BIJLAGE D: BEOORDELINGSCRITERIA VOOR RISICOSPECIFIEKE BEHEERSING

D1 RISICOCATEGORIE: MATCHING-/RENTERISICO

Beoordeel de risicomitigerende werking van de aanwezige risicospecifieke beheersing voor de risicocategorie matching-/renterisico. Kies de score die het beste de kwaliteit van de bestaande risicospecifieke beheers-maatregelen weergeeft. Hierbij hoeft niet steeds aan alle geformuleerde criteria voldaan te worden. Het is aan de toezichthouder om te beoordelen welke criteria de doorslag geven bij de toekenning van een score.

Generieke indeling van de beheersmaatregelen:
- risico-identificatie;
- risicobeleid;
- administratieve organisatie en interne controle;
- risicomonitoring.

Definities van de generieke indeling van de beheersmaatregelen

Risico-identificatie
De mate waarin en de wijze waarop de instelling de specifieke risicocategorie zelfstandig reeds in beeld heeft gebracht, onder andere op basis van risico-inventarisatie en risicoanalyse.

Risicobeleid
De kwaliteit van het vastgelegde beleid over de mate waarin (risk appetite) en de wijze waarop (hoofdlijnen te implementeren beheersingsmaatregelen) men de betreffende risicocategorie wenst te beheersen.

Administratieve organisatie en interne controle
De mate waarin en de wijze waarop procedures, functiescheidingen, bevoegdheden, limieten en andere preventieve of overige maatregelen zijn geïmplementeerd teneinde de risicocategorie te beheersen en daarmee uitvoering te geven aan het bijbehorende risicobeleid.

Risicomonitoring
De mate waarin en de wijze waarop wordt toegezien (en bijgestuurd) op het specifieke risico en de getroffen beheersingsmaatregelen, bijvoorbeeld door middel van performancerapportages, incident- of uitzonderingen-rapportages en analyses.

Beoordelingscriteria voor risicospecifieke beheersing

1. Sterke beheersing	*2. Voldoende beheersing*
Risico-identificatie • Frequent en gedetailleerd in kaart brengen van alle relevante facetten van matching-/renterisico. • Instelling heeft goed inzicht in de verdeling van activa en passiva over looptijden. • Nieuwe producten, initiatieven, projecten worden voorafgegaan door een gedegen analyse van gerelateerd matching-/renterisico. • Op productniveau is een analyse gemaakt van de aard en omvang van het matching-/renterisico. • In risicoanalyse wordt ook expliciet aandacht besteed aan matching risico's uit hoofde van embedded options, herbelegging, garantieproducten en vreemde valuta. • Het risicomodel is volgens best-practicemethoden ontwikkeld en wordt frequent onderhouden en geëvalueerd en onafhankelijk gevalideerd. • De voor de risicomodellering gehanteerde aannames en data zijn actueel, volledig, juist, betrouwbaar en beslaan een lange horizon en zijn verkregen uit onafhankelijke bronnen. • Management en betrokkenen van alle relevante niveaus en competenties betrokken bij risico-identificatie. Volledig begrip van alle aspecten van matching-/renterisico door verantwoordelijke staf. • Risico-identificatie transparant gedocumenteerd. • Risico-identificatie gebaseerd op systematische aanpak. • Risico-identificatie vertaald in adequate prioriteitenstelling.	Risico-identificatie • Periodiek in kaart brengen van belangrijke facetten van matching-/renterisico. • Instelling heeft voldoende inzicht in de verdeling van activa en passiva over looptijden. • Belangrijke nieuwe producten, initiatieven, projecten worden voorafgegaan door een analyse op hoofdlijnen van gerelateerd matching-/renterisico. • Voor belangrijke producten is een analyse gemaakt van de aard en omvang van het matching-/renterisico. • In risicoanalyse wordt voor de belangrijkste producten aandacht besteed aan matching risico's uit hoofde van embedded options, herbelegging, garantieproducten en vreemde valuta. • Het risicomodel is volgens gebruikelijke methoden ontwikkeld en wordt periodiek geëvalueerd en onafhankelijk gevalideerd. • De voor de risicomodellering gehanteerde aannames en data zijn redelijk actueel, volledig, juist en betrouwbaar en beslaan een lange horizon en zijn gebaseerd op eigen data en data verkregen uit onafhankelijke bronnen. • Management en overige medewerkers in voldoende mate betrokken bij risico-identificatie. Voldoende begrip van alle aspecten van matching-/renterisico door verantwoordelijke staf. • Risico-identificatie acceptabel gedocumenteerd. • Risico-identificatie meestal gebaseerd op systematische aanpak. • Risico-identificatie vertaald in redelijke prioriteitenstelling.
Risicobeleid • Risicobeleid is goed afgestemd op geïdentificeerde risico's die als belangrijk zijn aangemerkt. • De instelling heeft beleid ontwikkeld ten aanzien van het aanbieden van rendementgaranties. Beleid wordt frequent geëvalueerd. • De instelling kent een sterk bezet en uitgebalanceerd ALM Comité (ALCO) wiens taken, bevoegdheden en verantwoordelijkheden in een eenduidig charter zijn vastgelegd. Het ALCO komt frequent bijeen. • ALM-beleid vastgesteld door hoogste leiding. • Kwaliteit van beleid (volledigheid, documentatieniveau, kwaliteit van de inhoud, diepgang) is sterk. • Frequent uitvoeren van ALM-studies. • Instelling heeft ten aanzien van het gebruik van derivaten om matchingrisico af te dekken uitgebreid beleid vastgesteld. • ALM-beleid adequaat vertaald naar limieten op risico's en de maximale impact op de financiële positie. • ALM-beleid adequaat doorvertaald naar onder meer kredietbeleid, marktrisicobeleid en productportefeuillebeleid.	Risicobeleid • Risicobeleid is redelijk afgestemd op geïdentificeerde risico's die als belangrijk zijn aangemerkt. • De instelling heeft beleid ontwikkeld ten aanzien van het aanbieden van rendementgaranties. • De instelling kent een ALM Comité (ALCO) waarvan taken, bevoegdheden en verantwoordelijkheden globaal zijn vastgelegd. Comité komt periodiek bijeen. • ALM-beleid, voorzover niet passend binnen de door de hoogste leiding vastgestelde kaders, wordt ter goedkeuring voorgelegd aan de hoogste leiding. • Kwaliteit van beleid (volledigheid, documentatieniveau, kwaliteit van de inhoud, diepgang) is bevredigend. • Eens in de paar jaar uitvoeren van ALM-studie. • Instelling heeft ten aanzien van het gebruik van derivaten om matchingrisico af te dekken beleid vastgesteld. • ALM-beleid vertaald naar de maximale impact op de financiële positie. • ALM-beleid voldoende doorvertaald naar onder meer krediet-beleid, marktrisicobeleid en productportefeuillebeleid.

1. Sterke beheersing (vervolg)	*2. Voldoende beheersing (vervolg)*
Administratieve organisatie en interne controle • Sterke inbedding in de organisatie van het vastgestelde risicobeleid (wat tot uiting komt in procedures, functiescheidingen, bevoegdheden, limieten en preventieve maatregelen). • Procedures adequaat gedocumenteerd en actueel. • Taken, verantwoordelijkheden en bevoegdheden zijn helder en adequaat. • Beheersing vindt op eenduidige wijze (één systeem) gecentraliseerd plaats vanuit één groepsfunctie. • Goede limietbewaking. • Zeer duidelijke communicatie over indexatiebeleid (indexatiematrix, indexatieambitie, invulling geven aan indexatieambitie, toekenning indexatie, afwegingen). • De instelling maakt frequent schattingen van de uitgaande kasstromen versus beschikbare middelen teneinde tijdig middelen te kunnen vrijmaken. • Instelling heeft goede toegang tot financiële markten waar instrumenten ter afdekking van matchingrisico's worden verhandeld. • Frequent aanpassen (al dan niet met behulp van derivaten) van de matching-/renterisicopositie (indien dat op grond van het beleid nodig is). • Gebruik van spiegelportefeuilles (replicating portfolio) om renterisico van producten zonder vaste looptijd (rekening-courant, bepaalde spaarproducten) te bewaken. • Verantwoordelijkheid voor monitoring limieten en meting van exposures is onafhankelijk belegd van degenen die posities innemen. • Frequent evalueren (back testing) van gemaakte aannames in gevoeligheidsanalyses en stress tests.	Administratieve organisatie en interne controle • Voldoende inbedding in de organisatie van het vastgestelde risicobeleid (wat tot uiting komt in procedures, functie-scheidingen, bevoegdheden, limieten en preventieve maat-regelen).Procedures voldoende vastgelegd en meestal actueel. • Taken, verantwoordelijkheden en bevoegdheden zijn over het algemeen duidelijk en toereikend. • Beheersing vindt grotendeels gecentraliseerd plaats. • Redelijk goede limietbewaking. • Adequate communicatie over indexatiebeleid (indexatie-ambitie, invulling geven aan indexatieambitie, toekenning indexatie). • De instelling maakt periodiek schattingen van de uitgaande kasstromen versus beschikbare middelen teneinde tijdig middelen te kunnen vrijmaken. • Instelling heeft voldoende toegang tot financiële markten waar instrumenten ter afdekking van matchingrisico's worden verhandeld. • Periodiek aanpassen (al dan niet met behulp van derivaten) van de matching-/renterisicopositie (indien dat op grond van het beleid nodig is). • Grotendeels gebruik van spiegelportefeuilles (replicating portfolio) om renterisico van producten zonder vaste looptijd (rekening-courant, bepaalde spaarproducten) te bewaken. • Verantwoordelijkheid voor monitoring limieten en meting van exposures is meestal onafhankelijk belegd van degenen die posities innemen. • Periodiek evalueren (back testing) van gemaakte aannames in gevoeligheidsanalyses en stress tests.
Risicomonitoring • Frequente kwantificering en rapportages aan topmanagement en ALCO van de diverse facetten van matching-/renterisico in de vorm van gapanalyse, Earnings at Risk (EaR), duration van het eigen vermogen, Economic Value van het Eigen vermogen (EVE) en/of Value at Risk (VaR). • Frequentie rapportages is zeer goed afgestemd op de mate van volatiliteit in posities. • Frequent worden scenarioanalyses verricht teneinde de impact van rentewijzigingen op de omvang van het matchingrisico te bewaken en toekomstige kasstromen te monitoren.	Risicomonitoring • Periodieke kwantificering en rapportages aan topmanagement en ALCO van de diverse facetten van matching-/renterisico in de vorm van gapanalyse, Earnings at Risk (EaR), duration van het eigen vermogen, Economic Value van het Eigen vermogen (EVE) en/of Value at Risk (VaR). • Frequentie rapportages sluit voldoende aan op de mate van volatiliteit in posities. • Periodiek worden scenarioanalyses verricht teneinde de impact van rentewijzigingen op de omvang van het matchingrisico te bewaken en toekomstige kasstromen te monitoren.

3. Onvoldoende beheersing	*4. Zwakke beheersing*
Risico-identificatie • Periodiek en op hoofdlijnen in kaart brengen van facetten van matching-/ renterisico. • Instelling heeft onvoldoende inzicht in de verdeling van activa en passiva over looptijden. • Belangrijke nieuwe producten, initiatieven, projecten worden veelal pas achteraf op hoofdlijnen geanalyseerd op gerelateerd mismatch-/renterisico. • Op productniveau is meestal geen analyse gemaakt van de aard en omvang van het matching-/renterisico. • In risicoanalyse wordt summier aandacht besteed aan matchingrisico's uit hoofde van embedded options, herbelegging, garantieproducten en vreemde valuta. • Voor modellering wordt gebruikgemaakt van vuistregels of professional judgement en geen onafhankelijke validatie. • De voor de risicomodellering gehanteerde aannames en data zijn enigszins verouderd, soms onvolledig, onjuist, onbetrouwbaar en hebben betrekking op een relatief korte periode en zijn grotendeels gebaseerd op eigen data. • Onvoldoende betrokkenheid van management en medewerkers bij risico-identificatie. Onvoldoende begrip van alle aspecten van matching-/renterisico door verantwoordelijke staf. • Risico-identificatie slecht gedocumenteerd. • Risico-identificatie in onvoldoende mate gebaseerd op systematische aanpak. • Risico-identificatie onvoldoende vertaald in prioriteiten-stelling.	Risico-identificatie • Incidenteel of niet in kaart brengen van facetten van matching-/renterisico. • Instelling heeft geen inzicht in de verdeling van activa en passiva over looptijden. • Belangrijke nieuwe producten, initiatieven, projecten worden niet geanalyseerd op gerelateerde operationele risico's. • Op productniveau is geen analyse gemaakt van de aard en omvang van matching-/renterisico. • In risicoanalyse wordt geen aandacht besteed aan matchingrisico's uit hoofde van embedded options, herbelegging, garantieproducten en vreemde valuta. • Het risicomodel is niet volgens gebruikelijke methoden ontwikkeld dan wel wordt niet geëvalueerd of afhankelijk gevalideerd. • De voor de risicomodellering gehanteerde aannames en data zijn grotendeels verouderd, onvolledig, onjuist, onbetrouwbaar en hebben betrekking op een korte periode en zijn uitsluitend gebaseerd op eigen data. • Nauwelijks betrokkenheid van management en medewerkers bij risico-identificatie. Nauwelijks begrip van alle aspecten van matching-/renterisico door verantwoordelijke staf. • Risico-identificatie niet gedocumenteerd. • Risico-identificatie niet gebaseerd op systematische aanpak. • Risico-identificatie niet vertaald in prioriteitenstelling.
Risicobeleid • Risicobeleid onvoldoende afgestemd op geïdentificeerde risico's die als belangrijk zijn aangemerkt. • Onduidelijk beleid hoe om te gaan met rendementgaranties. • Op ad-hocbasis wordt een ALM-werkgroep ingesteld waarvan taken, bevoegdheden en verantwoordelijkheden zeer globaal zijn vastgelegd. • ALM-beleid, voorzover niet passend binnen de door de hoogste leiding vastgestelde kaders, wordt geregeld niet ter goedkeuring voorgelegd aan de hoogste leiding. • Kwaliteit van beleid (volledigheid, documentatieniveau, kwaliteit van de inhoud, diepgang) is onbevredigend. • Incidenteel uitvoeren ALM-studie. • Instelling heeft ten aanzien van het gebruik van derivaten om matchingrisico af te dekken nauwelijks richtlijnen vastgesteld. • ALM-beleid niet vertaald naar limieten op risico's en de maximale impact op de financiële positie. • ALM-beleid onvoldoende doorvertaald naar onder meer kredietbeleid, marktrisicobeleid en productportefeuillebeleid.	Risicobeleid • Risicobeleid niet afgestemd op geïdentificeerde risico's die als belangrijk zijn aangemerkt. • Geen beleid hoe om te gaan met rendementgaranties. • Geen ALM-werkgroep of comité • ALM-beleid, voorzover niet passend binnen de door de hoogste leiding vastgestelde kaders, wordt niet ter goed-keuring voorgelegd aan de hoogste leiding. • Kwaliteit van beleid (volledigheid, documentatieniveau, kwaliteit van de inhoud, diepgang) is onduidelijk. • Niet uitvoeren van ALM-studie. • Instelling heeft ten aanzien van het gebruik van derivaten om matchingrisico af te dekken geen beleid vastgesteld. • ALM-beleid niet vertaald naar limieten op risico's en de maximale impact op de financiële positie. • ALM-beleid niet doorvertaald naar onder meer kredietbeleid, marktrisicobeleid en productportefeuillebeleid.

3. Onvoldoende beheersing (vervolg)	*4. Zwakke beheersing (vervolg)*
Administratieve organisatie en interne controle • Onvoldoende inbedding in de organisatie van het vastgestelde risicobeleid (wat tot uiting komt in procedures, functie-scheidingen, bevoegdheden, limieten en preventieve maat-regelen). • Procedures geregeld niet vastgelegd en/of niet actueel. • Taken, verantwoordelijkheden en bevoegdheden zijn veelal onduidelijk en ontoereikend. • Beheersing vindt grotendeels decentraal plaats. • Limietbewaking is onvoldoende. • Onvoldoende communicatie over indexatiebeleid (communicatie alleen in geval van toekenning indexatie, beperkte uitleg over indexatieambitie en wijze waarop instelling hieraan invulling wil geven). • De instelling maakt incidenteel schattingen van de uitgaande kasstromen versus beschikbare middelen teneinde tijdig middelen te kunnen vrijmaken. • Instelling heeft in beperkte mate toegang tot financiële markten waar instrumenten ter afdekking van matchingrisico's worden verhandeld. • Met een lage frequentie aanpassen (al dan niet met behulp van derivaten) van de matchingrenterisicopositie. • In beperkte mate gebruik van spiegelportefeuilles (replicating portfolio) om renterisico van producten zonder vaste looptijd (rekening-courant, bepaalde spaarproducten) te bewaken. • Verantwoordelijkheid voor monitoring limieten en meting van exposures is meestal niet onafhankelijk belegd van degenen die posities innemen. • In beperkte mate evalueren (back testing) van gemaakte aannames in gevoeligheidsanalyses en stress tests.	Administratieve organisatie en interne controle • Vrijwel geen inbedding in de organisatie van het vastgestelde risicobeleid (wat tot uiting komt in procedures, functie-scheidingen, bevoegdheden, limieten en preventieve maat-regelen). • Procedures nauwelijks vastgelegd en niet actueel. • Taken, verantwoordelijkheden en bevoegdheden zijn onduidelijk en ontoereikend. • Beheersing vindt uitsluitend decentraal plaats. • Geen of zeer slechte limietbewaking. • Zwakke communicatie over indexatiebeleid (alleen communicatie over toegekende indexatie). • De instelling maakt geen schattingen van de uitgaande kasstromen versus beschikbare middelen teneinde tijdig middelen te kunnen vrijmaken. • Instelling heeft slecht toegang tot financiële markten waar instrumenten ter afdekking van matchingrisico's worden verhandeld. • Incidenteel aanpassen van de matchingrenterisicopositie. • Geen gebruik van spiegelportefeuilles (replicating portfolio) om renterisico van producten zonder vaste looptijd (rekening-courant, bepaalde spaarproducten) te bewaken. • Verantwoordelijkheid voor monitoring limieten en meting van exposures is niet onafhankelijk belegd van degenen die posities innemen. • Niet evalueren (back testing) van gemaakte aannames in gevoeligheidsanalyses en stress test.
Risicomonitoring • Incidentele kwantificering en rapportages aan topmanagement en ALCO van de diverse facetten van matching-/renterisico in de vorm van gapanalyse, Earnings at Risk (EaR), duration van het eigen vermogen, Economic Value van het Eigen vermogen (EVE) en/of Value at Risk (VaR). • Frequentie rapportages sluit onvoldoende aan op de mate van volatiliteit in posities. • Incidenteel worden scenarioanalyses verricht teneinde de impact van rentewijzigingen op de omvang van het matchingrisico te bewaken en toekomstige kasstromen te monitoren.	Risicomonitoring • Geen kwantificering en rapportages aan topmanagement en ALCO van de diverse facetten van matching-/renterisico in de vorm van gapanalyse, Earnings at Risk (EaR), duration van het eigen vermogen, Economic Value van het Eigen vermogen (EVE) en/of Value at Risk (VaR). • Frequentie van rapportages houdt geen rekening met mate van volatiliteit in posities. • Geen scenarioanalyses teneinde de impact van rente-wijzigingen op de omvang van het matchingrisico te bewaken en toekomstige kasstromen te monitoren.

D2 RISICOCATEGORIE: MARKTRISICO

Beoordeel de risicomitigerende werking van de aanwezige risicospecifieke beheersing voor de risicocategorie marktrisico. Kies de score die het beste de kwaliteit van de bestaande risicospecifieke beheersmaatregelen weergeeft. Hierbij hoeft niet steeds aan alle geformuleerde criteria voldaan te worden. Het is aan de toezichthouder om te beoordelen welke criteria de doorslag geven bij de toekenning van een score.

Generieke indeling van de beheersmaatregelen:
- risico-identificatie;
- risicobeleid;
- administratieve organisatie en interne controle;
- risicomonitoring.

Definities van de generieke indeling van de beheersmaatregelen.

Risico-identificatie
De mate waarin en de wijze waarop de instelling de specifieke risicocategorie zelfstandig reeds in beeld heeft gebracht, onder andere op basis van risico-inventarisatie en risicoanalyse.

Risicobeleid
De kwaliteit van het vastgelegde beleid over de mate waarin (risk appetite) en de wijze waarop (hoofdlijnen te implementeren beheersingsmaatregelen) men de betreffende risicocategorie wenst te beheersen.

Administratieve organisatie en interne controle
De mate waarin en de wijze waarop procedures, functiescheidingen, bevoegdheden, limieten en andere preventieve of overige maatregelen zijn geïmplementeerd teneinde de risicocategorie te beheersen en daarmee uitvoering te geven aan het bijbehorende risicobeleid.

Risicomonitoring
De mate waarin en de wijze waarop wordt toegezien (en bijgestuurd) op het specifieke risico en de getroffen beheersingsmaatregelen, bijvoorbeeld door middel van performancerapportages, incident- of uitzonderingenrapportages en analyses.

