controls Practitioners*. Altamonte Springs: The Institute of Internal Auditors, 2008. https://na.theiia.org/standards-guidance/Public%20Documents/Sarbanes-Oxley_Section_404_--_A_Guide_for_Management_2nd_edition_1_08.pdf.

International Auditing and Assurance Standards Board. International Standard on Auditing 620, "Using the Work of an Expert." New York: IFAC, 2008. http://www.ifac.org/system/files/downloads/2008_Auditing_Handbook_A190_ISA_620.pdf.

Office of the Comptroller of the Currency. Bulletin OCC 2011-12, "Description: Supervisory Guidance on Model Risk Management," by Mark Levonian. Washington, D.C.: OCC, 2011. https://www.occ.gov/news-issuances/bulletins/2011/bulletin-2011-12.html.

Office of the Superintendent for Financial Institutions. "Enterprise-Wide Model Risk Management for Deposit-Taking Institutions." No. E-23. Ottawa: OFSI, 2017. http://www.osfi-bsif.gc.ca/Eng/Docs/e23.pdf.

Organization of England, Prudential Regulation Authority. Policy Statement 2/15: *Solvency II: a new regime for insurers*. London: PRA, 2015. https://www.bankofengland.co.uk/prudential-regulation/publication/2015/solvency-2-a-new-regime-for-insurers.

Rao, Vasant, and Swaminathan Aiyer. "Models, Model Risk and Running Effective Model Management Programs" (white paper). *Cognizant*. april 2015. Teaneck: Cognizant, 2015. https://www.cognizant.com/whitepapers/model-risk-and-running-effective.pdf.

Solvency and Actuarial Issues Subcommittee. "Standard No. 2.2.7: IAIS Standard on the Use of Internal Models for Regulatory Purposes." Basel: International Association of Insurance Supervisors, 2008. https://www.iaisweb.org/file/34143/16-standard-no-227-on-the-use-of-internal-models-for-regulatory-capital-purposes.

Dankwoord

Guidance Development Team

Mark Carawan, CIA, QIAL, United States (Chairman)
Stacey Schabel, United States (Project Lead)

Global Guidance Contributors

Karl Erhardt, United States
Margaret Warianka, United States
Gloria DeSantis-Stahl, United States

IIA Global Standards and Guidance

Jeanette York, CCSA, Director (Project Lead)
Lisa Hirtzinger, CIA, QIAL, CCSA, CRMA, vice-president
Debi Roth, CIA, Managing Director
Shelli Browning, technisch schrijver
Lauressa Nelson, technisch schrijver

Het IIA wil de volgende toezichthoudende instanties bedanken voor hun steun: Financial Services Guidance Committee, Professional Guidance Advisory Council, International Internal Audit Standards Board, Professional Responsibility and Ethics Committee, en International Professional Practices Framework Oversight Council.

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 interne accountants. 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.

Disclaimer

Het IIA publiceert dit document voor informatieve en educatieve doeleinden en is als zodanig alleen bedoeld als leidraad. Deze richtlijnen zijn niet bedoeld om definitieve oplossingen te geven voor specifieke afzonderlijke omstandigheden. 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

Maart 2018

The Institute of Internal Auditors | Global

Wereldwijd hoofdkantoor
The Institute of Internal Auditors
1035 Greenwood Blvd., Suite 401
Lake Mary, FL 32746, USA
Telefoon: +1-407-937-1111
Fax: +1-407-937-1101
www.theiia.org

Instituut van
Internal Auditors
Nederland

Burgemeester Stramanweg 102a
1101 AA Amsterdam
www.iia.nl
iia@iia.nl
Tel.: 088 00 37 100