1. Sterke beheersing	*2. Voldoende beheersing*
Risico-identificatie • Frequent en gedetailleerd in kaart brengen van alle relevante facetten van marktrisico. • Nieuwe beleggingsinitiatieven, complexe beleggingsproducten, nieuwe asset classes, investeringsprojecten worden voorafgegaan door een gedegen analyse van gerelateerde marktrisico's. • Nieuwe producten worden altijd beoordeeld door een hiervoor opgericht product approval comité met vertegenwoordigers van management, front-office, risicomanagement en audit. • De voor de risicomodellering gehanteerde aannames en data zijn actueel, volledig, juist, betrouwbaar, beslaan een lange horizon en zijn verkregen uit onafhankelijke bronnen. • Het risicomodel voor modellering van marktrisico en prijsstelling van OTC-producten is volgens best-practicemethoden ontwikkeld en wordt frequent onderhouden en geëvalueerd en onafhankelijk gevalideerd. • Management en betrokkenen van alle relevante niveaus en competenties zijn betrokken bij risico-identificatie. Volledig begrip van alle aspecten van marktrisico door verantwoordelijke staf. • Risico-identificatie transparant gedocumenteerd. • Risico-identificatie gebaseerd op systematische aanpak. • Risico-identificatie vertaald in adequate prioriteitenstelling.	Risico-identificatie • Periodiek in kaart brengen van belangrijke facetten van marktrisico. • Belangrijke nieuwe beleggingsinitiatieven, complexe beleggingsproducten, nieuwe asset classes, investeringsprojecten worden voorafgegaan door een analyse op hoofdlijnen van gerelateerde marktrisico's. • Nieuwe producten worden meestal beoordeeld door een hiervoor opgericht product approval comité met vertegenwoordigers van management, front-office, risicomanagement en audit. • De voor de risicomodellering gehanteerde aannames en data zijn redelijk actueel, volledig, juist, betrouwbaar, beslaan een lange horizon en zijn gebaseerd op eigen data en data uit onafhankelijke bronnen. • Het risicomodel voor modellering van marktrisico en prijsstelling van OTC-producten is volgens gebruikelijke methoden ontwikkeld en wordt periodiek geëvalueerd en onafhankelijk gevalideerd. • Management en overige medewerkers zijn in voldoende mate betrokken bij risico-identificatie. Voldoende begrip van alle aspecten van marktrisico door verantwoordelijke staf. • Risico-identificatie acceptabel gedocumenteerd. • Risico-identificatie meestal gebaseerd op systematische aanpak. • Risico-identificatie vertaald in redelijke prioriteitenstelling.
Risicobeleid • Marktrisicomanagementbeleid en risk appetitie in deze vastgesteld door hoogste leiding. • Beleid niet alleen op het hoogste niveau binnen de instelling beschikbaar, echter ook voor individuele vergunninghouders binnen het grotere geheel. • Kwaliteit van beleid (volledigheid, documentatieniveau, kwaliteit van de inhoud, diepgang) is sterk. • In beleid zijn onder meer de toegestane asset classes en hun omvang, toegestane posities, limieten, value-at-risk, gewenste spreiding en de gehanteerde benchmarks gedetailleerd uitgewerkt. • Periodiek uitvoeren van (betrouwbare) lange termijn scenarioanalyses waarin een zeer breed kader van mogelijke catastrofes/externe gebeurtenissen wordt bekeken. • Er is een breed samengesteld Marktrisicocomité met een duidelijk uitgewerkt charter waarin taken, bevoegdheden en verantwoordelijkheden zijn vastgelegd.	Risicobeleid • Marktrisicomanagementbeleid en risk appetitie in deze, voorzover niet passend binnen de door de hoogste leiding vastgestelde kaders, wordt ter goedkeuring voorgelegd aan de hoogste leiding. • Beleid alleen op hoogste niveau binnen de instelling beschikbaar. • Kwaliteit van beleid (volledigheid, documentatieniveau, kwaliteit van de inhoud, diepgang) is bevredigend. • In beleid zijn onder meer de toegestane asset classes en hun omvang, toegestane posities, limieten, value-at-risk, gewenste spreiding en gehanteerde benchmarks voldoende uitgewerkt. • Periodiek uitvoeren van lange termijn scenarioanalyses waarin mogelijke catastrofes/externe gebeurtenissen wordt bekeken. • De instelling kent een Marktrisicocomité waarvan taken, bevoegdheden en verantwoordelijkheden globaal zijn vastgelegd.

1. Sterke beheersing (vervolg)	*2. Voldoende beheersing (vervolg)*
Administratieve organisatie en interne controle • Sterke inbedding in de organisatie van het vastgestelde risicobeleid (wat tot uiting komt in procedures, functiescheidingen, bevoegdheden, limieten en preventieve maatregelen). • Adequate functiescheiding en toepassing van vierogenprincipes ten aanzien van initiatie, autorisatie, uitvoering, administratie en controle van beleggings- of investeringstransacties. • Scheiding tussen front- en back-office integraal doorgevoerd. • Scheiding tussen commercie en marktrisicobeheer tot op het hoogste niveau in de organisatie doorgevoerd. • Voicerecording wordt permanent toegepast bij transacties. • Duidelijke limietstellingen voor uit te voeren transacties en in te nemen posities. • Procedures adequaat gedocumenteerd en actueel. • Taken, verantwoordelijkheden en bevoegdheden zijn helder en adequaat. • Juist, tijdig, volledig vastleggen van uitgevoerde transacties, ingenomen risicoposities en aangegane verplichtingen. • Kwalitatief hoogwaardig systeem voor ondersteuning van de administratie van transacties en posities en voor signalering van overschrijding van limieten. • Frequent evalueren (back testing) van gemaakte aannames in gevoeligheidsanalyses en stress tests. • Adequate procedure voor onafhankelijke vaststelling en toetsing van prijzen van wel en niet-marktgenoteerde producten.	Administratieve organisatie en interne controle • Voldoende inbedding in de organisatie van het vastgestelde risicobeleid (wat tot uiting komt in procedures, functiescheidingen, bevoegdheden, limieten en preventieve maatregelen). • Voldoende functiescheiding en toepassing van vierogenprincipes ten aanzien van initiatie, autorisatie, uitvoering, administratie en controle van beleggings- of investeringstransacties. • Voldoende scheiding tussen front- en back-office. • Scheiding tussen commercie en marktrisicobeheer op een hoog niveau in de organisatie doorgevoerd. • Voicerecording wordt toegepast bij belangrijke transacties. • Limietstellingen voor uit te voeren transacties en in te nemen posities. • Procedures voldoende vastgelegd en meestal actueel. • Taken, verantwoordelijkheden en bevoegdheden zijn over het algemeen duidelijk en toereikend. • Voldoende vastlegging van ingenomen risicoposities en aangegane verplichtingen. • Adequaat systeem voor ondersteuning van de administratie van transacties en posities en voor signalering voor overschrijding van limieten. • Periodiek evalueren (back testing) van gemaakte aannames in gevoeligheidsanalyses en stress tests. • Redelijk adequate procedure voor onafhankelijke vaststelling en toetsing van prijzen van wel en niet-marktgenoteerde producten.
Risicomonitoring • Dagelijkse en inzichtelijke rapportages inzake ingenomen posities, overschrijdingen van limieten en resultaten. • Wereldwijde monitoring van marktrisicoposities en hiermee samenhangende overdracht van posities voor alle producten. • Zeer frequente benchmarking van eigen beleggingsresultaten aan de markt gevolgd door analyse van afwijkingen. • Management laat zich periodiek informeren over status van risico's, kwaliteit van beheersing en status van verbeteracties. • Naast rapportages over de gebruikelijke aan (beheersing van) marktrisico gerelateerde activiteiten wordt standaard ook frequent gerapporteerd over klachten, incidenten en uitzonderingen. • Frequent uitvoeren van (betrouwbare) korte termijnscenarioanalyses en stress testing waarin een zeer breed kader van mogelijke catastrofes/externe gebeurtenissen wordt bekeken.	Risicomonitoring • Periodieke rapportages inzake ingenomen posities en overschrijdingen van limieten en resultaten. • Wereldwijde monitoring van marktrisicoposities en hiermee samenhangende overdracht van posities voor het merendeel van alle producten . • Periodieke benchmarking van eigen beleggingsresultaten aan de markt gevolgd door analyse van afwijkingen. • Management laat zich met voldoende regelmaat op hoofdlijnen informeren over risico's en de beheersing daarvan. • Naast rapportages over de gebruikelijke aan (beheersing van) marktrisico gerelateerde activiteiten wordt ook gerapporteerd over klachten, incidenten en uitzonderingen. • Periodiek uitvoeren van korte termijn scenarioanalyses en stress testing waarin mogelijke mogelijke catastrofes/externe gebeurtenissen wordt bekeken.

3. Onvoldoende beheersing	*4. Zwakke beheersing*
Risico-identificatie • Periodiek en op hoofdlijnen in kaart brengen van facetten van marktrisico. • Belangrijke nieuwe beleggingsinitiatieven, complexe beleggingsproducten, nieuwe asset classes, investeringsprojecten worden veelal pas achteraf op hoofdlijnen geanalyseerd op gerelateerde marktrisico's. • Nieuwe producten worden incidenteel beoordeeld door een hiervoor opgericht product approval comité met vertegenwoordigers van management, front-office, risicomanagement en audit. • De voor de risicomodellering gehanteerde aannames en data zijn enigszins verouderd, zijn soms niet volledig, soms niet juist, soms niet betrouwbaar en hebben betrekking op een relatief korte periode en zijn grotendeels gebaseerd op eigen data. • Voor modellering van marktrisico en prijsstelling van OTC-producten wordt gebruikgemaakt van vuistregels of professional judgement en geen onafhankelijke validatie. • Onvoldoende betrokkenheid van management en medewerkers bij risico-identificatie. Onvoldoende begrip van alle aspecten van marktrisico door verantwoordelijke staf. • Risico-identificatie slecht gedocumenteerd. • Risico-identificatie in onvoldoende mate gebaseerd op systematische aanpak. • Risico-identificatie onvoldoende vertaald in prioriteitenstelling.	Risico-identificatie • Incidenteel of niet in kaart brengen van facetten van marktrisico. • Belangrijke nieuwe beleggingsinitiatieven, complexe beleggingsproducten, nieuwe asset classes, investeringsprojecten worden niet geanalyseerd op gerelateerde marktrisico's. • Nieuwe producten worden niet beoordeeld door een product approval comité met vertegenwoordigers van management, front-office, risicomanagement en audit. • De voor de risicomodellering gehanteerde aannames en data zijn grotendeels verouderd, zijn niet volledig, niet juist, niet betrouwbaar en hebben betrekking op een korte periode en zijn uitsluitend gebaseerd op eigen data. • Het risicomodel voor modellering van marktrisico en prijsstelling van OTC-producten is niet volgens gebruikelijke methoden ontwikkeld dan wel wordt niet geëvalueerd of onafhankelijk gevalideerd. • Nauwelijks betrokkenheid van management en medewerkers bij risico-identificatie. Nauwelijks begrip van alle aspecten van marktrisico door verantwoordelijke staf. • Risico-identificatie niet gedocumenteerd. • Risico-identificatie niet gebaseerd op systematische aanpak. • Risico-identificatie niet vertaald in prioriteitenstelling.
Risicobeleid • Marktrisicomanagementbeleid en risk appetitie in deze, voorzover niet passend binnen de door de hoogste leiding vastgestelde kaders, wordt geregeld niet ter goedkeuring voorgelegd aan de hoogste leiding. • Kwaliteit van beleid (volledigheid, documentatieniveau, kwaliteit van de inhoud, diepgang) is onbevredigend. • In beleid zijn onder meer de toegestane asset classes en hun omvang, toegestane posities, limieten, value-at-risk, gewenste spreiding en gehanteerde benchmarks onvoldoende uitgewerkt. • Incidenteel uitvoeren van langetermijnscenarioanalyses waarin mogelijke catastrofes/externe gebeurtenissen wordt bekeken. • De instelling stelt op ad-hocbasis een werkgroep 'Marktrisico' in waarvan taken, bevoegdheden en verantwoordelijkheden zeer globaal zijn vastgelegd.	Risicobeleid • Marktrisicomanagementbeleid en risk appetitie in deze, voorzover niet passend binnen de door de hoogste leiding vastgestelde kaders, wordt niet ter goedkeuring voorgelegd aan de hoogste leiding. • Kwaliteit van beleid (volledigheid, documentatieniveau, kwaliteit van de inhoud, diepgang) is onduidelijk. • Zeer summier uitgewerkt beleid. • Niet uitvoeren van langetermijnscenarioanalyses waarin mogelijke catastrofes/extreme gebeurtenissen wordt bekeken. • De instelling kent geen werkgroep of comité 'Marktrisico'.

3. Onvoldoende beheersing (vervolg)	*4. Zwakke beheersing (vervolg)*
<u>Administratieve organisatie en interne controle</u> • Onvoldoende inbedding in de organisatie van het vastgestelde risicobeleid (wat tot uiting komt in procedures, functiescheidingen, bevoegdheden, limieten en preventieve maatregelen). • Onvoldoende functiescheiding en toepassing van vierogenprincipes ten aanzien van initiatie, autorisatie, uitvoering, administratie en controle van beleggings- of investeringstransacties. • Scheiding tussen front- en back-office echter binnen één afdeling. • Scheiding tussen commercie en marktrisicobeheer op een laag niveau in de organisatie doorgevoerd. • Voicerecording wordt incidenteel toegepast. • Voor uit te voeren transacties en in te nemen posities niet altijd heldere limietstellingen. • Procedures geregeld niet vastgelegd en/of niet actueel. • Taken, verantwoordelijkheden en bevoegdheden zijn veelal onduidelijk en ontoereikend. • Onvoldoende vastlegging van ingenomen risicoposities en aangegane verplichtingen. • Systeem voor ondersteuning van de administratie van transacties en posities en voor signalering van overschrijding van limieten bevat op enkele onderdelen belangrijke tekortkomingen. • In beperkte mate evalueren (back testing) van gemaakte aannames in gevoeligheidsanalyses en stress tests. • Onduidelijke procedure voor onafhankelijke vaststelling en toetsing van prijzen van wel en niet-marktgenoteerde producten.	<u>Administratieve organisatie en interne controle</u> • Vrijwel geen inbedding in de organisatie van het vastgestelde risicobeleid (wat tot uiting komt in procedures, functiescheidingen, bevoegdheden, limieten en preventieve maatregelen). • Slechte functiescheiding en toepassing van vierogenprincipes ten aanzien van initiatie, autorisatie, uitvoering, administratie en controle van beleggings- of investeringstransacties. • Geen scheiding front- en back-office. • Scheiding tussen commercie en marktrisicobeheer op een zeer laag niveau in de organisatie doorgevoerd. • Voicerecording wordt niet toegepast. • Geen limietstellingen voor uit te voeren transacties en in te nemen posities. • Procedures nauwelijks vastgelegd en niet actueel. • Taken, verantwoordelijkheden en bevoegdheden zijn onduidelijk en ontoereikend. • Nauwelijks vastlegging van ingenomen risicoposities en aangegane verplichtingen. • Systeem voor ondersteuning van de administratie van transacties en posities en voor signalering van overschrijding van limieten bevat belangrijke tekortkomingen. • Niet evalueren (back testing) van gemaakte aannames in gevoeligheidsanalyses en stress tests. • Geen procedure voor onafhankelijke vaststelling en toetsing van prijzen van wel en niet-marktgenoteerde producten.
<u>Risicomonitoring</u> • Op ad-hocbasis rapportages inzake ingenomen posities en overschrijding van limieten en resultaten. • Wereldwijde monitoring van marktrisicoposities en hiermee samenhangende overdracht van posities voor beperkt aantal producten . • Incidenteel benchmarking van eigen beleggingsresultaten aan de markt gevolgd door analyse van afwijkingen. • Management laat zich op ad-hocbasis informeren over belangrijke risico's en de beheersing daarvan. • Naast rapportages over de gebruikelijke aan (beheersing van) marktrisico gerelateerde activiteiten wordt nauwelijks gerapporteerd over klachten, incidenten en uitzonderingen. • Incidenteel uitvoeren van korte termijn scenarioanalyses en stress testing waarin mogelijke catastrofes/externe gebeurtenissen wordt bekeken.	<u>Risicomonitoring</u> • Nauwelijks rapportages inzake ingenomen posities en overschrijding van limieten en resultaten. • Wereldwijde monitoring van marktrisicoposities zonder samenhangende overdracht van posities van producten. • Geen benchmarking van eigen beleggingsresultaten aan de markt gevolgd door analyse van afwijkingen. • Management besteedt nauwelijks aandacht aan informatie over belangrijke risico's en de beheersing daarvan. • Naast rapportages over de gebruikelijke aan (beheersing van) marktrisico gerelateerde activiteiten wordt verder niet gerapporteerd over klachten, incidenten en uitzonderingen. • Niet uitvoeren van korte termijn scenarioanalyses en stress testing waarin mogelijke catastrofes/externe gebeurtenissen wordt bekeken.

D3 RISICOCATEGORIE: KREDIETRISICO

Beoordeel de risicomitigerende werking van de aanwezige risicospecifieke beheersing voor de risicocategorie kredietrisico. Kies de score die het beste de kwaliteit van de bestaande risicospecifieke beheersmaatregelen weergeeft. Hierbij hoeft niet steeds aan alle geformuleerde criteria voldaan te worden. Het is aan de toezichthouder om te beoordelen welke criteria de doorslag geven bij de toekenning van een score.

Generieke indeling van de beheersmaatregelen:
- risico-identificatie;
- risicobeleid;
- administratieve organisatie en interne controle;
- risicomonitoring.

Definities van de generieke indeling van de beheersmaatregelen

Risico-identificatie
De mate waarin en de wijze waarop de instelling de specifieke risicocategorie zelfstandig reeds in beeld heeft gebracht, onder andere op basis van risico-inventarisatie en risicoanalyse.

Risicobeleid
De kwaliteit van het vastgelegde beleid over de mate waarin (risk appetite) en de wijze waarop (hoofdlijnen te implementeren beheersingsmaatregelen) men de betreffende risicocategorie wenst te beheersen.

Administratieve organisatie en interne controle
De mate waarin en de wijze waarop procedures, functiescheidingen, bevoegdheden, limieten en andere preventieve maatregelen of overige maatregelen zijn geïmplementeerd ten einde de risicocategorie te beheersen en daarmee uitvoering te geven aan het bijbehorende risicobeleid.

Risicomonitoring
De mate waarin en de wijze waarop wordt toegezien (en bijgestuurd) op het specifieke risico en de getroffen beheersingsmaatregelen, bijvoorbeeld door middel van performancerapportages, incident- of uitzonderingenrapportages en analyses.

1. Sterke beheersing

Risico-identificatie

- Frequent en gedetailleerd in kaart brengen van alle relevante kredietrisico's.
- Frequente analyse van het risicoprofiel van de kredieten-portefeuille en classificatie naar risicobronnen en krediet-nemers.
- De voor de risicomodellering gehanteerde aannames en data zijn actueel, volledig, juist en betrouwbaar en beslaan een lange horizon en zijn verkregen uit onafhankelijke bronnen.
- Het risicomodel is volgens best-practicemethoden ontwikkeld en wordt frequent onderhouden en geëvalueerd en onafhankelijk gevalideerd.
- Gebruikte modellen voor schatting van PD, EAD en LGD zijn van hoge kwaliteit, onafhankelijk gevalideerd en door de toezichthouder geaccepteerd. De IAD heeft een audit gedaan ten aanzien van de juistheid en volledigheid van de gegevens-stromen.
- Nieuwe producten, initiatieven, projecten worden voorafgegaan door een gedegen analyse van gerelateerde kredietrisico's.
- Management en betrokkenen van alle relevante niveaus en competenties zijn betrokken bij risico-identificatie. Volledig begrip van alle aspecten van kredietrisico door verantwoordelijke staf.
- Risico-identificatie transparant gedocumenteerd.
- Risico-identificatie gebaseerd op systematische aanpak.
- Risico-identificatie vertaald in adequate prioriteitenstelling.

Risicobeleid

- Risicobeleid goed afgestemd op geïdentificeerde risico's die als belangrijk zijn aangemerkt.
- Kredietrisicobeleid geeft aan in welke mate kredietrisico's verzekerd en/of beheerst dienen te worden en met welke instrumenten.
- Kredietrisicobeleid geeft uitgebreide richtlijnen voor te verkrijgen zekerheden bij verstrekken van kredieten.
- De instelling kent een breed samengesteld kredietrisicocomité wiens taken en verantwoordelijkheden zijn vastgelegd in een charter.
- Het kredietrisicocomité komt zeer regelmatig bijeen en heeft een goede ingang tot het topmanagement. Het topmanagement is sterk betrokken.
- Beleid vastgesteld door hoogste leiding.
- Beleid uitgebreid aandacht voor concentratierisico (zeer evenwichtige spreiding in de portefeuille).
- Goed onderbouwd en gedocumenteerd kredietrisicobeleid (doelgroep, producten, markten).
- Goede vertaling naar acceptatiebeleid.
- Specifiek voor pensioenfonds: afspraken over hoogte en betaling voorschot en afrekening van de pensioenpremie liggen duidelijk vast in de financieringsovereenkomst. Voorschot pensioenpremie moet in één keer, aan het begin van het jaar, voldaan worden.

2. Voldoende beheersing

Risico-identificatie

- Periodiek op instellingsniveau in kaart brengen van relevante kredietrisico's.
- Periodieke analyse van het risicoprofiel van de kredieten-portefeuille.
- De voor de risicomodellering gehanteerde aannames en data zijn redelijk actueel, volledig, juist en betrouwbaar en hebben betrekking op een langere periode en zijn gebaseerd op eigen data en data uit onafhankelijke bron.
- Het risicomodel is volgens gebruikelijke methoden ontwikkeld en wordt periodiek geëvalueerd en onafhankelijk gevalideerd.
- Gebruikte modellen voor schatting van PD, EAD en LGD zijn van voldoende kwaliteit en door de toezichthouder geaccepteerd.
- Belangrijke nieuwe producten, initiatieven, projecten worden voorafgegaan door een analyse op hoofdlijnen van gerelateerde kredietrisico's.
- Management en overige medewerkers in voldoende mate betrokken bij risico-identificatie. Voldoende begrip van alle aspecten van kredietrisico door verantwoordelijke staf.
- Risico-identificatie acceptabel gedocumenteerd.
- Risico-identificatie meestal gebaseerd op systematische aanpak.
- Risico-identificatie vertaald in redelijke prioriteitenstelling.

Risicobeleid

- Risicobeleid redelijk afgestemd op geïdentificeerde risico's die als belangrijk zijn aangemerkt.
- Kredietrisicobeleid geeft aan of kredietrisico's verzekerd en/of beheerst dienen te worden.
- Kredietrisicobeleid geeft beperkte richtlijnen voor te verkrijgen zekerheden bij verstrekken van kredieten.
- De instelling kent een kredietrisicocomité.
- Het kredietrisicocomité komt periodiek bijeen en heeft ingang tot het topmanagement. Voldoende betrokkenheid van het topmanagement.
- Beleid, voorzover niet passend binnen de door de hoogste leiding vastgestelde kaders, wordt ter goedkeuring voorgelegd aan de hoogste leiding.
- Beleid voldoende aandacht voor concentratierisico (even-wichtige spreiding in de portefeuille).
- In het kredietrisicobeleid is voldoende onderscheid gemaakt naar doelgroep, producten en markten.
- Kredietrisicobeleid is vertaald naar acceptatiebeleid.
- Specifiek voor pensioenfonds: afspraken over hoogte en betaling voorschot en afrekening van de pensioenpremie liggen duidelijk vast in de financieringsovereenkomst. Voorschot pensioenpremie hoeft niet aan het begin van het jaar voldaan te worden.

1. Sterke beheersing (vervolg)	*2. Voldoende beheersing (vervolg)*
Administratieve organisatie en interne controle • Zeer heldere en gedegen procedure voor besluitvorming en uitvoering van transacties met kredietderivaten of garanties. • Goede inbedding in de organisatie van het vastgestelde risicobeleid (wat tot uiting komt in procedures, functiescheidingen, bevoegdheden, limieten en preventieve maatregelen). • Taken, verantwoordelijkheden en bevoegdheden zijn helder en adequaat gedocumenteerd. • Functiescheiding tussen commercie en kredietbeheer en operations is doorgevoerd tot op het hoogste besturingsniveau binnen de instelling. • Goed gedocumenteerde acceptatievoorwaarden en autorisatieprocedures. • Gedegen escalatieprocedures voor fiattering bijzondere posten. • Uitgebreide screening bij acceptatie (nieuwe derde partijen) op basis van duidelijke grondslagen. • Strikte incassoprocedure en stringente toepassing ervan. • Bij verslechtering van kredietkwaliteit worden posten tijdig overgedragen naar bijzondere beheersfuncties. • Duidelijke procedures rondom intensief beheer van moeilijke kredieten. • Frequente analyse van de kredietwaardigheid van herverzekeraars. • Frequent evalueren (back testing) van gemaakte aannames in gevoeligheidsanalyses en stress tests. • Zeer uitvoerige documentatie inzake waardering en inspectie van de zekerheden. • Zeer zorgvuldig juridisch beheer van zekerheden.	Administratieve organisatie en interne controle • Adequate procedure voor besluitvorming en uitvoering van transacties met kredietderivaten of garanties. • Voldoende inbedding in de organisatie van het vastgestelde risicobeleid (wat tot uiting komt in procedures, functiescheidingen, bevoegdheden, limieten en preventieve maatregelen). • Taken, verantwoordelijkheden en bevoegdheden zijn over het algemeen duidelijk en toereikend gedocumenteerd. • Functiescheiding tussen commercie en kredietbeheer en operations is doorgevoerd tot een hoog besturingsniveau binnen de instelling. • Acceptatievoorwaarden en autorisatieprocedures zijn van voldoende niveau. • Escalatieprocedures voor fiattering bijzondere posten. • Screening bij acceptatie (nieuwe derde partijen) op basis van duidelijke grondslagen. • Adequate incassoprocedure en adequate toepassing ervan. • Bij verslechtering van kredietkwaliteit worden posten meestal op tijd overgedragen naar bijzondere beheersfuncties. • Procedures voor beheer van moeilijke kredieten. • Analyse van de kredietwaardigheid van herverzekeraars. • Periodiek evalueren (back testing) van gemaakte aannames in gevoeligheidsanalyses en stress tests. • Voldoende documentatie inzake waardering en inspectie van de zekerheden. • Zorgvuldig juridisch beheer van zekerheden.
Risicomonitoring • Management laat zich periodiek informeren over status van risico's, kwaliteit van beheersing en status van verbeteracties. • Naast rapportages over de gebruikelijke aan (beheersing van) kredietrisico gerelateerde activiteiten wordt standaard ook frequent gerapporteerd over klachten, incidenten en uitzonderingen. • Frequente, juiste en volledige informatie over en bewaking van uitstaande kredietposities, nog niet benutte kredietposities, de ouderdom, achterstanden, verliezen, voorzieningen alsmede de kredietwaardigheid, gestelde zekerheden en concentraties. • Veranderingen in kredietwaardigheid worden tijdig gesignaleerd (bijvoorbeeld door credit-spreadanalyse) en waar nodig direct vertaald in aangepaste ratings. • Kredietinspectie is kwalitatief hoogwaardig en wordt met hoge frequentie uitgevoerd.	Risicomonitoring • Management laat zich met voldoende regelmaat op hoofdlijnen informeren over risico's en de beheersing daarvan. • Naast rapportages over de gebruikelijke aan (beheersing van) kredietrisico gerelateerde activiteiten wordt ook gerapporteerd over klachten, incidenten en uitzonderingen. • Periodieke informatie over en bewaking van uitstaande kredietposities, nog niet benutte kredietposities, de ouderdom, achterstanden, verliezen, voorzieningen alsmede de kredietwaardigheid, gestelde zekerheden en concentraties. • Veranderingen in kredietwaardigheid worden met enige vertraging gesignaleerd (bijvoorbeeld door credit-spreadanalyse) en waar nodig vertaald in aangepaste ratings. • Kredietinspectie is van voldoende kwalitatief niveau en wordt met voldoende frequentie uitgevoerd.

3. Onvoldoende beheersing	*4. Zwakke beheersing*
Risico-identificatie • Periodiek en op hoofdlijnen op instellingsniveau in kaart brengen van kredietrisico's. • Incidenteel analyse van het risicoprofiel van de kredieten-portefeuille. • De voor de risicomodellering gehanteerde aannames en data zijn enigszins verouderd, soms onvolledig, onjuist en onbetrouwbaar en hebben betrekking op een relatief korte periode en zijn grotendeels gebaseerd op eigen data. • Voor modellering wordt gebruikgemaakt van vuistregels of professional judgement en geen onafhankelijke validatie. • Belangrijke nieuwe producten, initiatieven, projecten worden veelal pas achteraf op hoofdlijnen geanalyseerd op gerelateerde kredietrisico's. • Onvoldoende betrokkenheid van management en medewerkers bij risico-identificatie. Onvoldoende begrip van alle aspecten van kredietrisico door verantwoordelijke staf. • Risico-identificatie slecht gedocumenteerd. • Risico-identificatie in onvoldoende mate gebaseerd op systematische aanpak. • Risico-identificatie onvoldoende vertaald in prioriteiten-stelling.	Risico-identificatie • Incidenteel of niet in kaart brengen van kredietrisico's. • Geen analyse van het risicoprofiel van de kredieten-portefeuille. • De voor de risicomodellering gehanteerde aannames en data zijn grotendeels verouderd, vaak onvolledig, onjuist en onbetrouwbaar en hebben betrekking op een korte periode en zijn uitsluitend gebaseerd op eigen data. • Het risicomodel is niet volgens gebruikelijke methoden ontwikkeld dan wel wordt niet geëvalueerd of onafhankelijk gevalideerd. • Belangrijke nieuwe producten, initiatieven, projecten worden niet geanalyseerd op gerelateerde kredietrisico's. • Nauwelijks betrokkenheid van management en medewerkers bij risico-identificatie. Nauwelijks begrip van alle aspecten van kredietrisico door verantwoordelijke staf. • Risico-identificatie niet gedocumenteerd. • Risico-identificatie niet gebaseerd op systematische aanpak. • Risico-identificatie niet vertaald in prioriteitenstelling.
Risicobeleid • Risicobeleid onvoldoende afgestemd op geïdentificeerde risico's die als belangrijk zijn aangemerkt. • Kredietrisicobeleid geeft onvoldoende aan of kredietrisico's verzekerd en/of beheerst dienen te worden en met welke instrumenten. • Kredietrisicobeleid geeft zeer summiere richtlijnen voor te verkrijgen zekerheden bij verstrekken van kredieten. • Kredietrisicocomité kotm slechts op ad hoc basis bijeen en bijeenkomsten vinden niet gestructureerd plaats • Kredietrisicocomité heeft in zeer beperkte mate toegang tot het topmanagement. Onvoldoende betrokkenheid van het topmanagement. • Beleid, voorzover niet passend binnen de door de hoogste leiding vastgestelde kaders, wordt geregeld niet ter goed-keuring voorgelegd aan de hoogste leiding. • Beleid onvoldoende aandacht voor concentratierisico (onvoldoende spreiding in de portefeuille). • In het kredietrisicobeleid is onvoldoende onderscheid gemaakt naar doelgroep, producten en markten. • Kredietrisicobeleid is onvoldoende vertaald naar acceptatie-beleid. • Specifiek voor pensioenfondsen: de in een financierings-overeenkomst vastgelegde afspraken over de hoogte en betaling van de pensioenpremie zijn op enkele onderdelen op diverse manieren te interpreteren.	Risicobeleid • Risicobeleid niet afgestemd op geïdentificeerde risico's die als belangrijk zijn aangemerkt. • Kredietrisicobeleid geeft niet aan of kredietrisico's verzekerd en/of beheerst dienen te worden en met welke instrumenten. • Kredietrisicobeleid geeft geen richtlijnen voor te verkrijgen zekerheden bij verstrekken van kredieten. • Geen kredietrisicocomité voor beschouwing van krediet-risico's. • Beleid, voorzover niet passend binnen de door de hoogste leiding vastgestelde kaders, wordt niet ter goedkeuring voorgelegd aan de hoogste leiding. • Beleid nauwelijks aandacht voor concentratierisico (nauwelijks spreiding in de portefeuille). • In het kredietrisicobeleid is geen onderscheid gemaakt naar doelgroep, producten en markten. • In acceptatiebeleid geen rekening gehouden met kredietrisico-beleid. • Specifiek voor pensioenfondsen: de in een financierings-overeenkomst vastgelegde afspraken over de hoogte en betaling van de pensioenpremie zijn onduidelijk.

3. Onvoldoende beheersing (vervolg)	*4. Zwakke beheersing (vervolg)*
Administratieve organisatie en interne controle • Onduidelijke procedure voor besluitvorming en uitvoering van transacties met kredietderivaten of garanties. • Onvoldoende inbedding in de organisatie van het vastgestelde risicobeleid (wat tot uiting komt in procedures, functiescheidingen, bevoegdheden, limieten en preventieve maatregelen). • Taken, verantwoordelijkheden en bevoegdheden zijn veelal onduidelijk en ontoereikend gedocumenteerd. • Functiescheiding tussen commercie en kredietbeheer en operations is doorgevoerd echter uitsluitend op een vrij laag niveau binnen de instelling. • Acceptatievoorwaarden en autorisatieprocedures zijn van onvoldoende niveau. • Voor enkele belangrijke procedures is niet voorzien in de fiattering van bijzondere posten. • Screening bij acceptatie (nieuwe derde partijen) is onvoldoende. • Incassoprocedure is niet op alle punten voldoende en/of wordt niet adequaat uitgevoerd. • Bij verslechtering van kredietkwaliteit worden posten altijd te laat overgedragen naar bijzondere beheersfuncties. • Onduidelijke procedures voor beheer van moeilijke kredieten. • Incidenteel onderzoek naar kredietwaardigheid herverzekeraar. • Incidenteel evalueren (back testing) van gemaakte aannames in gevoeligheidsanalyses en stress tests. • Onvoldoende documentatie inzake waardering en inspectie van de zekerheden. • Gebrekkig juridisch beheer van zekerheden.	Administratieve organisatie en interne controle • Geen procedure voor besluitvorming en uitvoering van transacties met kredietderivaten of garanties. • Vrijwel geen inbedding in de organisatie van het vastgestelde risicobeleid (wat tot uiting komt in procedures, functiescheidingen, bevoegdheden, limieten en preventieve maatregelen) • Taken, verantwoordelijkheden en bevoegdheden zijn onduidelijk en ontoereikend gedocumenteerd. • Functiescheiding tussen commercie en kredietbeheer en operations is op een zeer laag niveau binnen de instelling doorgevoerd. • Slechte acceptatievoorwaarden en autorisatieprocedures. • Geen procedures voor fiattering bijzondere posten. • Zeer slechte screening bij acceptatie (nieuwe derde partijen). • Slechte incassoprocedure en/of slechte naleving ervan. • Bij verslechtering van kredietkwaliteit worden posten alleen op initiatief van het accountmanagement overgedragen naar bijzondere beheersfuncties. • Geen procedures voor beheer van moeilijke kredieten. • Geen onderzoek naar kredietwaardigheid herverzekeraar. • Niet evalueren (back testing) van gemaakte aannames in gevoeligheidsanalyses en stress tests. • Slechte documentatie inzake waardering en inspectie van de zekerheden. • Slecht juridisch beheer van zekerheden.
Risicomonitoring • Management laat zich op ad hoc basis informeren over belangrijke risico's en de beheersing daarvan. • Naast rapportages over de gebruikelijke aan (beheersing van) kredietrisico gerelateerde activiteiten wordt op ad-hocbasis ook gerapporteerd over klachten, incidenten en uitzonderingen. • Juistheid, tijdigheid en volledigheid van de informatie over en bewaking van uitstaande kredietposities, nog niet benutte kredietposities, de ouderdom, achterstanden, verliezen, voorzieningen alsmede kredietwaardigheid, gestelde zekerheden en concentraties laat te wensen over. • Veranderingen in kredietwaardigheid worden met een lage frequentie gesignaleerd (bijvoorbeeld door creditspreadanalyse) en waar nodig vertaald in aangepaste ratings. • Kredietinspectie is van kwalitatief gebrekkig niveau en wordt met een lage frequentie uitgevoerd.	Risicomonitoring • Management besteedt nauwelijks aandacht aan informatie over belangrijke risico's en de beheersing daarvan. • Naast rapportages over de gebruikelijke aan (beheersing van) kredietrisico gerelateerde activiteiten wordt er verder niet gerapporteerd over klachten, incidenten en uitzonderingen. • Matige informatie over en bewaking van uitstaande kredietposities, nog niet benutte kredietposities, de ouderdom, achterstanden, verliezen, voorzieningen alsmede kredietwaardigheid, gestelde zekerheden en concentraties. • Veranderingen in kredietwaardigheid worden met een zeer lage frequentie gesignaleerd (bijvoorbeeld door creditspreadanalyse) en waar nodig vertaald in aangepaste ratings. • Geen kredietinspectie.

D4: RISICOCATEGORIE: VERZEKERINGSTECHNISCH RISICO

Beoordeel de risicomitigerende werking van de aanwezige risicospecifieke beheersing voor de risicocategorie verzekeringstechnisch risico. Kies de score die het beste de kwaliteit van de bestaande risicospecifieke beheersmaatregelen weergeeft. Hierbij hoeft niet steeds aan alle geformuleerde criteria voldaan te worden. Het is aan de toezichthouder om te beoordelen welke criteria de doorslag geven bij de toekenning van een score.

Generieke indeling van de beheersmaatregelen:
- risico-identificatie;
- risicobeleid:
- administratieve organisatie en interne controle;
- risicomonitoring.

Definities van de generieke indeling van de beheersmaatregelen.

Risico-identificatie
De mate waarin en de wijze waarop de instelling de specifieke risicocategorie zelfstandig reeds in beeld heeft gebracht, onder andere op basis van risico-inventarisatie en risicoanalyse.

Risicobeleid
De kwaliteit van het vastgelegde beleid over de mate waarin (risk appetite) en de wijze waarop (hoofdlijnen te implementeren beheersingsmaatregelen) men de betreffende risicocategorie wenst te beheersen.

Administratieve organisatie en interne controle
De mate waarin en de wijze waarop procedures, functiescheidingen, bevoegdheden, limieten, preventieve maatregelen en overige maatregelen zijn geïmplementeerd teneinde de risicocategorie te beheersen en daarmee uitvoering te geven aan het bijbehorende risicobeleid.

Risicomonitoring
De mate waarin en de wijze waarop wordt toegezien (en bijgestuurd) op het specifieke risico en de getroffen beheersingsmaatregelen, bijvoorbeeld door middel van performancerapportages, incident- of uitzonderingenrapportages en analyses.

Beoordelingscriteria voor risicospecifieke beheersing

1. Sterke beheersing	*2. Voldoende beheersing*
Risico-identificatie • Frequent in kaart brengen van alle relevante verzekerings-technische risico's op productniveau, portefeuilleniveau en het verzekerdenbestand. • Nieuwe producten, initiatieven, projecten worden voor-afgegaan door een gedegen analyse van gerelateerde verzekeringstechnische risico's- • Verzekeringstechnisch risico's worden kwantitatief gemodelleerd, grotendeels gebaseerd op eigen ervaringscijfers. • Veel aandacht voor risico's rondom concentratie en correlatie in de portefeuille. • Management en betrokkenen van alle relevante niveaus en competenties (waaronder actuarieel geschoolden) betrokken bij risico-identificatie. Volledig begrip van alle aspecten van verzekeringstechnisch risico door verantwoordelijke staf. • Risico-identificatie transparant gedocumenteerd. • Risico-identificatie gebaseerd op systematische aanpak. • Risico-identificatie vertaald in adequate prioriteitenstelling.	Risico-identificatie • Periodiek in kaart brengen van relevante verzekeringstechnische risico's op instellingsniveau. • Belangrijke nieuwe producten, initiatieven, projecten worden voorafgegaan door een analyse op hoofdlijnen van gerelateerde verzekeringstechnische risico's. • Verzekeringstechnisch risico's worden kwantitatief gemodelleerd, gebaseerd op eigen ervaringscijfers en actuele GBM/V-tabellen. • Aandacht voor risico's rondom concentratie en correlatie in de portefeuille. • Management en overige medewerkers in voldoende mate betrokken bij risico-identificatie. Voldoende begrip van alle aspecten van verzekeringstechnisch risico door verantwoordelijke staf. • Risico-identificatie acceptabel gedocumenteerd. • Risico-identificatie meestal gebaseerd op systematische aanpak. • Risico-identificatie vertaald in redelijke prioriteitenstelling.
Risicobeleid • Risicobeleid goed afgestemd op geïdentificeerde risico's die als belangrijk zijn aangemerkt. • Risicobeleid geeft aan in welke mate en op welke wijze risico's beheerst dienen te worden. • Beleid vastgesteld door hoogste leiding. • Kwaliteit van beleid (volledigheid, documentatieniveau, kwaliteit van de inhoud, diepgang) is sterk. • Stringente en heldere polisvoorwaarden. • Deugdelijk acceptatiebeleid, goed gedocumenteerd en vastgesteld door de hoogste leiding. • Op grond van polisvoorwaarden grote ruimte voor premie-stijgingen en voorwaardenwijzigingen. • Herverzekeringsbeleid vastgesteld per onder toezicht staande instelling (i.c. vergunninghouder) als mede op groepsniveau. • De instelling heeft een minimale winstgevendheids- dan wel rendementseis geformuleerd voor de prijsstelling van producten. • De instelling heeft prudent beleid geformuleerd ten aanzien van het gebruik van actuariële grondslagen. • Adequaat claimbehandelingsbeleid, goed gedocumenteerd en vastgesteld door de hoogste leiding.	Risicobeleid • Risicobeleid redelijk afgestemd op geïdentificeerde risico's die als belangrijk zijn aangemerkt. • Risicobeleid geeft aan of risico's beheerst dienen te worden. • Beleid, voorzover niet passend binnen de door de hoogste leiding vastgestelde kaders, wordt ter goedkeuring voorgelegd aan de hoogste leiding. • Kwaliteit van beleid (volledigheid, documentatieniveau, kwaliteit van de inhoud, diepgang) is bevredigend. • Duidelijke polisvoorwaarden. • Acceptabel acceptatiebeleid, voldoende gedocumenteerd. • Op grond van polisvoorwaarden ruimte voor premiestijgingen en voorwaardenwijzigingen. • Herverzekeringsbeleid vastgesteld op instellingsniveau. • De instelling heeft een winstgevendheids- dan wel rendementseis geformuleerd voor de prijsstelling van producten. • Beleid ten aanzien van actuariële grondslagen is in lijn met de minimumvereisten zoals opgenomen in wet- en regelgeving. • Acceptabel claimbehandelingsbeleid, redelijk gedocumenteerd.

1. Sterke beheersing (vervolg)	*2. Voldoende beheersing (vervolg)*
Administratieve organisatie en interne controle • Kwaliteit van procedures voor goedkeuring van nieuwe producten en activiteiten is goed. • Kwaliteit van procedures voor uitvoering van acceptatiebeleid is goed. • Productintroducties worden standaard voorafgegaan door een toets van een actuaris. • Procedures adequaat gedocumenteerd en actueel. • Goed inzicht in kostenstructuur. • Eenduidige en sterke procedures en verantwoordelijkheden voor claimafhandeling en claimreserveringen. • Deugdelijke procedures rondom acceptatie en claim-behandeling van bijzondere (grote danwel risicovolle) posten. • Heldere procedures en verantwoordelijkheden rondom beroep op herverzekering. Risicomonitoring • Heldere maandrapportages op diverse managementniveaus, waaronder topmanagement met samenvattingen van resultaten per productgroep en per component van het verzekeringstechnisch risico. • Gedegen analyses van de resultaten voorzien van toelichtingen. • Periodieke kwantitatieve analyse van concentratie en correlatie binnen de portefeuille. • Naast rapportages over de gebruikelijke aan (beheersing van) verzekeringstechnische risico gerelateerde activiteiten wordt standaard ook frequent gerapporteerd over klachten, incidenten en uitzonderingen. • Periodieke evaluatie van aannames en uitgangspunten alsmede gehanteerde prijsstelling. • Periodieke analyse van uitloopresultaten, IBNR, IBNER. • Maandelijkse monitoring van de waarde (embedded value) van nieuwe productie alsmede de bestaande portefeuille. • Periodieke analyse van transacties die ten grondslag liggen aan de resultaten, als aanvulling op de analyse van de resultaten (zoals analyse van claimgedrag, claimomvang).	Administratieve organisatie en interne controle • Kwaliteit van procedures voor goedkeuring van nieuwe producten en activiteiten is bevredigend. • Kwaliteit van procedures voor uitvoering van acceptatiebeleid is voldoende. • Nieuwe producten zijn vergezeld van een toets van een actuaris. • Procedures voldoende vastgelegd en meestal actueel. • Inzicht in kostenstructuur. • Duidelijke procedures en verantwoordelijkheden voor claimafhandeling en claimreserveringen. • Procedures rondom acceptatie en claimbehandeling van bijzondere (grote dan wel risicovolle) posten adequaat. • Vastgelegd hoe om te gaan met beroep op herverzekering. Risicomonitoring • Managementinformatie is van acceptabel niveau (betreffende resultaten per productgroep, per component van het verzekeringstechnisch risico). • Resultaten worden geanalyseerd. • Op ad-hocbasis analyse van concentratie en correlatie binnen de portefeuille. • Naast rapportages over de gebruikelijke aan (beheersing van) verzekeringstechnische risico gerelateerde activiteiten wordt ook gerapporteerd over klachten, incidenten en uitzonderingen. • Evaluatie van aannames en uitgangspunten alsmede gehanteerde prijsstelling. • Op ad-hocbasis analyse van uitloopresultaten, IBNR; IBNER. • Monitoring van de waarde (embedded value) van nieuwe productie alsmede bestaande portefeuille. • Op ad-hocbasis analyse van transacties die ten grondslag liggen aan de resultaten, als aanvulling op de analyse van de resultaten (zoals analyse van claimgedrag, claimomvang).

3. Onvoldoende beheersing	*4. Zwakke beheersing*
<u>Risico-identificatie</u> • Periodiek en op hoofdlijnen in kaart brengen van verzekeringstechnische risico's op instellingsniveau. • Belangrijke nieuwe producten, initiatieven, projecten worden veelal pas achteraf op hoofdlijnen geanalyseerd op gerelateerde verzekeringstechnische risico's. • Verzekeringstechnisch risico's worden kwantitatief gemodelleerd, grotendeels gebaseerd op GBM/V-tabellen. Gebruikte data zijn niet actueel. • Geringe aandacht voor risico's rondom concentratie en correlatie in de portefeuille. • Onvoldoende betrokkenheid van management en medewerkers bij risico-identificatie. Onvoldoende begrip van alle aspecten van verzekeringstechnisch risico door verantwoordelijke staf. • Risico-identificatie slecht gedocumenteerd. • Risico-identificatie in onvoldoende mate gebaseerd op systematische aanpak. • Risico-identificatie onvoldoende vertaald in prioriteiten-stelling.	<u>Risico-identificatie</u> • Incidenteel of niet in kaart brengen van verzekeringstechnische risico's. • Belangrijke nieuwe producten, initiatieven, projecten worden niet geanalyseerd op gerelateerde verzekeringstechnische risico's. • Verzekeringstechnisch risico's worden kwantitatief gemodelleerd, gebaseerd op verouderde GBM/V-tabellen. • Geen aandacht voor risico's rondom concentratie en correlatie in de portefeuille. • Nauwelijks betrokkenheid van management en medewerkers bij risico-identificatie. Nauwelijks begrip van alle aspecten van verzekeringstechnisch risico door verantwoordelijke staf. • Risico-identificatie niet gedocumenteerd. • Risico-identificatie niet gebaseerd op systematische aanpak. • Risico-identificatie niet vertaald in prioriteitenstelling.
<u>Risicobeleid</u> • Risicobeleid onvoldoende afgestemd op geïdentificeerde risico's die als belangrijk zijn aangemerkt. • Risicobeleid geeft onvoldoende aan of risico's beheerst dienen te worden. • Beleid, voorzover niet passend binnen de door de hoogste leiding vastgestelde kaders, wordt geregeld niet ter goed-keuring voorgelegd aan de hoogste leiding. • Kwaliteit van beleid (volledigheid, documentatieniveau, kwaliteit van de inhoud, diepgang) is onbevredigend. • Polisvoorwaarden bevatten onduidelijkheden. • Onduidelijk acceptatiebeleid. • Op grond van polisvoorwaarden nauwelijks ruimte voor premiestijgingen en voorwaardenwijzigingen. • Herverzekeringsbeleid bevat onduidelijkheden. • De instelling heeft voor enkele belangrijke producten geen winstgevendheids- dan wel rendementseis geformuleerd. • Gehanteerde actuariële grondslagen zijn deels niet prudent. • Gebrekkig claimbehandelingsbeleid, onvoldoende gedocumenteerd.	<u>Risicobeleid</u> • Risicobeleid niet afgestemd op geïdentificeerde risico's die als belangrijk zijn aangemerkt. • Risicobeleid geeft niet aan of risico's verzekerd en/of beheerst dienen te worden. • Beleid, voorzover niet passend binnen de door de hoogste leiding vastgestelde kaders, wordt niet ter goedkeuring voorgelegd aan de hoogste leiding. • Kwaliteit van beleid (volledigheid, documentatieniveau, kwaliteit van de inhoud, diepgang) is onduidelijk. • Onduidelijke polisvoorwaarden. • Geen acceptatiebeleid. • Op grond van polisvoorwaarden geen ruimte voor premie-stijgingen en voorwaardenwijzigingen. • Onduidelijk herverzekeringsbeleid. • De instelling heeft voor diverse producten geen winstgevendheids- dan wel rendementseis geformuleerd. • Gehanteerde actuariële grondslagen zijn niet prudent. • Geen claimbehandelingsbeleid.

3. Onvoldoende beheersing (vervolg)	*4. Zwakke beheersing (vervolg)*
Administratieve organisatie en interne controle • Kwaliteit van procedures voor goedkeuring van nieuwe producten en activiteiten is onvoldoende. • Acceptatieprocedure laat te wensen over. • Belangrijke nieuwe producten zijn niet vergezeld van een toets van een actuaris. • Procedures geregeld niet vastgelegd en/of niet actueel. • Onvoldoende inzicht in kostenstructuur. • Onduidelijke procedures en verantwoordelijkheden voor claimafhandeling en claimreserveringen. • Procedures rondom acceptatie en claimbehandeling van bijzondere (grote dan wel risicovolle) posten laten te wensen over. • Onduidelijk hoe om te gaan met beroep op herverzekering.	Administratieve organisatie en interne controle • Kwaliteit van procedures voor goedkeuring van nieuwe producten en activiteiten is slecht of niet beschikbaar. • Slechte acceptatieprocedures. • Nieuwe producten zijn niet vergezeld van een toets van een actuaris. • Procedures nauwelijks vastgelegd en niet actueel. • Geen inzicht in kostenstructuur. • Geen procedures en verantwoordelijkheden geregeld voor claimafhandeling en claimreserveringen. • Geen procedure rondom acceptatie en claimbehandeling van bijzondere (grote dan wel risicovolle) posten. • Geen procedure voor beroep op herverzekering.
Risicomonitoring • Managementinformatie is ontoereikend. • Geen gedegen analyse van de resultaten. • Nauwelijks analyse van concentratie en correlatie binnen de portefeuille. • Naast rapportages over de gebruikelijke aan (beheersing van) verzekeringstechnisch risico gerelateerde activiteiten wordt op ad hoc basis ook gerapporteerd over klachten, incidenten en uitzonderingen. • Nauwelijks evaluatie van aannames en uitgangspunten alsmede gehanteerde prijsstelling. • Nauwelijks analyse van uitloopresultaten, IBNR; IBNER. • Nauwelijks monitoring van de waarde (embedded value) van nieuwe productie alsmede bestaande portefeuille. • Nauwelijks analyse van transacties die ten grondslag liggen aan de resultaten, als aanvulling op de analyse van de resultaten (zoals analyse van claimgedrag, claimomvang).	Risicomonitoring • Geen managementinformatie. • Geen analyse van de resultaten. • Geen analyse van concentratie en correlatie binnen de portefeuille. • Naast rapportages over de gebruikelijke aan (beheersing van) gerelateerde operationele werkzaamheden wordt verder niet gerapporteerd over klachten, incidenten en uitzonderingen. • Geen evaluatie van aannames en uitgangspunten alsmede gehanteerde prijsstelling. • Geen analyse van uitloopresultaten, IBNR; IBNER. • Geen monitoring van de waarde (embedded value) van nieuwe productie alsmede bestaande portefeuille. • Geen analyse van transacties die ten grondslag liggen aan de resultaten, als aanvulling op de analyse van de resultaten (zoals analyse van claimgedrag, claimomvang).

D5: RISICOCATEGORIE: OMGEVINGSRISICO

Beoordeel de risicomitigerende werking van de aanwezige risicospecifieke beheersing voor de risicocategorie omgevingsrisico. Kies de score die het beste de kwaliteit van de bestaande risicospecifieke beheersmaatregelen weergeeft. Hierbij hoeft niet steeds aan alle geformuleerde criteria voldaan te worden. Het is aan de toezicht-houder om te beoordelen welke criteria de doorslag geven bij de toekenning van een score.

Generieke indeling van de beheersmaatregelen:
- risico-identificatie;
- risicobeleid;
- administratieve organisatie en interne controle;
- risicomonitoring.

Definities van de generieke indeling van de beheersmaatregelen.

Risico-identificatie
De mate waarin en de wijze waarop de instelling de specifieke risicocategorie zelfstandig reeds in beeld heeft gebracht, onder andere op basis van risico-inventarisatie en risicoanalyse.

Risicobeleid
De kwaliteit van het vastgelegde beleid over de mate waarin (risk appetite) en de wijze waarop (hoofdlijnen te implementeren beheersingsmaatregelen) men de betreffende risicocategorie wenst te beheersen.

Administratieve organisatie en interne controle
De mate waarin en de wijze waarop procedures, functiescheidingen, bevoegdheden, limieten en andere preventieve of overige maatregelen zijn geïmplementeerd teneinde de risicocategorie te beheersen en daarmee uitvoering te geven aan het bijbehorende risicobeleid.

Risicomonitoring
De mate waarin en de wijze waarop wordt toegezien (en bijgestuurd) op het specifieke risico en de getroffen beheersingsmaatregelen, bijvoorbeeld door middel van performance rapportages, incident- of uitzonderingen-rapportages en analyses.

Beoordelingscriteria voor risicospecifieke beheersing

1. Sterke beheersing	*2. Voldoende beheersing*
Risico-identificatie • Minimaal jaarlijkse analyse van kansen en bedreigingen vanuit de omgeving. • Frequent uitgevoerde, betrouwbare en brede scenarioanalyses. • Frequente en betrouwbare analyses van de markt, de eigen marktpositie en de veranderingen bij de concurrent. • Frequente analyse en actieve monitoring van wet- en regelgeving en de implicaties hiervan op de instelling. • De instelling is zich goed bewust van potentiële reputatie-risico's • De instelling voert een adequate analyse van afhankelijkheids-risico's en besmettingsrisico's uit (waaronder afhankelijkheid van tussenpersonen, groepsmaatschappijen, klanten, besmetting door groepsmaatschappijen). • Frequente analyse van producten van de instelling met het oog op nieuwe risico's die voortkomen uit maatschappelijke ontwikkelingen en trends (bijvoorbeeld wijzigingen in klantengedrag, moraal). • Management en betrokkenen van alle relevante niveaus en competenties betrokken bij risico-identificatie. Volledig begrip van alle aspecten van omgevingsrisico door verantwoordelijke staf. • Risico-identificatie transparant gedocumenteerd. • Risico-identificatie gebaseerd op systematische aanpak. • Risico-identificatie vertaald in adequate prioriteitenstelling. Risicobeleid • Risicobeleid goed afgestemd op geïdentificeerde risico's die als belangrijk zijn aangemerkt. • Risicobeleid geeft aan in welke mate risico's beheerst dienen te worden. • Beleid vastgesteld door hoogste leiding. • Kwaliteit van beleid (volledigheid, documentatieniveau, kwaliteit van de inhoud, diepgang) is sterk. • Instellingsstrategie geeft blijk van inzicht in belangrijke kansen en bedreigingen van buiten de instelling. Strategie goed afgestemd op ontwikkelingen op het gebied van de markt, de technologie, de politiek en het bestuur. • Zeer adequaat anticyclisch beleid inzake conjunctuurcyclus. • Gedetailleerd uitgewerkt noodscenario aanwezig inzake reactie op eventuele reputatieschade. • Gedetailleerd beleid uitgewerkt inzake toegang van verbonden ondernemingen tot het kapitaal/dividend van de instelling (waaronder het schuiven met kapitaal). • Sponsor pensioenfonds heeft geen invloed op het beleggings-beleid. • Bevoegdheden sponsor pensioenfonds gaan niet verder dan strikt noodzakelijk en zijn ook als zodanig vastgelegd.	risico-identificatie • Eens in de paar jaar een analyse van kansen en bedreigingen vanuit de omgeving. • Periodiek uitgevoerde adequate scenarioanalyses. • Periodiek uitgevoerde adequate analyses van de markt, de eigen marktpositie en de veranderingen bij de concurrent. • Periodiek analyse en monitoring van wet- en regelgeving en de implicaties hiervan op de instelling. • De instelling is zich bewust van potentiële reputatierisico's. • De instelling voert een analyse van afhankelijkheidsrisico's en besmettingsrisico's uit (waaronder afhankelijkheid van tussenpersonen, groepsmaatschappijen, klanten, besmetting door groepsmaatschappijen). • Periodieke analyse van producten van de instelling met het oog op nieuwe risico's die voortkomen uit maatschappelijke ontwikkelingen en trends (bijvoorbeeld wijzigingen in klantengedrag, moraal). • Management en overige medewerkers in voldoende mate betrokken bij risico-identificatie. Voldoende begrip van alle aspecten van omgevingsrisico door verantwoordelijke staf. • Risico-identificatie acceptabel gedocumenteerd. • Risico-identificatie meestal gebaseerd op systematische aanpak. • Risico-identificatie vertaald in redelijke prioriteitenstelling. Risicobeleid • Risicobeleid redelijk afgestemd op geïdentificeerde risico's die als belangrijk zijn aangemerkt. • Risicobeleid geeft aan of risico's beheerst dienen te worden. • Beleid, voorzover niet passend binnen de door de hoogste leiding vastgestelde kaders, wordt ter goedkeuring voorgelegd aan de hoogste leiding. • Kwaliteit van beleid (volledigheid, documentatieniveau, kwaliteit van de inhoud, diepgang) is bevredigend. • Strategie voldoende afgestemd op ontwikkelingen op het gebied van de markt, de technologie, de politiek en het bestuur. • Anticylisch beleid inzake conjunctuurcyclus is voldoende. • Noodscenario aanwezig inzake reactie op eventuele reputatie-schade. • Beleid aanwezig inzake toegang van verbonden onder-nemingen tot het kapitaal/dividend van de instelling (waaronder het schuiven met kapitaal). • Sponsor pensioenfonds heeft vrijwel geen invloed op het beleggingsbeleid. • Bevoegdheden sponsor pensioenfonds voldoende ingeperkt en als zodanig vastgelegd.

1. Sterke beheersing (vervolg)	*2. Voldoende beheersing (vervolg)*
Administratieve organisatie en interne controle • Zeer heldere taakverdeling tussen bestuur pensioenfonds en de sponsor, vastgelegd in statuten en pensioenreglementen. • Pensioenfondsbestuursleden namens de werknemers worden ruimschoots in de gelegenheid gesteld kwalitatieve opleidingen te volgen en tijd te spenderen voor pensioenfonds-activiteiten. Voorzitter pensioenfonds is afwisselend werkgevers- en werknemerslid. • Goede communicatie tussen belanghebbenden. • Juridische beschermingsconstructies zijn kwalitatief hoog-waardig. Aanwezigheid van 'firewalls' om afhankelijkheids-risico's te beperken. • Instelling heeft afdeling communicatie en public relations die betrokken wordt bij externe communicatie omtrent reputatie-gevoelige onderwerpen.	Administratieve organisatie en interne controle • Heldere taakverdeling tussen bestuur pensioenfonds en de sponsor, vastgelegd in statuten en pensioenreglementen. • Pensioenfondsbestuursleden namens de werknemers worden voldoende in de gelegenheid gesteld kwalitatieve opleidingen te volgen en tijd te spenderen aan pensioenfondsactiviteiten. • Voldoende communicatie tussen belanghebbenden. • Juridische beschermingsconstructies zijn adequaat. • Instelling heeft afdeling communicatie en public relations die meestal betrokken wordt bij externe communicatie omtrent reputatiegevoelige onderwerpen.
Risicomonitoring • Heldere rapportages. • De instelling voert een frequente analyse van de markt en haar positie hierin uit (marktaandeel, rendementsvergelijkingen). • Periodieke onderzoeken naar de reputatie van de instelling. • Adequate klachtenprocedure met periodieke rapportage aan topmanagement over aard, omvang en frequentie van klachten ter identificatie van potentiële reputatierisico's. • Management laat zich periodiek informeren over status van externe risico's, kwaliteit van beheersing en status van verbeteracties.	Risicomonitoring • Rapportages van acceptabel niveau. • De instelling voert periodiek een analyse van de markt en haar positie hierin uit. • Eens in de paar jaar een onderzoek naar de reputatie van de instelling. • Klachtenprocedure met rapportage aan topmanagement over aard, omvang en frequentie van klachten ter identificatie van potentiële reputatierisico's. • Management laat zich met voldoende regelmaat op hoofd-lijnen informeren over risico's en de beheersing daarvan.

3. Onvoldoende beheersing	*4. Zwakke beheersing*
Risico-identificatie • Incidenteel een analyse van kansen en bedreigingen vanuit de omgeving. • Incidenteel uitgevoerde scenarioanalyses met onvoldoende diepgang. • Incidenteel uitgevoerde summiere analyse van de markt, de eigen marktpositie en de veranderingen bij de concurrent. • Incidenteel analyse en monitoring van wet- en regelgeving en de implicaties hiervan op de instelling. • De instelling is zich onvoldoende bewust van potentiële reputatierisico's. • De instelling voert incidenteel een analyse van afhankelijkheidsrisico's en besmettingsrisico's uit (waaronder afhankelijkheid van tussenpersonen, groepsmaatschappijen, klanten, besmetting door groepsmaatschappijen). • De instelling voert incidenteel een analyse uit van producten van de instelling met het oog op nieuwe risico's die voortkomen uit maatschappelijke ontwikkelingen en trends (bijvoorbeeld wijzigingen in klantengedrag, moraal). • Onvoldoende betrokkenheid van management en medewerkers bij risico-identificatie. Onvoldoende begrip van alle aspecten van omgevingsrisico door verantwoordelijke staf. • Risico-identificatie slecht gedocumenteerd. • Risico-identificatie in onvoldoende mate gebaseerd op systematische aanpak. • Risico-identificatie onvoldoende vertaald in prioriteiten-stelling.	Risico-identificatie • Geen analyse van kansen en bedreigingen vanuit de omgeving. • Geen scenarioanalyses uitgevoerd. • Geen periodieke analyses van de markt, de eigen marktpositie en de veranderingen bij de concurrent. • Geen analyse en monitoring van wet- en regelgeving en de implicaties hiervan op de instelling. • De instelling is zich nauwelijks bewust van potentiële reputatierisico's. • De instelling voert geen analyse van afhankelijkheidsrisico's en besmettingsrisico's uit (waaronder afhankelijkheid van tussenpersonen, groepsmaatschappijen, klanten, besmetting door groepsmaatschappijen). • De instelling voert geen analyse uit van producten van de instelling met het oog op nieuwe risico's die voortkomen uit maatschappelijke ontwikkelingen en trends (bijvoorbeeld wijzigingen in klantengedrag, moraal). • Nauwelijks betrokkenheid van management en medewerkers bij risico-identificatie. Nauwelijks begrip van alle aspecten van omgevingsrisico door verantwoordelijke staf. • Risico-identificatie niet gedocumenteerd. • Risico-identificatie niet gebaseerd op systematische aanpak. • Risico-identificatie niet vertaald in prioriteitenstelling.
Risicobeleid • Risicobeleid onvoldoende afgestemd op geïdentificeerde risico's die als belangrijk zijn aangemerkt. • Risicobeleid geeft onvoldoende aan of risico's beheerst dienen te worden. • Beleid, voorzover niet passend binnen de door de hoogste leiding vastgestelde kaders, wordt geregeld niet ter goedkeuring voorgelegd aan de hoogste leiding. • Kwaliteit van beleid (volledigheid, documentatieniveau, kwaliteit van de inhoud, diepgang) is onbevredigend. • Strategie onvoldoende afgestemd op ontwikkelingen op het gebied van de markt, de technologie, de politiek en het bestuur. • Anticyclisch beleid inzake conjunctuurcyclus is onvoldoende. • Onvoldoende uitgewerkt noodscenario aanwezig inzake reactie op eventuele reputatieschade. • Onvoldoende uitgewerkt beleid aanwezig inzake toegang van verbonden ondernemingen tot het kapitaal/dividend van de instelling (waaronder het schuiven met kapitaal). • Sponsor pensioenfonds heeft een belangrijke stem in het besluitvormingsproces inzake het beleggingsbeleid. • Bevoegdheden sponsor pensioenfonds zijn ruim en niet altijd even duidelijk vastgelegd.	Risicobeleid • Risicobeleid niet afgestemd op geïdentificeerde risico's die als belangrijk zijn aangemerkt. • Risicobeleid geeft niet aan of risico's beheerst dienen te worden. • Beleid, voorzover niet passend binnen de door de hoogste leiding vastgestelde kaders, wordt niet ter goedkeuring voorgelegd aan de hoogste leiding. • Kwaliteit van beleid (volledigheid, documentatieniveau, kwaliteit van de inhoud, diepgang) is onduidelijk. • Strategie nauwelijks afgestemd op ontwikkelingen op het gebied van de markt, de technologie, de politiek en het bestuur. • Geen anticyclisch beleid inzake conjunctuurcyclus. • Geen noodscenario aanwezig inzake reactie op eventuele reputatieschade. • Geen beleid aanwezig inzake toegang van verbonden ondernemingen tot het kapitaal/dividend van de instelling (waaronder het schuiven met kapitaal). • Sponsor pensioenfonds bepaalt het beleggingsbeleid, het bestuur voert slechts uit. • Nauwelijks inperking bevoegdheden sponsor pensioenfonds.

3. Onvoldoende beheersing (vervolg)	*4. Zwakke beheersing (vervolg)*
Administratieve organisatie en interne controle • Taakverdeling tussen bestuur pensioenfonds en de sponsor niet altijd helder (blijkt onvoldoende uit statuten en pensioen-reglementen). • Pensioenfondsbestuursleden namens de werknemers worden onvoldoende in de gelegenheid gesteld kwalitatieve opleidingen te volgen en tijd te spenderen aan pensioenfonds-activiteiten. • Onvoldoende communicatie tussen belanghebbenden. • Juridische beschermingsconstructies zijn onvoldoende. • Instelling heeft afdeling communicatie en public relations die niet altijd betrokken wordt bij externe communicatie omtrent belangrijke reputatiegevoelige onderwerpen.	Administratieve organisatie en interne controle • Taakverdeling tussen bestuur pensioenfonds en de sponsor onduidelijk (statuten en pensioenreglementen). • Pensioenfondsbestuursleden namens de werknemers krijgen nauwelijks gelegenheid opleidingen te volgen en/of tijd te spenderen aan pensioenfondsactiviteiten. • Zeer slechte communicatie tussen belanghebbenden. • Geen juridische beschermingsconstructies. • Instelling heeft geen afdeling communicatie en public relations die betrokken wordt bij externe communicatie omtrent reputatiegevoelige onderwerpen.
Risicomonitoring • Rapportages van onacceptabel niveau. • De instelling voert incidenteel een analyse van de markt en haar positie hierin uit. • Incidenteel een onderzoek naar de reputatie van de instelling. • Onduidelijke klachtenprocedure met rapportage aan topmanagement over aard, omvang en frequentie van klachten ter identificatie van potentiële reputatierisico's. • Management laat zich op ad-hocbasis informeren over belangrijke risico's en de beheersing daarvan.	Risicomonitoring • Geen rapportages. • De instelling voert geen analyse van de markt en haar positie hierin uit. • Geen onderzoek naar de reputatie van de instelling. • Geen klachtenprocedure met rapportage aan topmanagement over aard, omvang en frequentie van klachten ter identificatie van potentiële reputatierisico's. • Management besteedt nauwelijks aandacht aan informatie over belangrijke risico's en de beheersing daarvan.

D6: RISICOCATEGORIE: OPERATIONEEL RISICO

Beoordeel de risicomitigerende werking van de aanwezige risicospecifieke beheersing voor de risicocategorie operationeel risico. Kies de score die het beste de kwaliteit van de bestaande risicospecifieke beheersmaatregelen weergeeft. Hierbij hoeft niet steeds aan alle geformuleerde criteria voldaan te worden. Het is aan de toezicht-houder om te beoordelen welke criteria de doorslag geven bij de toekenning van een score.

Generieke indeling van de beheersmaatregelen:
- risico-identificatie;
- risicobeleid;
- administratieve organisatie en interne controle;
- risicomonitoring.

Definities van de generieke indeling van de beheersmaatregelen.

Risico-identificatie
De mate waarin en de wijze waarop de instelling de specifieke risicocategorie zelfstandig reeds in beeld heeft gebracht, onder andere op basis van risico-inventarisatie en risicoanalyse.

Risicobeleid
De kwaliteit van het vastgelegde beleid over de mate waarin (risk appetite) en de wijze waarop (hoofdlijnen te implementeren beheersingsmaatregelen) men de betreffende risicocategorie wenst te beheersen.

Administratieve organisatie en interne controle
De mate waarin en de wijze waarop procedures, functiescheidingen, bevoegdheden, limieten en andere preventieve maatregelen of overige maatregelen zijn geïmplementeerd teneinde de risicocategorie te beheersen en daarmee uitvoering te geven aan het bijbehorende risicobeleid.

Risicomonitoring
De mate waarin en de wijze waarop wordt toegezien (en bijgestuurd) op het specifieke risico en de getroffen beheersingsmaatregelen, bijvoorbeeld door middel van performance rapportages, incident- of uitzonderingen-rapportages en analyses.

Beoordelingscriteria voor risicospecifieke beheersing

1. Sterke beheersing	*2. Voldoende beheersing*
Risico-identificatie • Frequent in kaart brengen van alle relevante operationele risico's op business unit, procesniveau en productniveau. • Nieuwe producten, initiatieven, projecten worden voorafgegaan door een gedegen analyse van gerelateerde operationele risico's en fraudegevoeligheid. • Instelling verricht frequent risico c.q. control self-assessment-sessies op diverse niveaus. • Management en betrokkenen van alle relevante niveaus en competenties betrokken bij risico-identificatie. Volledig begrip van alle aspecten van operationeel risico door verantwoordelijke staf. • Risico-identificatie onderkent ook risico's in de staart van de kansverdeling (zeer hoge impact, zeer kleine kans). • Risico-identificatie transparant per bedrijfsonderdeel gedocumenteerd. • Risico-identificatie gebaseerd op systematische aanpak. Binnen deze aanpak is expliciet plaats ingeruimd voor operationele risico's. • Risico-identificatie vertaald in adequate prioriteitenstelling. • Potentiële risico's worden nader geanalyseerd naar mogelijk onderliggende oorzaken. • Instelling gebruikt een model voor de modellering van operationele risico's. De voor de risicomodellering gehanteerde aannames zijn actueel, volledig, juist en betrouwbaar.	Risico-identificatie • Periodiek in kaart brengen van relevante operationele risico's op instellingsniveau. • Belangrijke nieuwe producten, initiatieven, projecten worden voorafgegaan door een analyse op hoofdlijnen van gerelateerde operationele risico's en fraudegevoeligheid. • Instelling verricht periodiek risico c.q. control self-assessmentsessies. • Management en overige medewerkers in voldoende mate betrokken bij risico-identificatie. Voldoende begrip van alle aspecten van operationeel risico door verantwoordelijke staf. • Risico-identificatie onderkent ook risico's in de staart van de kansverdeling (zeer hoge impact, zeer kleine kans). • Risico-identificatie acceptabel per bedrijfsonderdeel gedocumenteerd. • Risico-identificatie meestal gebaseerd op systematische aanpak. • Risico-identificatie vertaald in redelijke prioriteitenstelling. • Belangrijke potentiële risico's worden nader geanalyseerd naar mogelijk onderliggende oorzaken. • Instelling gebruikt een model voor de modellering van operationele risico's. De voor de risicomodellering gehanteerde aannames zijn redelijk actueel, volledig, juist en betrouwbaar.
Risicobeleid • Risicobeleid goed afgestemd op geïdentificeerde risico's die als belangrijk zijn aangemerkt. • Risicobeleid geeft aan in welke mate risico's verzekerd en/of beheerst dienen te worden. • De instelling heeft een adequaat bemenste afdeling operationeel risicomanagement, wiens taken en verantwoordelijkheden zijn vastgelegd in een charter. Aanpassingen van beleid worden tijdig in het charter verwerkt. • De instelling kent een breed samengesteld operationeel risico comité wiens taken en verantwoordelijkheden zijn vastgelegd in een charter. • Het operationeel risico comité komt zeer regelmatig bijeen en er is sprake van sterk betrokken topmanagement. • Personeelsbeleid is goed ontwikkeld en in lijn met de strategie en is vastgesteld door de hoogste leiding. • De instelling heeft beleid opgesteld ten aanzien van fraude-preventie, het ontmoedigen van fraude alsmede het bestraffen van fraude zowel ten aanzien van interne als externe fraude. • De instelling heeft normen gesteld ten aanzien van operationele indicatoren, zoals doorlooptijden, werkvoorraden, uitval. • Operationeel risicobeleid adequaat gedocumenteerd en vastgesteld door de hoogste leiding. • Kwaliteit van beleid (volledigheid, documentatieniveau, kwaliteit van de inhoud, diepgang) is sterk.	Risicobeleid • Risicobeleid redelijk afgestemd op geïdentificeerde risico's die als belangrijk zijn aangemerkt. • Risicobeleid geeft aan of risico's verzekerd en/of beheerst dienen te worden. • De instelling heeft een afdeling operationeel risicomanagement, wienst taken en verantwoordelijkheden zijn vastgelegd in een charter. • De instelling kent een operationeel risico comité. • Het operationeel risico comité komt periodiek bijeen en er is sprake van voldoende betrokken topmanagement. • Personeelsbeleid is voldoende ontwikkeld en voldoende in lijn met de strategie. • De instelling heeft beleid opgesteld ten aanzien van fraude-preventie. • De instelling heeft normen gesteld ten aanzien van belangrijke operationele indicatoren. • Operationeel risicobeleid, voorzover niet passend binnen de door de hoogste leiding vastgestelde kaders, wordt ter goed-keuring voorgelegd aan de hoogste leiding. • Kwaliteit van beleid (volledigheid, documentatieniveau, kwaliteit van de inhoud, diepgang) is bevredigend.

1. Sterke beheersing (vervolg)

Administratieve organisatie en interne controle

- Sterke inbedding in de organisatie van het vastgestelde risicobeleid (wat tot uiting komt in procedures, functiescheidingen, bevoegdheden, limieten en preventieve maatregelen).
- Kwaliteit van procedures voor goedkeuring van nieuwe cliënten, producten en activiteiten is goed.
- Procedures adequaat gedocumenteerd en actueel.
- Taken, verantwoordelijkheden en bevoegdheden zijn helder en adequaat.
- Adequate functiescheidingen en vierogenprincipes doorgevoerd binnen risicovolle processen.
- Gedegen escalatieprocedures voor fiattering bijzondere posten.
- Adequate en onafhankelijke checks en balances bij ontwikkeling nieuwe producten.
- Productintroducties gebaseerd op goed uitgewerkte business cases en besluit hoogste leiding.
- Kwaliteit van operationele beheersmaatregelen (met betrekking tot de input, onafhankelijkheid van medewerkers, onafhankelijkheid van en afstemming tussen front-, middle- en back-office) is hoog.
- Adequate klachtenprocedure.
- Goede, onafhankelijke en frequente analyse van en rapportage over tussenrekeningen.
- Grote mate van 'straight-through-processing' en minimaal gebruik van interfaces.
- Zeer strikte en adequate procedures rondom initiatie en autorisatie van uitgaande geldstromen (waaronder een adequate procuratieregeling).

Risicomonitoring

- Heldere rapportages over operationele prestaties (operationele kengetallen en gedegen toelichting).
- Frequente en gedetaileerde uitzonderingenrapportages ten aanzien van bijzondere (grote, risicovolle) transacties.
- Management laat zich periodiek informeren over status van risico's, kwaliteit van beheersing en status van verbeteracties.
- Naast rapportages over de gebruikelijke operationele werkzaamheden wordt standaard ook frequent gerapporteerd over klachten, incidenten, fraudes en uitzonderingen.
- Beschikking over 'loss events' database opgebouwd uit zowel externe als interne data.
- Frequente en voldoende diepgaande rapportages over key risk indicatoren op cruciale processen (inclusief norm-/grenswaarden).
- Verbeterpunten van onder meer de IAD en de toezichthouder worden vastgelegd en onafhankelijk van de business bewaakt.
- Frequent uitvoeren van (betrouwbare) korte termijn scenarioanalyses en stress testing waarin een zeer breed kader van mogelijke catastrofes/externe gebeurtenissen wordt bekeken.

2. Voldoende beheersing (vervolg)

Administratieve organisatie en interne controle

- Voldoende inbedding in de organisatie van het vastgestelde risicobeleid (wat tot uiting komt in procedures, functiescheidingen, bevoegdheden, limieten en preventieve maatregelen).
- Kwaliteit van procedures voor goedkeuring van nieuwe cliënten, producten en activiteiten is bevredigend.
- Procedures voldoende vastgelegd en meestal actueel.
- Taken, verantwoordelijkheden en bevoegdheden zijn over het algemeen duidelijk en toereikend.
- Voldoende functiescheiding aanwezig.
- Voor belangrijke procedures is voorzien in fiattering van bijzondere posten.
- Voldoende checks en balances bij ontwikkeling nieuwe producten.
- Productintroducties gebaseerd op business cases en betrokkenheid van de hoogste leiding.
- Kwaliteit van operationele beheersmaatregelen (met betrekking tot de input, onafhankelijkheid van medewerkers, onafhankelijkheid van en afstemming tussen front, middle en back-office) is voldoende.
- Acceptabele klachtenprocedure.
- Periodieke analyse van en rapportage over tussenrekeningen.
- Voldoende mate van 'straight-through-processing' en redelijk beperkt gebruik van interfaces.
- Procedures rondom initiatie en autorisatie van uitgaande geldstromen (waaronder een adequate procuratieregeling) van voldoende kwalitatief niveau.

Risicomonitoring

- Managementinformatie over operationele prestaties is van acceptabel niveau.
- Periodieke uitzonderingenrapportages ten aanzien van bijzondere (grote, risicovolle) transacties.
- Management laat zich met voldoende regelmaat op hoofdlijnen informeren over risico's en de beheersing daarvan.
- Naast rapportages over de gebruikelijke operationele werkzaamheden wordt ook gerapporteerd over klachten, incidenten en uitzonderingen.
- Periodieke rapportage over key risk indicatoren op cruciale processen.
- Verbeterpunten van onder meer de IAD en de toezichthouder worden vastgelegd en bewaakt.
- Periodiek uitvoeren van (betrouwbare) korte ermijn scenarioanalyses en stress testing waarin een zeer breed kader van mogelijke catastrofes/externe gebeurtenissen wordt bekeken.

3. Onvoldoende beheersing	*4. Zwakke beheersing*
Risico-identificatie • Incidenteel in kaart brengen van operationele risico's op instellingsniveau. • Belangrijke nieuwe producten, initiatieven, projecten worden veelal pas achteraf op hoofdlijnen geanalyseerd op gerelateerde operationele risico's en fraudegevoeligheid. • Instelling verricht incidenteel risico c.q. control self-assessmentsessies. • Onvoldoende betrokkenheid van management en medewerkers bij risico-identificatie. Onvoldoende begrip van alle aspecten van operationeel risico door verantwoordelijke staf. • Risico-identificatie onderkent slechts in beperkte mate risico's in de staart van de kansverdeling (zeer hoge impact, zeer kleine kans). • Risico-identificatie acceptabel globaal gedocumenteerd. • Risico-identificatie slecht gedocumenteerd. • Risico-identificatie in onvoldoende mate gebaseerd op systematische aanpak. • Risico-identificatie onvoldoende vertaald in prioriteiten-stelling. • Belangrijke potentiële risico's worden niet nader geanalyseerd naar mogelijk onderliggende oorzaken.	Risico-identificatie • Niet in kaart brengen van operationele risico's. • Belangrijke nieuwe producten, initiatieven, projecten worden niet geanalyseerd op gerelateerde operationele risico's en fraudegevoeligheid. • Instelling verricht geen risico c.q. control self-assessment-sessies. • Nauwelijks betrokkenheid van management en medewerkers bij risico-identificatie. Nauwelijks begrip van alle aspecten van operationeel risico door verantwoordelijke staf. • Risico-identificatie onderkent geen risico's in de staart van de kansverdeling (zeer hoge impact, zeer kleine kans). • Risico-identificatie niet gedocumenteerd. • Risico-identificatie niet gebaseerd op systematische aanpak. • Risico-identificatie niet vertaald in prioriteitenstelling. • Potentiële risico's worden niet nader geanalyseerd naar mogelijk onderliggende oorzaken.
Risicobeleid • Risicobeleid onvoldoende afgestemd op geïdentificeerde risico's die als belangrijk zijn aangemerkt. • Risicobeleid geeft onvoldoende aan of risico's verzekerd en/of beheerst dienen te worden. • De instelling heeft een afdeling operationeel risicomanagement., Taken en verantwoordelijkheden zijn niet vastgelegd in een charter. • De instelling stelt op ad hoc basis een werkgroep operationeel risicomanagement in. • De werkgroep operationeel risicomanagement komt periodiek bijeen en er is sprake van een beperkte mate van betrokken-heid van het topmanagement. • Personeelsbeleid is onvoldoende van kwaliteit. • De instelling heeft summier beleid opgesteld ten aanzien van fraudepreventie. • De instelling heeft nauwelijks normen gesteld ten aanzien van enkele belangrijke operationele indicatoren. • Operationeel risicobeleid, voorzover niet passend binnen de door de hoogste leiding vastgestelde kaders, wordt geregeld niet ter goedkeuring voorgelegd aan de hoogste leiding. • Kwaliteit van beleid (volledigheid, documentatieniveau, kwaliteit van de inhoud, diepgang) is onbevredigend.	Risicobeleid • Risicobeleid niet afgestemd op geïdentificeerde risico's die als belangrijk zijn aangemerkt. • Risicobeleid geeft niet aan of risico's verzekerd en/of beheerst dienen te worden. • De instelling heeft geen afdeling operationeel risico-management. • De instelling kent geen werkgroep operationeel risico-management. • Personeelsbeleid is erg gebrekkig. • De instelling heeft geen beleid opgesteld inzake fraude-preventie. • De instelling heeft geen normen gesteld ten aanzien van enkele belangrijke operationele indicatoren. • Operationeel risicobeleid, voorzover niet passend binnen de door de hoogste leiding vastgestelde kaders, wordt niet ter goedkeuring voorgelegd aan de hoogste leiding. • Kwaliteit van beleid (volledigheid, documentatieniveau, kwaliteit van de inhoud, diepgang) is onduidelijk.

3. Onvoldoende beheersing (vervolg)	*4. Zwakke beheersing (vervolg)*
Administratieve organisatie en interne controle • Onvoldoende inbedding in de organisatie van het vastgestelde risicobeleid (wat tot uiting komt in procedures, functie-scheidingen, bevoegdheden, limieten en preventieve maat-regelen). • Kwaliteit van procedures voor goedkeuring van nieuwe cliënten, producten en activiteiten is onvoldoende. • Procedures geregeld niet vastgelegd en/of niet actueel. • Taken, verantwoordelijkheden en bevoegdheden zijn veelal onduidelijk en ontoereikend. • Onvoldoende functiescheiding aanwezig. • Voor enkele belangrijke procedures is niet voorzien in fiattering bijzondere posten. • Onvoldoende checks en balances bij ontwikkeling nieuwe producten. • Productintroducties regelmatig niet gebaseerd op business cases en betrokkenheid van de hoogste leiding. • Kwaliteit van operationele beheersmaatregelen (met betrekking tot de input, onafhankelijkheid van medewerkers, onafhankelijkheid van en afstemming tussen front-, middle- en back-office) is onvoldoende. • Ontoereikende klachtenprocedure. • Op ad-hocbasis analyse van en rapportage over tussen-rekeningen. • Onvoldoende mate van 'straight-through-processing' en meer dan gemiddeld gebruik van interfaces. • Gebrekkige procedures rondom initiatie en autorisatie van uitgaande geldstromen (waaronder een procuratieregeling).	Administratieve organisatie en interne controle • Vrijwel geen inbedding in de organisatie van het vastgestelde risicobeleid (wat tot uiting komt in procedures, functiescheidingen, bevoegdheden, limieten en preventieve maatregelen) • Kwaliteit van procedures voor goedkeuring van nieuwe cliënten, producten en activiteiten is slecht of niet beschikbaar. • Procedures nauwelijks vastgelegd en niet actueel. • Taken, verantwoordelijkheden en bevoegdheden zijn onduidelijk en ontoereikend. • Vrijwel geen functiescheiding aanwezig. • In procedures wordt geen rekening gehouden met fiattering van bijzondere posten. • Geen checks en balances bij ontwikkeling nieuwe producten. • Productintroducties niet gebaseerd op business cases en betrokkenheid van de hoogste leiding. • Kwaliteit van operationele beheersmaatregelen (met betrekking tot de input, onafhankelijkheid van medewerkers, onafhankelijkheid van en afstemming tussen front-, middle- en back-office) is bijzonder slecht. • Geen klachtenprocedure. • Geen analyse van en rapportage over tussenrekeningen. • Nauwelijks sprake van 'straight-through-processing' en aanzienlijk gebruik van interfaces. • Slechte procedures rondom initiatie en autorisatie van uitgaande geldstromen (waaronder een procuratieregeling).
Risicomonitoring • Managementinformatie over operationele prestaties is ontoereikend. • Incidenteel uitzonderingenrapportages ten aanzien van bijzondere (grote, risicovolle) transacties. • Management laat zich op ad-hocbasis informeren over belangrijke risico's en de beheersing daarvan. • Naast rapportages over de gebruikelijke operationele werkzaamheden wordt op ad-hocbasis ook gerapporteerd over klachten, incidenten en uitzonderingen. • Incidenteel rapportage over key risk indicatoren op cruciale processen. • Gebrekkige vastlegging en bewaking van verbeterpunten van onder meer de IAD en de toezichthouder. • Incidenteel uitvoeren van (betrouwbare) korte termijn - scenarioanalyses en stress testing waarin een zeer breed kader van mogelijke catastrofes/externe gebeurtenissen wordt bekeken.	Risicomonitoring • Geen managementinformatie over operationele prestaties. • Geen uitzonderingenrapportages ten aanzien van bijzondere (grote, risicovolle) transacties. • Management besteedt nauwelijks aandacht aan informatie over belangrijke risico's en de beheersing daarvan. • Naast rapportages over de gebruikelijke operationele werk-zaamheden wordt verder niet gerapporteerd over klachten, incidenten en uitzonderingen. • Geen rapportage over key risk indicatoren op cruciale processen. • Slechte dan wel geen vastlegging en bewaking van verbeter-punten van onder meer de IAD en de toezichthouder. • Er worden geen (betrouwbare) korte termijn scenarioanalyses en stress testing uitgevoerd van waarin een zeer breed kader van mogelijke catastrofes/externe gebeurtenissen wordt bekeken.

D7: RISICOCATEGORIE: UITBESTEDINGSRISICO

Beoordeel de risicomitigerende werking van de aanwezige risicospecifieke beheersing voor de risicocategorie uitbestedingsrisico. Kies de score die het beste de kwaliteit van de bestaande risicospecifieke beheers-maatregelen weergeeft. Hierbij hoeft niet steeds aan alle geformuleerde criteria voldaan te worden. Het is aan de toezichthouder om te beoordelen welk criteria de doorslag geven bij de toekenning van een score.

Generieke indeling van de beheersmaatregelen:
- risico-identificatie;
- risicobeleid;
- administratieve organisatie en interne controle;
- risicomonitoring.

Definities van de generieke indeling van de beheersmaatregelen

Risico-identificatie
De mate waarin en de wijze waarop de instelling de specifieke risicocategorie zelfstandig reeds in beeld heeft gebracht, onder andere op basis van risico-inventarisatie en risicoanalyse.

Risicobeleid
De kwaliteit van het vastgelegde beleid over de mate waarin (risk appetite) en de wijze waarop (hoofdlijnen te implementeren beheersingsmaatregelen) men de betreffende risicocategorie wenst te beheersen.

Administratieve organisatie en interne controle
De mate waarin en de wijze waarop procedures, functiescheidingen, bevoegdheden, limieten en andere preventieve maatregelen of overige maatregelen zijn geïmplementeerd teneinde de risicocategorie te beheersen en daarmee uitvoering te geven aan het bijbehorende risicobeleid.

Risicomonitoring
De mate waarin en de wijze waarop wordt toegezien (en bijgestuurd) op het specifieke risico en de getroffen beheersingsmaatregelen, bijvoorbeeld door middel van performancerapportages, incident- of uitzonderingen-rapportages en analyses.

Beoordelingscriteria voor risicospecifieke beheersing

1. Sterke beheersing	*2. Voldoende beheersing*
Risico-identificatie • Frequent uitvoeren van een systematische analyse van risico's die samenhangen met de uitbesteding van bedrijfsprocessen. • Analyse uitvoeren zowel op het niveau van de organisatie in zijn geheel als op het niveau van de onderscheiden bedrijfsonderdelen als per individueel uitbesteed proces. • Management en betrokkenen van alle relevante niveaus en competenties betrokken bij risico-identificatie. Volledig begrip van alle aspecten van uitbestedingsrisico door verantwoordelijke staf. • Risico-identificatie transparant gedocumenteerd. • Risico-identificatie vertaald in adequate prioriteitenstelling.	Risico-identificatie • Periodiek uitvoeren van een systematische analyse van risico's die samenhangen met de uitbesteding van bedrijfsprocessen. • Analyse uitvoeren zowel op het niveau van de organisatie in zijn geheel als op het niveau van de onderscheiden bedrijfsonderdelen. • Management en overige medewerkers in voldoende mate betrokken bij risico-identificatie. Voldoende begrip van alle aspecten van uitbestedingsrisico door verantwoordelijke staf. • Risico-identificatie acceptabel gedocumenteerd. • Risico-identificatie vertaald in redelijke prioriteitenstelling.
Risicobeleid • Instelling heeft uitbestedingsbeleid geformuleerd waarin uitgebreide aandacht is voor belangrijke hiermee samenhangende risico's alsmede algemene uitgangspunten rondom uitbesteding. • Risicobeleid goed afgestemd op geïdentificeerde risico's die als belangrijk zijn aangemerkt. • Risicobeleid geeft aan welke zaken niet door externe partijen verricht mogen worden en die niet uitbesteed mogen worden. • Risicobeleid zodanig vormgegeven dat niet tot uitbesteding over zal worden gegaan indien de instelling onvoldoende waarborgen heeft voor het handhaven van een beheerste en integere bedrijfsvoering. Er is een gedetailleerd overzicht gemaakt waaraan moet worden voldaan om een beheerste en integere bedrijfsvoering te waarborgen. • Risicobeleid zodanig vormgegeven dat niet tot uitbesteding over zal worden gegaan indien uitvoerende organisatie onvoldoende maatregelen heeft getroffen inzake fraudepreventie. Er is een gedetailleerd overzicht gemaakt waaraan moet worden voldaan om sprake te zijn van adequate fraudepreventie. • Beleid vastgesteld door hoogste leiding. • Kwaliteit van beleid (volledigheid, documentatieniveau, kwaliteit van de inhoud, diepgang) is sterk. • Keuze van de partij waaraan zaken zijn uitbesteed is goed afgestemd op de strategie van de instelling	Risicobeleid • Instelling heeft uitbestedingsbeleid geformuleerd waarin aandacht is voor belangrijke hiermee samenhangende risico's alsmede algemene uitgangspunten rondom uitbesteding. • Risicobeleid redelijk afgestemd op geïdentificeerde risico's die als belangrijk zijn aangemerkt. • Risicobeleid geeft aan welke zaken niet door externe partijen verricht mogen worden. • Risicobeleid zodanig vormgegeven dat niet tot uitbesteding over zal worden gegaan indien de instelling onvoldoende waarborgen heeft voor het handhaven van een beheerste en integere bedrijfsvoering . • Risicobeleid zodanig vormgegeven dat niet tot uitbesteding over zal worden gegaan indien uitvoerende organisatie onvoldoende maatregelen heeft getroffen inzake fraudepreventie. • Beleid, voorzover niet passend binnen de door de hoogste leiding vastgestelde kaders, wordt ter goedkeuring voorgelegd aan de hoogste leiding. • Kwaliteit van beleid (volledigheid, documentatieniveau, kwaliteit van de inhoud, diepgang) is bevredigend. • Keuze van de partij waaraan zaken zijn uitbesteed is voldoende afgestemd op de strategie van de instelling.

1. Sterke beheersing (vervolg)	*2. Voldoende beheersing (vervolg)*
Administratieve organisatie en interne controle • Adequate en strikte criteria bij het selecteren van een partner. • Nauwe betrokkenheid van het topmanagement bij besluit tot uitbesteding van kritische processen. • Zeer gedetailleerde, in een service level agreement vastgelegde kwaliteitsnormen (aard, omvang, kwaliteit, tijdigheid, servicegraad, deskundigheid, informatievoorziening, eigendom van gegevens en verplichting tot naleving van relevante wet- en regelgeving) voor zowel interne als externe leveranciers. • Mogelijkheid om uitbesteding direct te beëindigen en zelfstandig, of elders, voort te zetten. • Actueel contractenregister, inclusief continue positiebepaling. • Indien de uitvoerende organisatie voor meer dan één opdrachtgever werkt: logische scheiding gegevens en bestanden van verschillende opdrachtgevers. • Adequate klachtenprocedure. • SLA voorziet in uitgebreide mogelijkheden voor de uitbestedende instelling om de kwaliteit en beheersing bij de leverancier te monitoren.	Administratieve organisatie en interne controle • Gebruik van redelijk adequate en strikte criteria bij het selecteren van een partner. • Topmanagement is voldoende betrokken bij besluit tot uitbesteding van kritische processen. • In een service level agreement vastgelegde kwaliteitsnormen (aard, omvang, kwaliteit, tijdigheid, servicegraad, deskundigheid, informatievoorziening, eigendom van gegevens en verplichting tot naleving van relevante wet- en regelgeving) voor zowel interne als externe leveranciers. • Mogelijkheid om uitbesteding op de meeste onderdelen direct te beëindigen en zelfstandig, of elders, voort te zetten. • Actueel contractenregister. • Indien de uitvoerende organisatie voor meer dan één opdrachtgever werkt: logische scheiding van belangrijke gegevens en bestanden van verschillende opdrachtgevers. • Acceptabele klachtenprocedure. • SLA voorziet in mogelijkheden voor de uitbestedende instelling om de kwaliteit en beheersing bij de leverancier te monitoren.
Risicomonitoring • Heldere rapportages over uitbestede werkzaamheden (rapportering conform SLA en gedegen toelichting). • Snelle bijsturing op basis van de resultaten. • Interne accountantsdienst van de instelling voert regelmatig audits uit bij de partij waaraan wordt uitbesteed. • Management laat zich periodiek informeren over status van risico's, kwaliteit van beheersing en status van verbeteracties rondom uitbestede processen. • Naast rapportages met de gebruikelijke informatie over uitbestede werkzaamheden wordt standaard ook frequent gerapporteerd over klachten, incidenten en uitzonderingen. • De instelling evalueert haar tevredenheid met de bestaande vormen van uitbesteding periodiek en met een adequate frequentie.	Risicomonitoring • Managementinformatie over uitbestede werkzaamheden is van acceptabel niveau en in lijn met service level agreement. • Tijdige bijsturing op basis van de resultaten. • Interne accountantsdienst van de instelling voert audits uit bij de partij waaraan wordt uitbesteed. • Management laat zich met voldoende regelmaat op hoofdlijnen informeren over risico's en de beheersing daarvan rondom uitbestede processen. • Naast rapportages met de gebruikelijke informatie over uitbestede werkzaamheden wordt ook gerapporteerd over klachten, incidenten en uitzonderingen. • De instelling evalueert haar tevredenheid met de bestaande vormen van uitbesteding op ad-hocbasis.

3. Onvoldoende beheersing	*4. Zwakke beheersing*
Risico-identificatie • Incidenteel uitvoeren van een analyse van risico's die samenhangen met de uitbesteding van bedrijfsprocessen. • Analyse uitvoeren op grotendeels het niveau van de organisatie in zijn geheel. • Onvoldoende betrokkenheid van management en medewerkers bij risico-identificatie. Onvoldoende begrip van alle aspecten van uitbestedingsrisico door verantwoordelijke staf. • Risico-identificatie slecht gedocumenteerd. • Risico-identificatie onvoldoende vertaald in prioriteiten-stelling. Risicobeleid • Instelling heeft slechts summier uitbestedingsbeleid geformuleerd waarin zeer bescheiden aandacht is voor belangrijke hiermee samenhangende risico's als mede algemene uitgangspunten rondom uitbesteding. • Risicobeleid onvoldoende afgestemd op geïdentificeerde risico's die als belangrijk zijn aangemerkt. • Risicobeleid geeft onvoldoende aan welke zaken niet door externe partijen verricht mogen worden. • Risicobeleid onvoldoende aandacht voor de vereiste waarborgen dat voor de instelling, ook bij uitbesteding, sprake moet zijn van een beheerste en integere bedrijfsvoering. • Risicobeleid onvoldoende aandacht voor de eis dat niet tot uitbesteding mag worden overgegaan indien uitvoerende organisatie onvoldoende maatregelen heeft getroffen inzake fraudepreventie. • Beleid, voorzover niet passend binnen de door de hoogste leiding vastgestelde kaders, wordt geregeld niet ter goedkeuring voorgelegd aan de hoogste leiding. • Kwaliteit van beleid (volledigheid, documentatieniveau, kwaliteit van de inhoud, diepgang) is onbevredigend. • Keuze van de partij waaraan zaken zijn uitbesteed is onvoldoende afgestemd op de strategie van de instelling.	Risico-identificatie • Geen analyse van risico's die samenhangen met de uitbesteding van bedrijfsprocessen. • Analyse uitvoeren op uitsluitend het niveau van de organisatie in zijn geheel. • Nauwelijks betrokkenheid van management en medewerkers bij risico-identificatie. Nauwelijks begrip van alle aspecten van uitbestedingsrisico door verantwoordelijke staf. • Risico-identificatie niet gedocumenteerd. • Risico-identificatie niet vertaald in prioriteitenstelling. Risicobeleid • Instelling heeft geen uitbestedingsbeleid geformuleerd. • Risicobeleid niet afgestemd op geïdentificeerde risico's die als belangrijk zijn aangemerkt. • Risicobeleid geeft niet aan welke zaken niet door externe partijen verricht mogen worden.. • Risicobeleid geen aandacht voor de vereiste waarborgen dat voor de instelling, ook bij uitbesteding, sprake moet zijn van een beheerste en integere bedrijfsvoering. • Risicobeleid geen aandacht voor de eis dat niet tot uitbesteding mag worden overgegaan indien uitvoerende organisatie onvoldoende maatregelen heeft getroffen inzake fraudepreventie. • Beleid, voorzover niet passend binnen de door de hoogste leiding vastgestelde kaders, wordt niet ter goedkeuring voorgelegd aan de hoogste leiding. • Kwaliteit van beleid (volledigheid, documentatieniveau, kwaliteit van de inhoud, diepgang) is onduidelijk. • Keuze van de partij waaraan zaken zijn uitbesteed is niet afgestemd op de strategie van de instelling.

3. Onvoldoende beheersing (vervolg)	*4. Zwakke beheersing (vervolg)*
Administratieve organisatie en interne controle • Gebruik van onvoldoende adequate en strikte criteria bij het selecteren van een partner. • Onvoldoende betrokkenheid van het topmanagement bij besluit tot uitbesteding van kritische processen. • Onvoldoende vastlegging van dan wel in summiere algemene bewoordingen afgesproken kwaliteitsnormen inzake uitbestede werkzaamheden. • Weinig mogelijkheden om uitbesteding direct te beëindigen en zelfstandig, of elders, voort te zetten. • Enigszins verouderd contractenregister. • Indien de uitvoerende organisatie voor meer dan één opdrachtgever werkt: onvoldoende logische scheiding gegevens en bestanden van verschillende opdrachtgevers. • Ontoereikende klachtenprocedure. • SLA voorziet in beperkte mogelijkheden voor de uitbestedende instelling om de kwaliteit en beheersing bij de leverancier te monitoren. Risicomonitoring • Managementinformatie over uitbestede werkzaamheden is ontoereikend. • Bijsturing op basis van de resultaten laat te wensen over. • Interne accountantsdienst van de instelling voert op ad-hocbasis audits uit bij de partij waaraan wordt uitbesteed. • Management laat zich op ad-hocbasis informeren over belangrijke risico's en de beheersing daarvan rondom uitbestede processen. • Naast rapportages met de gebruikelijke informatie over uitbestede werkzaamheden wordt op ad-hocbasis ook gerapporteerd over klachten, incidenten en uitzonderingen. • De instelling evalueert haar tevredenheid met de bestaande vormen van uitbesteding nauwelijks.	Administratieve organisatie en interne controle • Geen gebruik van adequate en strikte criteria bij het selecteren van een partner. • Vrijwel geen betrokkenheid van het topmanagement bij besluit tot uitbesteding van kritische processen. • Geen vastlegging van dan wel geen afspraken gemaakt over kwaliteitsnormen inzake uitbestede werkzaamheden. • Geen mogelijkheid om uitbesteding direct te beëindigen en zelfstandig, of elders, voort te zetten. • Verouderd contractenregister. • Indien de uitvoerende organisatie voor meer dan één opdrachtgever werkt: geen logische scheiding gegevens en bestanden van verschillende opdrachtgevers • Geen klachtenprocedure. • SLA voorziet nauwelijks in mogelijkheden voor de uitbestedende instelling om de kwaliteit en beheersing bij de leverancier te monitoren. risicomonitoring • Geen managementinformatie over uitbestede werkzaamheden. • Geen bijsturing op basis van de resultaten. • Interne accountantsdienst van de instelling voert geen audits uit bij de partij waaraan wordt uitbesteed. • Management besteedt nauwelijks aandacht aan informatie over belangrijke risico's en de beheersing daarvan rondom uitbestede processen. • Naast rapportages met de gebruikelijke informatie over uitbestede werkzaamheden wordt verder niet gerapporteerd over klachten, incidenten en uitzonderingen. • De instelling evalueert haar tevredenheid met de bestaande vormen van uitbesteding niet.

D8: RISICOCATEGORIE: IT-RISICO

Beoordeel de risicomitigerende werking van de aanwezige specifieke beheersmaatregelen voor de risicocategorie. Kies de score die het beste de kwaliteit van de bestaande risicospecifieke beheersmaatregelen weergeeft. Hierbij hoeft niet steeds aan alle geformuleerde criteria voldaan te worden. Het is aan de toezichthouder om te beoordelen welke criteria de doorslag geven bij de toekenning van een score.

Generieke indeling van de beheersmaatregelen:
- risico-identificatie;
- risicobeleid;
- administratieve organisatie en interne controle;
- risicomonitoring.

Definities van de generieke indeling van de beheersmaatregelen

Risico-identificatie
De mate waarin en de wijze waarop de instelling de specifieke risicocategorie zelfstandig reeds in beeld heeft gebracht, onder andere op basis van risico-inventarisatie en risicoanalyse.

Risicobeleid
De kwaliteit van het vastgelegde beleid over de mate waarin (risk appetite) en de wijze waarop (hoofdlijnen te implementeren beheersingsmaatregelen) men de betreffende risicocategorie wenst te beheersen.

Administratieve organisatie en interne controle
De mate waarin en de wijze waarop procedures, functiescheidingen, bevoegdheden, limieten, andere preventieve maatregelen en overige maatregelen zijn geïmplementeerd teneinde de risicocategorie te beheersen en daarmee uitvoering te geven aan het bijbehorende risicobeleid.

Risicomonitoring
De mate waarin en de wijze waarop wordt toegezien (en bijgestuurd) op het specifieke risico en de getroffen beheersingsmaatregelen, bijvoorbeeld door middel van performancerapportages, incident- of uitzonderingenrapportages en analyses.

Beoordelingscriteria voor risicospecifieke beheersing

1. Sterke beheersing	*2. Voldoende beheersing*
Risico-identificatie • Periodiek in kaart brengen van alle relevante IT-risico's op instellingsniveau, platformniveau, op niveau van sleutel applicaties, op procesniveau en productniveau (i.e. periodieke IT-risicoanalyse). • Nieuwe producten, initiatieven, projecten worden voor-afgegaan door een gedegen analyse van gerelateerde IT-risico's. • Management en betrokkenen van alle relevante niveaus en competenties (zowel IT-als business) betrokken bij risico-identificatie. • Risico-identificatie transparant gedocumenteerd. • Risico-identificatie gebaseerd op systematische aanpak. • Risico-identificatie vertaald in adequate prioriteitenstelling.	Risico-identificatie • Periodiek in kaart brengen van relevante IT-risico's op instellingsniveau. • Belangrijke nieuwe producten, initiatieven, projecten worden voorafgegaan door een analyse op hoofdlijnen van gerelateerde IT-risico's. • Management en overige medewerkers in voldoende mate betrokken bij risico-identificatie. • Risico-identificatie acceptabel gedocumenteerd. • Risico-identificatie meestal gebaseerd op systematische aanpak. • Risico-identificatie vertaald in redelijke prioriteitenstelling.
Risicobeleid • Instelling heeft top down informatiebeleid geformuleerd resulterende in: een beoogde c.q. gewenste informatie-architectuur, een informatieplan en het automatiseringsbeleid. • Het informatiebeleid is in lijn met de businessstrategie. • Deugdelijk beveiligingsbeleid conform algemeen erkende standaarden dat actief door de organisatie wordt gehanteerd. • IT-beleidsdocumenten worden vastgesteld door hoogste leiding. • Kwaliteit van de IT-beleidsdocumenten (volledigheid, documentatieniveau, kwaliteit van de inhoud, diepgang, actualiteit) is sterk. • Beleid ten aanzien van continuïteit en uitwijk uitgebreid geformuleerd en zichtbaar geïmplementeerd. • IT-beleidsdocumenten geven aan in welke mate risico's beheerst dienen te worden (mate van risk appetite). • Alle beveiligingseisen, inclusief de noodzaak voor uitwijk-voorzieningen, worden onderkend tijdens het specificeren van de eisen voor een project en worden goedgekeurd en gedocumenteerd als onderdeel van de algehele zakelijke verantwoording van het systeem. • Systemen zijn ingericht conform intern gehanteerde baselines.	Risicobeleid • Deugdelijk beveiligingsbeleid conform algemeen erkende standaarden dat actief door de organisatie wordt gehanteerd. • Beleid, voorzover niet passend binnen de door de hoogste leiding vastgestelde kaders, wordt ter goedkeuring voorgelegd aan de hoogste leiding. • Kwaliteit van de IT-beleidsdocumenten (volledigheid, documentatieniveau, kwaliteit van de inhoud, diepgang, actualiteit) is bevredigend. • Het informatiebeleid is voldoende in lijn met de strategie. • Op beleidsniveau voldoende aandacht voor continuïteit en uitwijk. • IT-beleidsdocumenten geven aan of risico's beheerst dienen te worden (mate van risk appetite).

1. Sterke beheersing (vervolg)

Administratieve organisatie en interne controle

Organisatie

- De IT Goverance structuur is duidelijk gedefinieerd en vastgelegd en sluit aan op de algemeen erkende standaarden.
- Een security-managementproces is aanwezig en gericht op het voldoen aan in- en externe beveiligingseisen en het realiseren van een hoog basisniveau aan beveiliging (conform algemeen aanvaarde standaarden).
- Een uitgebreid managementkader is vastgesteld om de implementatie van informatiebeveiliging in de organisatie te beheersen
- Taken en verantwoordelijkheden binnen de IT-organisatie zijn duidelijk en toereikend belegd, rekeninghoudend met de gewenste functiescheidingen.

Beveiliging

- Alle belangrijke informatiebedrijfsmiddelen zijn verantwoord en aan een 'eigenaar' toegewezen.
- IT-voorzieningen die kritieke of gevoelige zakelijke activiteiten ondersteunen zijn fysiek ondergebracht in beveiligde ruimten in een streng gecontroleerde omgeving, uitgebreid beveiligd met fysieke barrières en met toegangsbeveiliging.
- Verantwoordelijkheden en procedures zijn vastgesteld voor onderhoud (inclusief patch management) het beheer en de bediening van alle IT-voorzieningen. Voor deze taken is uitgebreide, makkelijk toegankelijke en actuele documentatie voorhanden.
- De toegang tot informatie, netwerken en bedrijfsprocessen wordt beheerst op grond van zakelijke behoeften en beveiligingseisen.
- Het continuïteitsmanagement bevat uitgebreide maatregelen voor het vaststellen en verminderen van risico's, het beperken van de gevolgen van incidenten die schade toebrengen en het tijdig hervatten van essentiële werkzaamheden (onder andere back-up, recovery, uitwijk, redundantie, et cetera).

Beheerprocessen

- Incident management is zodanig ingericht dat gewaarborgd wordt dat de dienstverlening zo snel mogelijk wordt hersteld met zo min mogelijk gevolgen voor de zakelijke activiteiten.
- Uitgebreid problem-managementproces gericht op: het opsporen en documenteren van fouten, het documenteren van symptomen en tijdelijke oplossingen, het voorkomen van nieuwe incidenten en het rapporteren over de kwaliteit van de IT-infrastructuur en het proces.
- Het configuratiemanagementproces leidt tot een betrouwbare rapportage en registratie van gegevens over de productiemiddelen en de diensten van de IT-organisatie.
- Het change-managementproces is zodanig ingericht dat alle wijzigingen op een gecontroleerde wijze worden uitgewerkt en doorgevoerd.
- Een service level managementproces is ingericht waarbij concrete afspraken zijn gemaakt tussen de IT-afdeling en haar klanten over het monitoren van en het rapporteren omtrent de prestaties van de IT-organisatie.
- Een capacity-managementproces is ingericht teneinde tijdig de juiste capaciteit aan IT-middelen te anticiperen en beschikbaar te stellen passend bij de huidige en toekomstige behoeften van de business.

2. Voldoende beheersing (vervolg)

Administratieve organisatie en interne controle

Organisatie

- De IT Goverance structuur is duidelijk gedefinieerd en vastgelegd en sluit aan op de algemeen erkende standaarden.
- Een security-managementproces is aanwezig en gericht op het voldoen aan in- en externe beveiligingseisen en het realiseren van een zeker basisniveau aan beveiliging (conform algemeen aanvaarde standaarden).
- Een toereikend managementkader is vastgesteld om de implementatie van informatiebeveiliging in de organisatie te beheersen.
- Taken en verantwoordelijkheden binnen de IT-organisatie zijn duidelijk en toereikend belegd, rekeninghoudend met de gewenste functiescheidingen.

Beveiliging

- Alle belangrijke informatiebedrijfsmiddelen zijn verantwoord en aan een 'eigenaar' toegewezen.
- IT-voorzieningen die kritieke of gevoelige zakelijke activiteiten ondersteunen zijn fysiek ondergebracht in beveiligde ruimten.
- Verantwoordelijkheden en procedures zijn vastgesteld voor onderhoud, het beheer en de bediening van alle IT-voorzieningen. Toereikende documentatie is voorhanden en redelijk toegankelijk.
- De toegang tot informatie, netwerken en bedrijfsprocessen wordt beheerst op grond van zakelijke behoeften en beveiligingseisen
- Het continuïteitsmanagement bevat voldoende maatregelen voor het vaststellen en verminderen van risico's, het beperken van de gevolgen van incidenten die schade toebrengen en het tijdig hervatten van essentiële werkzaamheden (onder andere back-up, recovery, uitwijk, redundantie, et cetera).

Beheerprocessen

- Problem- en incidentprocessen zijn toereikend opgezet
- Het change-managementproces is zodanig ingericht dat alle wijzigingen op een gecontroleerde wijze worden uitgewerkt en doorgevoerd.
- Het configuratiemanagementproces leidt tot een betrouwbare rapportage en registratie van gegevens over de productie-middelen en de diensten van de IT-organisatie.

1. Sterke beheersing (vervolg)	*2. Voldoende beheersing (vervolg)*
Systeem- c.q. applicatiegebonden criteria • Geprogrammeerde controles ondersteunen de in de betreffende bedrijfsprocessen benodigde interne controle-maatregelen in hoge mate (hier zit bijvoorbeeld ook het vierogenprincipe, limieten, autorisaties door anderen et cetera in). • Geprogrammeerde controles en infrastructurele maatregelen (bijvoorbeeld gebruik RDBMS in plaats van flatfiles) die de integriteit (juistheid, volledigheid) en tijdigheid van de invoer, geautomatiseerde verwerking en uitvoer waarborgen zijn in hoge mate aanwezig. • De juiste werking van de geprogrammeerde controles is eenvoudig te toetsen aan de hand van uitzonderingsverslagen (rapportages). • Applicaties en systemen bieden uitgebreide functionaliteit voor de beheersing van gebruikersrechten en analyse van gebruikershandelingen.	**Systeem- c.q. applicatiegebonden criteria** • Geprogrammeerde controles ondersteunen de in de betreffende bedrijfsprocessen benodigde interne controle-maatregelen in voldoende mate. • Geprogrammeerde controles en infrastructurele maatregelen (bijvoorbeeld gebruik RDBMS in plaats van flatfiles) die de integriteit (juistheid, volledigheid) en tijdigheid van de invoer, geautomatiseerde verwerking en uitvoer waarborgen zijn in toereikende mate aanwezig. • Applicaties en systemen bieden basisfunctionaliteit voor de beheersing van gebruikersrechten en analyse van gebruikers-handelingen.
<u>Risicomonitoring</u> • Heldere rapportages over IT-activiteiten, performance en verstoringen in de dienstverlening (kengetallen en gedegen toelichting). • Management laat zich periodiek informeren over status van risico's, kwaliteit van beheersing en status van verbeteracties. • Naast rapportages over de gebruikelijke IT-werkzaamheden wordt standaard ook frequent gerapporteerd over klachten, incidenten en uitzonderingen. • Continue monitoring van netwerken en systemen. • Snelle bijsturing op basis van de resultaten van deze monitoring • Proactieve inschakeling van IT-audit door het IT-management (IT-audit als tool of management) incombinatie met strikt geplande en uitgevoerde IT-audits. • Aanwezigheid van tools en specifieke programmatuur ter ondersteuning van de frequente monitoring en analyse van logbestanden. • Compliance aan in- en externe regelgeving op het gebied van IT wordt periodiek vastgesteld.	<u>Risicomonitoring</u> • Management laat zich met voldoende regelmaat op hoofd-lijnen informeren over risico's en de beheersing daarvan. • Naast rapportages over de gebruikelijke IT-werkzaamheden wordt ook gerapporteerd over klachten, incidenten en uitzonderingen. • Voldoende monitoring van netwerken en systemen. • Tijdige bijsturing op basis van de resultaten van deze monitoring. • Managementinformatie over IT-activiteiten is van acceptabel niveau. • Aanwezigheid van tools en specifieke programmatuur ter ondersteuning van de frequente monitoring en analyse van kritische logbestanden • Compliance aan in- en externe regelgeving op het gebied van IT wordt regelmatig vastgesteld. • Strikt geplande en uitgevoerde IT-audits

3. Onvoldoende beheersing	*4. Zwakke beheersing*
Risico-identificatie • Incidenteel in kaart brengen van IT-risico's op instellingsniveau. • Belangrijke nieuwe producten, initiatieven, projecten worden veelal pas achteraf op hoofdlijnen geanalyseerd op gerelateerde IT-risico's. • Onvoldoende betrokkenheid van management en medewerkers bij risico-identificatie. • Risico-identificatie slecht gedocumenteerd. • Risico-identificatie in onvoldoende mate gebaseerd op systematische aanpak. • Risico-identificatie onvoldoende vertaald in prioriteiten-stelling.	Risico-identificatie • Niet in kaart brengen van IT-risico's. • Belangrijke nieuwe producten, initiatieven, projecten worden niet geanalyseerd op gerelateerde IT-risico's. • Nauwelijks betrokkenheid van management en medewerkers bij risico-identificatie. • Risico-identificatie niet gedocumenteerd. • Risico-identificatie niet gebaseerd op systematische aanpak. • Risico-identificatie niet vertaald in prioriteitenstelling.
Risicobeleid • Kwaliteit van beleid (volledigheid, documentatieniveau, kwaliteit van de inhoud, diepgang, actualiteit) is onbevredigend. • Beleid, voorzover niet passend binnen de door de hoogste leiding vastgestelde kaders, wordt geregeld niet ter goedkeuring voorgelegd aan de hoogste leiding. • De IT-beleidsdocumenten zijn onvoldoende in lijn met de strategie. • De IT-beleidsdocumenten zijn onvoldoende afgestemd op risico's die als belangrijk zijn aangemerkt. • De IT-beleidsdocumenten geven onvoldoende aan of risico's beheerst dienen te worden (mate van risk appetite). • Op beleidsniveau nauwelijks aandacht voor continuïteit en uitwijk	Risicobeleid • Kwaliteit van beleid (volledigheid, documentatieniveau, kwaliteit van de inhoud, diepgang, actualiteit) is onduidelijk of slecht. • Beleid, voorzover niet passend binnen de door de hoogste leiding vastgestelde kaders, wordt niet ter goedkeuring voor-gelegd aan de hoogste leiding. • De IT-beleidsdocumenten zijn erg gebrekkig en onvoldoende in lijn met de strategie. • De IT-beleidsdocumenten zijn niet afgestemd op risico's die als belangrijk zijn aangemerkt. • De IT-beleidsdocumenten geven niet aan of risico's beheerst dienen te worden (mate van risk appetite). • Op beleidsniveau geen aandacht voor continuïteit en uitwijk.
Administratieve organisatie en interne controle **Organisatie** • De IT Goverance structuur is slechts op hoofdlijnen gedefinieerd en niet vastgelegd • Een formeel security-managementproces is afwezig. Taken en verantwoordelijkheden zijn informeel wel belegd. • Een managementkader voor de implementatie en beheersing van informatiebeveiliging in de organisatie is afwezig. Taken en verantwoordelijkheden zijn informeel wel belegd. • Taken en verantwoordelijkheden binnen de IT-organisatie zijn onduidelijk en niet geheel toereikend belegd. Essentiële functiescheidingen kunnen worden doorbroken. **Beveiliging** • Belangrijke informatiebedrijfsmiddelen zijn verantwoord maar niet aan een 'eigenaar' toegewezen. • IT-voorzieningen die kritieke of gevoelige zakelijke activiteiten ondersteunen zijn fysiek ondergebracht in zwak beveiligde ruimten. • Zeer beperkte documentatie aangaande beheer en gebruik van sytemen is aanwezig. • De toegang tot informatie, netwerken en bedrijfsprocessen wordt niet alleen beheerst op grond van zakelijke behoeften en beveiligingseisen. Functiescheidingen kunnen worden door-broken. • Het continuïteitsmanagement bevat ontoereikende maat-regelen voor het vaststellen en verminderen van risico's, het beperken van de gevolgen van incidenten die schade toebrengen en het tijdig hervatten van essentiële werkzaam-heden (onder andere back-up, recovery, uitwijk, redundantie, et cetera).	administratieve organisatie en interne controle **Organisatie** • Geen formele IT Governance structuur. • Geen security-managementproces ingericht. • Geen beveiligingsorganisatie opgezet. • Taken en verantwoordelijkheden zijn niet duidelijk toegewezen en belegd en/of essentiële functiescheidingen worden doorbroken. **Beveiliging** • Bruikbaar inzicht in aanwezigheid en gebruik van informatie-bedrijfsmiddelen ontbreekt. • IT-voorzieningen die kritieke of gevoelige zakelijke activiteiten ondersteunen zijn ondergebracht in niet-beveiligde en/of publiek toegankelijke ruimten. • Geen of volstrekt ontoereikende documentatie aanwezig. • Toegang tot informatie, netwerken en bedrijfsprocessen lijkt te berusten op willekeur. Functiescheidingen worden door-broken. • Geen of volstrekt ontoereikende aandacht voor beschikbaar-heids- en/of continuïteitsmaatregelen.

3. Onvoldoende beheersing (vervolg)	*4. Zwakke beheersing (vervolg)*
Beheerprocessen • Incident management is versnipperd ingericht en geen gecoördineerd problem-managementproces • Het configuratiemanagementproces is informeel en leidt tot een onbetrouwbare rapportage en registratie van gegevens over de productiemiddelen en de diensten van de IT-organisatie (onvolledig, niet juist en niet tijdig). • Het change-managementproces bevat lacunes waardoor wijzigingen buiten het proces om kunnen worden door-gevoerd.	**Beheerprocessen** • Geen problem- en incident-managementprocessen ingericht- • Geen configuratiemanagementproces. • Geen change-managementproces dan wel het change-managementproces kan en wordt regelmatig gepasseerd.
Systeem- c.q. applicatiegebonden criteria • Geprogrammeerde controles ondersteunen de in de betreffende bedrijfsprocessen benodigde interne controlemaatregelen in te beperkte mate. • Geprogrammeerde controles en infrastructurele maatregelen die de integriteit (juistheid, volledigheid) en tijdigheid van de invoer, geautomatiseerde verwerking en uitvoer waarborgen zijn in te beperkte mate aanwezig. • De juiste werking van de geprogrammeerde controles is niet te toetsen. • Applicaties en systemen bieden te beperkte functionaliteit voor de beheersing van gebruikersrechten en analyse van gebruikershandelingen.	**Systeem- c.q. applicatiegebonden criteria** • Geprogrammeerde controles ondersteunen de in de betreffende bedrijfsprocessen benodigde interne controle-maatregelen in het geheel niet. Controles zijn eenvoudig te omzeilen en worden niet gecompenseerd met handmatige controles. • In de verwerkingsprocessen is geen enkele integriteits-waarborg opgenomen. • Applicaties bieden geen functionaliteit ten behoeve van security management en/of de analyse van gebruikers-handelingen.
<u>Risicomonitoring</u> • Managementinformatie over IT-activiteiten is ontoereikend. • Management laat zich op ad-hocbasis informeren over belangrijke risico's en de beheersing daarvan. • Naast rapportages over de gebruikelijke IT-werkzaamheden wordt op ad-hocbasis ook gerapporteerd over klachten, incidenten en uitzonderingen. • Onvoldoende monitoring van netwerken en systemen. • Bijsturing op basis van de resultaten van de monitoring laat te wensen over. • Nauwelijks monitoring en analyse van logbestanden. • IT-audit op ad-hocbasis zonder risicogebaseerde onderbouwing. • Compliance aan in- en externe regelgeving wordt op ad-hocbasis vastgesteld	<u>Risicomonitoring</u> • Geen managementinformatie over IT-activiteiten. • Management besteedt nauwelijks aandacht aan informatie over belangrijke risico's en de beheersing daarvan. • Naast rapportages over de gebruikelijke IT-werkzaamheden wordt verder niet gerapporteerd over klachten, incidenten en uitzonderingen. • Geen monitoring van netwerken en systemen. • Geen bijsturing op basis van de resultaten. • Geen monitoring en analyse van logbestanden. • Geen IT-audits. • Compliance aan in- en externe regelgeving wordt niet vastgesteld.

D9: RISICOCATEGORIE: INTEGRITEITSRISICO

Beoordeel de risicomitigerende werking van de aanwezige risicospecifieke beheersing voor de risicocategorie integriteitsrisico. Kies de score die het beste de kwaliteit van de bestaande risicospecifieke beheersmaatregelen weergeeft. Hierbij hoeft niet steeds aan alle geformuleerde criteria voldaan te worden. Het is aan de toezichthouder om te beoordelen welke criteria de doorslag geven bij de toekenning van een score.

Generieke indeling van de beheersmaatregelen:
- risico-identificatie;
- risicobeleid;
- administratieve organisatie en interne controle;
- risicomonitoring.

Definities van de generieke indeling van de beheersmaatregelen

Risico-identificatie
De mate waarin en de wijze waarop de instelling de specifieke risicocategorie zelfstandig reeds in beeld heeft gebracht, onder andere op basis van risico-inventarisatie en risicoanalyse.

Risicobeleid
De kwaliteit van het vastgelegde beleid over de mate waarin (risk appetite) en de wijze waarop (hoofdlijnen te implementeren beheersing) men de betreffende risicocategorie wenst te beheersen.

Administratieve organisatie en interne controle
De mate waarin en de wijze waarop procedures, functiescheidingen, bevoegdheden, limieten en andere preventieve maatregelen of overige maatregelen zijn geïmplementeerd teneinde de risicocategorie te beheersen en daarmee uitvoering te geven aan het bijbehorende risicobeleid.

Risicomonitoring
De mate waarin en de wijze waarop wordt toegezien (en bijgestuurd) op het specifieke risico en de getroffen beheersingsmaatregelen, bijvoorbeeld door middel van performancerapportages, incident- of uitzonderingenrapportages en analyses.

Beoordelingscriteria voor risicospecifieke beheersing

1. Sterke beheersing	*2. Voldoende beheersing*
Risico-identificatie • Frequent in kaart brengen van relevante integriteitsrisico's per organisatieonderdeel, op procesniveau, per productsoort, per klantgroep en per distributiekanaal. • Sterk gemotiveerde, zeer expliciete en zeer transparante indeling van productsoorten, klantgroepen en distributiekanalen naar risicogroepen. • Nieuwe producten, initiatieven, projecten worden voor-afgegaan door een gedegen analyse van gerelateerde integriteitsrisico's. • Management en betrokkenen van alle relevante niveaus en competenties betrokken bij risicoidentificatie. Volledig begrip van alle aspecten van integriteitsrisico door verantwoordelijke staf. • Risico-identificatie transparant gedocumenteerd. • Risico-identificatie gebaseerd op systematische aanpak. • Risico-identificatie vertaald in adequate prioriteitenstelling.	Risico-identificatie • Periodiek in kaart brengen van relevante integriteitsrisico's op instellingsniveau. • Gemotiveerde, expliciete en transparante indeling van productsoorten, klantgroepen en distributiekanalen naar risicogroepen. • Belangrijke nieuwe producten, initiatieven, projecten worden voorafgegaan door een analyse op hoofdlijnen van gerelateerde integriteitsrisico's. • Management en overige medewerkers in voldoende mate betrokken bij risico identificatie. Voldoende begrip van alle aspecten van integriteitsrisico door verantwoordelijke staf. • Risico-identificatie acceptabel gedocumenteerd. • Risico-identificatie meestal gebaseerd op systematische aanpak. • Risico-identificatie vertaald in redelijke prioriteitenstelling.

Risicobeleid
• Risicobeleid goed afgestemd op geïdentificeerde risico's die als belangrijk zijn aangemerkt.
• Risicobeleid geeft aan in welke mate risico's beheerst dienen te worden.
• Integriteitsaspecten goed doorvertaald naar acceptatiebeleid.
• De instelling heeft zeer duidelijk en inhoudelijk zeer deugdelijk beleid opgesteld rondom het ´ken uw klant´ principe (CDD). Een en ander expliciet vastgesteld door de hoogste leiding en adequaat gecommuniceerd binnen de organisatie. Alles conform de betreffende regeling van DNB.
• Ruime aandacht voor integriteitsaspecten in personeelsbeleid.
• Deugdelijk Compliance charter opgesteld en geaccordeerd door hoogste leiding. Wijzigingen in beleid/omstandigheden worden terstond verwerkt in het Compliance charter.
• Beleid vastgesteld door hoogste leiding.
• Kwaliteit van beleid (volledigheid, documentatieniveau, kwaliteit van de inhoud, diepgang) is sterk.
• Zeer duidelijk en goed uitgewerkt beleid rondom:
  • verstrekking van bestuurderskredieten,
  • behandeling van afgeschermde rekeningen
  • omgaan met incidenten in het kader van integere bedrijfsvoering
  • omgaan met integriteitsgevoelige functies
Een en ander expliciet vastgesteld door de hoogste leiding en adequaat gecommuniceerd binnen de organisatie. Alles conform de betreffende regeling van DNB.
	Risicobeleid
	• Risicobeleid redelijk afgestemd op geïdentificeerde risico's die als belangrijk zijn aangemerkt.
	• Risicobeleid geeft aan of risico's beheerst dienen te worden.
	• Integriteitsaspecten voldoende doorvertaald naar acceptatie-beleid.
	• De instelling heeft duidelijk en inhoudelijk deugdelijk beleid opgesteld rondom het ´ken uw klant´ principe (CDD). Een en ander vastgesteld door de hoogste leiding en in voldoende mate gecommuniceerd binnen de organisatie. Alles conform de betreffende regeling van DNB.
	• Aandacht voor integriteitsaspecten in personeelsbeleid.
	• Deugdelijk Compliance charter opgesteld en geaccordeerd door hoogste leiding.
	• Beleid, voorzover niet passend binnen de door de hoogste leiding vastgestelde kaders, wordt ter goedkeuring voorgelegd aan de hoogste leiding.
	• Kwaliteit van beleid (volledigheid, documentatieniveau, kwaliteit van de inhoud, diepgang) is bevredigend.
	• Duidelijk en voldoende uitgewerkt beleid rondom:
	  • verstrekking van bestuurderskredieten,
	  • behandeling van afgeschermde rekeningen
	  • omgaan met incidenten in het kader van integere bedrijfsvoering
	  • omgaan met integriteitsgevoelige functies
	Een en ander expliciet vastgesteld door de hoogste leiding en voldoende gecommuniceerd binnen de organisatie. Alles in voldoende mate conform de betreffende regeling van DNB.

1. Sterke beheersing (vervolg)	*2. Voldoende beheersing (vervolg)*
Administratieve organisatie en interne controle • Procedures voor goedkeuring van nieuwe cliënten, producten en activiteiten kennen ruimschoots aandacht voor integriteits-aspecten. • Taken, verantwoordelijkheden en bevoegdheden zijn helder en adequaat. • Duidelijke en breed gecommuniceerde gedragscode beschikbaar, waarin ruim voldoende aandacht is voor risico´s in verband met bijvoorbeeld belangenverstrengeling en moraliteit. • Adequate functiescheidingen en toepassing van vierogen-principes doorgevoerd bij beleggingsprocessen. • Actief toepassen van functieroulatie. • Zorgvuldige screening van tussenpersonen en cliënten. • Beleidsuitgangspunten met betrekking tot integriteitsgevoelige functies zijn vastgelegd en omgeven door administratief-organisatorische maatregelen. • Gedegen screening van nieuw personeel op integriteits-gevoelige functies • Sterke controle op geldstromen. • Veel aandacht voor integriteits- en compliance-bewustzijn (onder andere via goed trainingsmaterieel en trainingen). • Compliancefuncties op een zeer hoog niveau en onafhankelijk belegd in de organisatie. • Getekende insiderregelingen inclusief voorlichting. • Adequate klachtenprocedure. • Onafhankelijke klokkenluidersregeling • Regelingen ‘bestuurderskredieten’ en ‘afgeschermde rekeningen’ volledig geïmplementeerd binnen de organisatie. • Regelingen ‘incidenten’ volledig geïmplementeerd binnen de organisatie. Goede vastlegging van incidenten die zich voordoen, duidelijke normen ten aanzien hoe te handelen bij incidenten alsmede wanneer en hoe te melden aan de toezichthouder. • Regeling ‘integriteitsgevoelige functies’ volledig geïmplementeerd binnen de organisatie. Er zijn objectieve en transparante criteria benoemd voor het onderkennen van integriteitsgevoelige functies. Medewerkers die in aanmerking komen voor integriteitsgevoelige functies worden systematisch op betrouwbaarheid beoordeeld.	Administratieve organisatie en interne controle • Procedures voor goedkeuring van nieuwe cliënten, producten en activiteiten kennen aandacht voor integriteitsaspecten. • Taken, verantwoordelijkheden en bevoegdheden zijn over het algemeen duidelijk en toereikend. • Beschikbare gedragscode is voldoende gecommuniceerd, en heeft voldoende aandacht voor risico´s in verband met bijvoorbeeld belangenverstrengeling en moraliteit. • Voldoende functiescheiding aanwezig bij beleggings-processen. • Voldoende bewerkstelligen van functieroulatie. • Redelijk zorgvuldige screening van tussenpersonen en cliënten. • Integriteitsgevoelige functies onderkend en gedocumenteerd. • Screening van nieuw personeel op integriteitsgevoelige functies. • Voldoende controle op geldstromen. • Aandacht voor integriteits- en compliancebewustzijn (onder andere via trainingsmaterieel en trainingen). • Compliancefunctie op een voldoende hoog niveau en voldoende onafhankelijk in de organisatie belegd. • Veel getekende insiderregelingen inclusief voorlichting. • Acceptabele klachtenprocedure. • Klokkenluidersregeling. • Regelingen ‘bestuurderskredieten’ en ‘afgeschermde rekeningen’ in voldoende mate geïmplementeerd binnen de organisatie. • Regelingen ‘incidenten’ in voldoende mate geïmplementeerd binnen de organisatie. Vastlegging van incidenten die zich voordoen, normen ten aanzien hoe te handelen bij incidenten alsmede wanneer en hoe te melden aan de toezichthouder. • Regeling ‘integriteitsgevoelige functies’ voldoende geïmplementeerd binnen de organisatie. Er zijn min of meer objectieve en transparante criteria benoemd voor het onderkennen van integriteitsgevoelige functies. Medewerkers die in aanmerking komen voor integriteitsgevoelige functies worden op betrouwbaarheid beoordeeld.
Risicomonitoring • Heldere en inzichtelijke rapportages. • Management laat zich periodiek informeren over status van risico’s, kwaliteit van beheersing en status van verbeteracties. • Naast rapportages over de aan integriteitsrisico gerelateerde gebruikelijke werkzaamheden wordt standaard ook frequent gerapporteerd over klachten, incidenten en uitzonderingen. • Frequent uitvoeren van compliance of integriteitsaudits (door compliancefunctie en door internal audit). • Zeer frequent en zeer effectief intern toezicht op naleving van integriteitsbeleid door b.v. de compliance-functie. • Zeer sterke monitoring op transacties en rekeningen van cliënten ter identificatie van mogelijke integriteitsgevoeligheden. • Integriteitsgerelateerde incidenten worden zeer adequaat en actiegericht opgevolgd en leiden waar nodig altijd tot bijstelling van beleid.	Risicomonitoring • Duidelijke rapportages. • Management laat zich met voldoende regelmaat op hoofd-lijnen informeren over status van risico’s, kwaliteit van beheersing en status van verbeteracties. • Naast rapportages over de aan integriteitsrisico gerelateerde gebruikelijke werkzaamheden wordt ook gerapporteerd over klachten, incidenten en uitzonderingen. • Periodiek uitvoeren van compliance of integriteitsaudits (door compliance functie en door internal audit). • Frequent en effectief intern toezicht op naleving van integriteitsbeleid door b.v. de compliance-functie. • Voldoende monitoring op transacties en rekeningen van cliënten ter identificatie van mogelijke integriteitsgevoeligheden. •

3. Onvoldoende beheersing

Risico-identificatie

- Incidenteel in kaart brengen van integriteitsrisico's op instellingsniveau.
- Nauwelijks indeling van productsoorten, klantgroepen en distributiekanalen naar risicogroepen.
- Belangrijke nieuwe producten, initiatieven, projecten worden veelal pas achteraf op hoofdlijnen geanalyseerd op gerelateerde integriteitsrisico's.
- Onvoldoende betrokkenheid van management en medewerkers bij risico-identificatie. Onvoldoende begrip van alle aspecten van integriteitsrisico door verantwoordelijke staf.
- Risico-identificatie slecht gedocumenteerd.
- Risico-identificatie in onvoldoende mate gebaseerd op systematische aanpak.
- Risico-identificatie onvoldoende vertaald in prioriteiten-stelling.

Risicobeleid

- Risicobeleid onvoldoende afgestemd op geïdentificeerde risico's die als belangrijk zijn aangemerkt.
- Risicobeleid geeft onvoldoende aan of risico's beheerst dienen te worden.
- Integriteitsaspecten onvoldoende doorvertaald naar acceptatie-beleid.
- De instelling heeft onvoldoende duidelijk en inhoudelijk onvoldoende deugdelijk beleid opgesteld rondom het ´ken uw klant´ principe (CDD). Een en ander niet vastgesteld door de hoogste leiding en slechts in zeer bescheiden kring gecommuniceerd binnen de organisatie.
- In personeelsbeleid geringe aandacht voor integriteitsaspecten.
- Compliance charter aanwezig maar sterk verouderd.
- Beleid, voorzover niet passend binnen de door de hoogste leiding vastgestelde kaders, wordt geregeld niet ter goedkeuring voorgelegd aan de hoogste leiding.
- Kwaliteit van beleid (volledigheid, documentatieniveau, kwaliteit van de inhoud, diepgang) is onbevredigend.
- Mager uitgewerkt beleid rondom:
  - verstrekking van bestuurderskredieten,
  - behandeling van afgeschermde rekeningen
  - omgaan met incidenten in het kader van integere bedrijfsvoering
  - omgaan met integriteitsgevoelige functies

  Een en ander niet vastgesteld door de hoogste leiding en slechts in zeer bescheiden kring gecommuniceerd binnen de organisatie.

4. Zwakke beheersing

Risico-identificatie

- Niet in kaart brengen van integriteitsrisico's.
- Productsoorten, klantgroepen en distributiekanalen worden niet expliciet ingedeeld naar risicogroepen.
- Belangrijke nieuwe producten, initiatieven, projecten worden niet geanalyseerd op gerelateerde integriteitsrisico's.
- Nauwelijks betrokkenheid van management en medewerkers bij risico-identificatie. Nauwelijks begrip van alle aspecten van integriteitsrisico door verantwoordelijke staf.
- Risico-identificatie niet gedocumenteerd.
- Risico-identificatie niet gebaseerd op systematische aanpak.
- Risico-identificatie niet vertaald in prioriteitenstelling.

Risicobeleid

- Risicobeleid niet afgestemd op geïdentificeerde risico's die als belangrijk zijn aangemerkt.
- Risicobeleid geeft niet aan of risico's beheerst dienen te worden.
- Bij acceptatiebeleid geen rekening gehouden met integriteits-aspecten.
- De instelling heeft geen of sterk onvoldoende beleid opgesteld rondom het ´ken uw klant´ principe (CDD). Een en ander niet vastgesteld door de hoogste leiding en niet of nauwelijks gecommuniceerd binnen de organisatie.
- In personeelsbeleid nauwelijks aandacht voor integriteits-aspecten.
- Geen compliance charter aanwezig.
- Beleid, voorzover niet passend binnen de door de hoogste leiding vastgestelde kaders, wordt niet ter goedkeuring voorgelegd aan de hoogste leiding.
- Kwaliteit van beleid (volledigheid, documentatieniveau, kwaliteit van de inhoud, diepgang) is onduidelijk.
- Geen of slecht uitgewerkt beleid rondom:
  - verstrekking van bestuurderskredieten,
  - behandeling van afgeschermde rekeningen
  - omgaan met incidenten in het kader van integere bedrijfsvoering
  - omgaan met integriteitsgevoelige functies

  Een en ander niet vastgesteld door de hoogste leiding en niet of nauwelijks gecommuniceerd binnen de organisatie.

3. Onvoldoende beheersing (vervolg)	*4. Zwakke beheersing*
<u>Administratieve organisatie en interne controle</u> • Procedures voor goedkeuring van nieuwe cliënten, producten en activiteiten kennen onvoldoende aandacht voor integriteitsaspecten. • Taken, verantwoordelijkheden en bevoegdheden zijn veelal onduidelijk en ontoereikend. • Gedragscode niet duidelijk gecommuniceerd en heeft onvoldoende aandacht voor risico´s in verband met bijvoorbeeld belangenverstrengeling en moraliteit. • Onvoldoende functiescheiding aanwezig bij beleggings-processen. • Onvoldoende bewerkstelligen van functieroulatie. • Nauwelijks screening van tussenpersonen en cliënten. • Integriteitsgevoelige functies zijn onderkend. • Geen screening van nieuw personeel op integriteitsgevoelige functies. • Onvoldoende controle op geldstromen. • Weinig aandacht voor integriteits- en compliance bewustzijn. • Compliance functie niet op voldoende hoog niveau en onvoldoende onafhankelijk in de organisatie belegd. • Nauwelijks getekende insider regelingen inclusief voor-lichting. • Ontoereikende klachtenprocedure. • Geen klokkenluidersregeling. • Regelingen ‘bestuurderskredieten’ en ‘afgeschermde rekeningen’ onvoldoende geïmplementeerd binnen de organisatie. • Regelingen ‘incidenten’ onvoldoende geïmplementeerd binnen de organisatie. Beperkte vastlegging van incidenten die zich voordoen, vage normen ten aanzien hoe te handelen bij incidenten alsmede wanneer en hoe te melden aan de toezichthouder. • Regeling ‘integriteitsgevoelige functies’ onvoldoende geïmplementeerd binnen de organisatie. Er zijn nauwelijks objectieve en transparante criteria benoemd voor het onderkennen van integriteitsgevoelige functies. Medewerkers die in aanmerking komen voor integriteitsgevoelige functies worden niet systematisch op betrouwbaarheid beoordeeld.	<u>Administratieve organisatie en interne controle</u> • Procedures voor goedkeuring van nieuwe cliënten, producten en activiteiten kennen nauwelijks aandacht voor integriteitsaspecten. • Taken, verantwoordelijkheden en bevoegdheden zijn onduidelijk en ontoereikend. • Geen gedragscode. • Vrijwel geen functiescheiding aanwezig bij beleggings-processen. • Geen functieroulatie. • Geen of vrijwel geen screening van tussenpersonen en cliënten. • Integriteit gevoelige functies niet in kaart gebracht. • Nauwelijks tot geen controle op geldstromen. • Geen aandacht voor integriteits- en compliance bewustzijn. • Compliance functie niet op voldoende hoog niveau en in het geheel niet onafhankelijk in de organisatie belegd. • Nauwelijks tot geen getekende insider regelingen inclusief voorlichting. • Geen klachtenprocedure. • Regelingen ‘bestuurderskredieten’ en ‘afgeschermde rekeningen’ niet geïmplementeerd binnen de organisatie. • Regelingen ‘incidenten’ niet geïmplementeerd binnen de organisatie. Geen of geen gestructureerde vastlegging van incidenten die zich voordoen, nauwelijks of geen normen ten aanzien hoe te handelen bij incidenten alsmede wanneer en hoe te melden aan de toezichthouder. • Regeling ‘integriteitsgevoelige functies’ onvoldoende of niet geïmplementeerd binnen de organisatie. Er zijn geen objectieve en transparante criteria benoemd voor het onderkennen van integriteitsgevoelige functies. Medewerkers die in aanmerking komen voor integriteitsgevoelige functies worden niet op betrouwbaarheid beoordeeld.
<u>Risicomonitoring</u> • Rapportages niet inzichtelijk. • Management laat zich op ad-hocbasis informeren over status van risico’s, kwaliteit van beheersing en status van verbeter-acties. • Naast rapportages over de aan integriteitsrisico gerelateerde gebruikelijke werkzaamheden wordt op ad-hocbasis ook gerapporteerd over klachten, incidenten en uitzonderingen. • Op ad-hocbasis uitvoeren van compliance of integriteitsaudits (door compliancefunctie en door internal audit). • Weinig frequent en weinig effectief intern toezicht op naleving van integriteitsbeleid door b.v. de compliance-functie. • Onvoldoende monitoring op transacties en rekeningen van cliënten ter identificatie van mogelijke integriteitsgevoeligheden. • Integriteitsgerelateerde incidenten worden onvoldoende adequaat en niet actiegericht opgevolgd en leiden zelden tot bijstelling van beleid.	<u>Risicomonitoring</u> • Rapportages niet inzichtelijk en uitsluitend op ad-hocbasis. • Management besteedt nauwelijks aandacht aan informatie over belangrijke risico’s en de beheersing daarvan. • Naast rapportages over de aan integriteitsrisico gerelateerde gebruikelijke werkzaamheden wordt verder niet gerapporteerd over klachten, incidenten en uitzonderingen. • Niet uitvoeren van compliance of integriteitsaudits (door compliancefunctie en door internal audit). • Nauwelijks tot geen intern toezicht op naleving van integriteitsbeleid door b.v. de compliance-functie. • Geen monitoring op transacties en rekeningen van cliënten ter identificatie van mogelijke integriteitsgevoeligheden. • Integriteitsgerelateerde incidenten worden niet adequaat en niet actiegericht opgevolgd en leiden zelden tot bijstelling van beleid.

D10: RISICOCATEGORIE: JURIDISCH RISICO

Beoordeel de risicomitigerende werking van de aanwezige risicospecifieke beheersing voor de risicocategorie juridisch risico. Kies de score die het beste de kwaliteit van de bestaande risicospecifieke beheersmaatregelen weergeeft. Hierbij hoeft niet steeds aan alle geformuleerde criteria voldaan te worden. Het is aan de toezichthouder om te beoordelen welke criteria de doorslag geven bij de toekenning van een score.

Generieke indeling van de beheersmaatregelen:
- risico-identificatie;
- risicobeleid;
- administratieve organisatie en interne controle;
- risicomonitoring.

Definities van de generieke indeling van de beheersmaatregelen:

Risico-identificatie
De mate waarin en de wijze waarop de instelling de specifieke risicocategorie zelfstandig reeds in beeld heeft gebracht, onder andere op basis van risico-inventarisatie en risicoanalyse.

Risicobeleid
De kwaliteit van het vastgelegde beleid over de mate waarin (risk appetite) en de wijze waarop (hoofdlijnen te implementeren beheersing) men de betreffende risicocategorie wenst te beheersen.

Administratieve organisatie en interne controle
De mate waarin en de wijze waarop procedures, functiescheidingen, bevoegdheden, limieten en andere preventieve maatregelen of overige maatregelen zijn geïmplementeerd teneinde de risicocategorie te beheersen en daarmee uitvoering te geven aan het bijbehorende risicobeleid.

risicomonitoring
De mate waarin en de wijze waarop wordt toegezien (en bijgestuurd) op het specifieke risico en de getroffen beheersingsmaatregelen, bijvoorbeeld door middel van performancerapportages, incident- of uitzonderingenrapportages en analyses.

Opmerking:
Gezien de samenhang tussen juridische risico's en integriteitsrisico's dient de toezichthouder bij de beoordeling van de beheersing van de juridische risico's te overwegen of zijn inschatting in deze wellicht ook van invloed is op de hoogte van de integriteitsrisico's.

Beoordelingscriteria voor risicospecifieke beheersing

1. Sterke beheersing	*2. Voldoende beheersing*
Risico-identificatie • Frequent en gedetailleerd in kaart brengen van alle relevante juridische risico's en ontwikkelingen (zowel intern als extern) binnen juridische entiteiten alsmede de juridische risico's verbonden aan activiteiten, producten en contracten. • Nieuwe producten, initiatieven, projecten worden voorafgegaan door een gedegen analyse van gerelateerde juridische risico's. • Management en betrokkenen van alle relevante niveaus en competenties (ook buiten juridische zaken) betrokken bij risico-identificatie. Volledig begrip van alle aspecten van juridisch risico door verantwoordelijke staf en management. • Risico-identificatie transparant gedocumenteerd. • Risico-identificatie gebaseerd op systematische aanpak. • Risico-identificatie vertaald in adequate prioriteitenstelling. Risicobeleid • Risicobeleid goed afgestemd op geïdentificeerde risico's die als belangrijk zijn aangemerkt. • Risicobeleid geeft aan in welke mate juridische risico's beheerst dienen te worden. • Afdeling juridische zaken heeft haar taken en verantwoordelijkheden uitgebreid vastgelegd in een charter. • Beleid vastgesteld door hoogste leiding. • Kwaliteit van beleid (volledigheid, documentatieniveau, kwaliteit van de inhoud, diepgang) is sterk. • Afdeling juridische zaken adequaat gepositioneerd met goede toegang tot het topmanagement. • In beleid uitvoerig vastgelegd wanneer externe juridische ondersteuning moet worden ingeschakeld.	Risico-identificatie • Periodiek in kaart brengen van relevante juridische risico's en ontwikkelingen (zowel intern als extern) binnen juridische entiteiten alsmede de juridische risico's verbonden aan activiteiten, producten en contracten. • Belangrijke nieuwe producten, initiatieven, projecten worden voorafgegaan door een analyse op hoofdlijnen van gerelateerde juridische risico's. • Management en overige medewerkers in voldoende mate betrokken bij risico-identificatie. Voldoende begrip van alle aspecten van juridisch risico door verantwoordelijke staf en management. • Risico-identificatie acceptabel gedocumenteerd. • Risico-identificatie meestal gebaseerd op systematische aanpak. • Risico-identificatie vertaald in redelijke prioriteitenstelling. Risicobeleid • Risicobeleid voldoende afgestemd op geïdentificeerde risico's die als belangrijk zijn aangemerkt. • Risicobeleid geeft aan of juridische risico's beheerst dienen te worden. • Afdeling juridische zaken heeft haar taken en verantwoordelijkheden vastgelegd in een charter. • Beleid, voorzover niet passend binnen de door de hoogste leiding vastgestelde kaders, wordt ter goedkeuring voorgelegd aan de hoogste leiding. • Kwaliteit van beleid (volledigheid, documentatieniveau, kwaliteit van de inhoud, diepgang) is bevredigend. • Afdeling juridische zaken adequaat gepositioneerd met voldoende toegang tot het topmanagement. • In beleid op hoofdlijnen vastgelegd wanneer externe juridische ondersteuning moet worden ingeschakeld.

1. Sterke beheersing (vervolg)	*2. Voldoende beheersing (vervolg)*
Administratieve organisatie en interne controle • Juridische expertise in ruime mate aanwezig en vaktechniek wordt zeer goed onderhouden. • Uitgebreide kennis van wet- en regelgeving. • Relevante wet- en regelgeving wordt voortvarend vertaald naar en geïmplementeerd in interne processen en procedures. • Veranderingen in wet- en regelgeving worden snel onderkend en goed binnen de instelling gecommuniceerd. • Vaktechniek is goed ingebed in de organisatie. • Voor complexere zaken wordt altijd advies ingewonnen bij gerenommeerde externe juristen. • In de lijn is veel juridische expertise aanwezig. • Medewerkers juridische zaken zijn ervaren en ruim voldoende gekwalificeerd. • Taken, bevoegdheden en verantwoordelijkheden van juridische zaken zijn goed geïntegreerd in de instelling. • Adequate klachtenprocedure (inzake juridische procedures, administratieve boetes, sancties). • Juridische expertise wordt standaard betrokken bij het opstellen of afsluiten van contracten, productvoorwaarden, polisvoorwaarden alsmede bij belangrijke en complexe transacties (waaronder complexe constructies, securitisaties, overnames, fusies, portefeuilleoverdrachten, oprichting juridische entiteiten). • Onafhankelijkheid c.q. zelfstandigheid van afdeling juridische zaken is zeer goed geborgd. • Veelvuldig gebruikmaken van kennisuitwisseling, coördinatie, signalering en contacten tussen juridische functies intern. Risicomonitoring • Standaard periodieke managementinformatie inzake juridische ontwikkelingen en risico's richting topmanagement. Idem escalatie bij ad-hocproblemen. • Standaard vastlegging van juridische lopende zaken binnen afdeling juridische zaken. • Management laat zich frequent en pro-actief informeren over belangrijke juridische ontwikkelingen, risico's en de beheersing daarvan. Topmanagement toont veel interesse in en bewustzijn omtrent juridische risico's. Juridische aspecten zijn een standaard onderdeel van de agenda van het top-management.	Administratieve organisatie en interne controle • Voldoende juridische expertise aanwezig en vaktechniek wordt adequaat onderhouden. • Voldoende kennis van wet- en regelgeving. • Relevante wet- en regelgeving wordt voldoende vertaald naar en geïmplementeerd in interne processen en procedures. • Veranderingen in wet- en regelgeving worden redelijk snel en voldoende binnen de instelling gecommuniceerd. • Vaktechniek is ingebed in de organisatie. • Voor complexere zaken wordt regelmatig advies ingewonnen bij gerenommeerde externe juristen. • In de lijn is voldoende juridische expertise aanwezig. • Medewerkers juridische zaken zijn voldoende ervaren en voldoende gekwalificeerd. • Taken, bevoegdheden en verantwoordelijkheden van juridische zaken zijn volledig geïntegreerd in de instelling. • Acceptabele klachtenprocedure (inzake juridische procedures, administratieve boetes, sancties). • Juridische expertise wordt ad hoc betrokken bij het opstellen of afsluiten van contracten, productvoorwaarden, polis-voorwaarden alsmede bij belangrijke transacties (waaronder complexe transacties, securitisaties, overnames, fusies, portefeuilleoverdrachten, oprichting juridische entiteiten). • Onafhankelijkheid c.q. zelfstandigheid van afdeling juridische zaken is voldoende geborgd. • In voldoende mate gebruikmaken van kennisuitwisseling, coördinatie, signalering en contacten tussen juridische functies intern. Risicomonitoring • Ad hoc wordt managementinformatie inzake juridische ontwikkelingen en risico's richting topmanagement opgesteld. Idem escalatie bij ad-hocproblemen. • Ad hoc vastlegging van juridische lopende zaken binnen afdeling juridische zaken. • Management laat zich periodiek en veelal proactief informeren over belangrijke juridische ontwikkelingen, risico's en de beheersing daarvan. Topmanagement toont interesse in en bewustzijn omtrent juridische risico's. Juridische aspecten belanden ad hoc op het niveau van topmanagement.

3. Onvoldoende beheersing	*4. Zwakke beheersing*
<u>Risico-identificatie</u> • Incidenteel in kaart brengen van juridische risico's en ontwikkelingen (zowel intern als extern) op instellingsniveau. • Belangrijke nieuwe producten, initiatieven, projecten worden veelal pas achteraf op hoofdlijnen geanalyseerd op gerelateerde juridische risico's. • Onvoldoende betrokkenheid van management en medewerkers bij risico-identificatie. Onvoldoende begrip van alle aspecten van juridisch risico door verantwoordelijke staf en management. • Risico-identificatie slecht gedocumenteerd. • Risico-identificatie in onvoldoende mate gebaseerd op systematische aanpak. • Risico-identificatie onvoldoende vertaald in prioriteitenstelling.	<u>Risico-identificatie</u> • Juridische risico's en ontwikkelingen (zowel intern als extern) worden niet expliciet in kaart gebracht. • Belangrijke nieuwe producten, initiatieven, projecten worden niet geanalyseerd op gerelateerde juridische risico's. • Nauwelijks betrokkenheid van management en medewerkers bij risico-identificatie. Nauwelijks begrip van alle aspecten van juridisch risico door verantwoordelijke staf en management. • Risico-identificatie niet gedocumenteerd. • Risico-identificatie niet gebaseerd op systematische aanpak. • Risico-identificatie niet vertaald in prioriteitenstelling.
<u>Risicobeleid</u> • Risicobeleid onvoldoende afgestemd op geïdentificeerde risico's die als belangrijk zijn aangemerkt. • Risicobeleid geeft onvoldoende aan of juridische risico's beheerst dienen te worden. • Afdeling juridische zaken heeft haar taken en verantwoordelijkheden zeer summier vastgelegd in een charter. • Beleid, voorzover niet passend binnen de door de hoogste leiding vastgestelde kaders, wordt geregeld niet ter goedkeuring voorgelegd aan de hoogste leiding. • Kwaliteit van beleid (volledigheid, documentatieniveau, kwaliteit van de inhoud, diepgang) is onbevredigend. • Afdeling juridische zaken niet sterk gepositioneerd; toegang tot het topmanagement te beperkt. • In beleid onvoldoende vastgelegd wanneer externe juridische ondersteuning moet worden ingeschakeld.	<u>Risicobeleid</u> • Risicobeleid niet afgestemd op geïdentificeerde risico's die als belangrijk zijn aangemerkt. • Risicobeleid geeft niet aan of juridische risico's beheerst dienen te worden. • Afdeling juridische zaken heeft haar taken en verantwoordelijkheden niet vastgelegd in een charter. • Beleid, voorzover niet passend binnen de door de hoogste leiding vastgestelde kaders, wordt niet ter goedkeuring voorgelegd aan de hoogste leiding. • Kwaliteit van beleid (volledigheid, documentatieniveau, kwaliteit van de inhoud, diepgang) is onduidelijk. • Afdeling juridische zaken zwak gepositioneerd; toegang tot het topmanagement ruim onvoldoende. • In beleid niet vastgelegd wanneer externe juridische ondersteuning moet worden ingeschakeld.

3. Onvoldoende beheersing (vervolg)	*4. Zwakke beheersing (vervolg)*
Administratieve organisatie en interne controle • Onvoldoende juridische expertise aanwezig en vaktechniek wordt onvoldoende onderhouden. • Onvoldoende kennis van wet- en regelgeving. • Relevante wet- en regelgeving wordt vertraagd en beperkt vertaald naar en geïmplementeerd in interne processen en procedures. • Veranderingen in wet- en regelgeving worden niet snel en onvoldoende binnen de instelling gecommuniceerd. • Vaktechniek onvoldoende ingebed in de organisatie. • Voor complexere zaken wordt met regelmaat onvoldoende advies ingewonnen bij gerenommeerde externe juristen. • In de lijn is weinig juridische expertise aanwezig. • Medewerkers juridische zaken zijn deels onervaren en/of onvoldoende gekwalificeerd. • Taken, bevoegdheden en verantwoordelijkheden van juridische zaken moeten duidelijk verbeterd worden op het gebied van documentatie en inbedding binnen de instelling. • Ontoereikende klachtenprocedure (inzake juridische procedures, administratieve boetes, sancties). • Juridische expertise onvoldoende betrokken bij het opstellen of afsluiten van contracten, productvoorwaarden, polisvoorwaarden alsmede bij belangrijke transacties (waaronder overnames, fusies, portefeuilleoverdrachten, oprichting juridische entiteiten). • Onafhankelijkheid c.q. zelfstandigheid van afdeling juridische zaken is onvoldoende geborgd. • In beperkte mate gebruikmaken van kennisuitwisseling, coördinatie, signalering en contacten tussen juridische functies intern.	Administratieve organisatie en interne controle • Zeer weinig juridische expertise aanwezig en vaktechniek wordt nauwelijks onderhouden. • Slechte kennis van wet- en regelgeving. • Relevante wet- en regelgeving wordt zeer traag en nauwelijks vertaald naar en geïmplementeerd in interne processen en procedures. • Veranderingen in wet- en regelgeving worden nauwelijks, en vaak te laat, binnen de instelling gecommuniceerd. • Vaktechniek slecht ingebed in de organisatie. • Geen advies inwinnen bij gerenommeerde externe juristen. • In de lijn is geen juridische expertise aanwezig. • Medewerkers juridische zaken zijn onervaren en van een laag kennisniveau. • Taken, bevoegdheden en verantwoordelijkheden juridische zaken zijn slecht gedocumenteerd en geïmplementeerd. • Geen klachtenprocedure (inzake juridische procedures, administratieve boetes, sancties). • Juridische expertise wordt substantieel onvoldoende betrokken bij het opstellen of afsluiten van contracten, productvoorwaarden, polisvoorwaarden alsmede bij belangrijke transacties (waaronder overnames, fusies, portefeuilleoverdrachten, oprichting juridische entiteiten). • Onafhankelijkheid c.q. zelfstandigheid van afdeling juridische zaken is niet geborgd. • Vrijwel niet gebruikmaken van kennisuitwisseling, coördinatie, signalering en contacten tussen juridische functies intern.
Risicomonitoring • Onvoldoende periodieke managementinformatie inzake juridische ontwikkelingen en risico's richting topmanagement. Idem escalatie bij ad-hocproblemen. • Weinig tot geen vastlegging van juridische lopende zaken binnen afdeling juridische zaken. • Management laat zich op ad-hocbasis en veelal reactief informeren over belangrijke juridische ontwikkelingen, risico's en de beheersing daarvan. • Topmanagement toont weinig interesse in en bewustzijn omtrent juridische risico's. Juridische aspecten belanden veelal niet tot nauwelijks op het niveau van topmanagement.	Risicomonitoring • Geen periodieke managementinformatie inzake juridische ontwikkelingen en risico's richting topmanagement. Idem escalatie bij ad-hocproblemen. • Geen vastlegging van juridische lopende zaken binnen afdeling juridische zaken. • Management laat zich op zeer ad-hocbasis en altijd reactief informeren over belangrijke juridische ontwikkelingen, risico's en de beheersing daarvan. Topmanagement toont weinig tot geen interesse in en bewustzijn omtrent juridische risico's. Juridische aspecten belanden niet tot nauwelijks op het niveau van topmanagement.

D11: BEHEERSINGSCATEGORIE: MANAGEMENT

Beoordeel de risicomitigerende werking van de risico-overstijgende beheersingscategorie Management.
Kies de score die het beste de kwaliteit van de beheersingsmaatregelen weergeeft. Hierbij hoeft niet steeds aan alle geformuleerde criteria voldaan te worden. Het is aan de toezichthouder om te beoordelen welke criteria de doorslag geven bij de toekenning van een score.

Items van de beheersingscategorie management:
- management kwaliteit en structuur;
- strategie;
- risico/control houding;
- besturing en besluitvorming.

Definitie van de items

Management kwaliteit en structuur
De wijze waarop effectief invulling wordt gegeven aan het leiderschap van de instelling. Hierbij kan worden gedacht aan:
- de competentie van het management (bestuur) als geheel om leiding te geven aan de instelling;
- de mate waarin het management (bestuur) voldoende uitgebalanceerd is in expertise en achtergrond;
- de mate waarin de managementstructuur en -samenstelling is toegesneden op de omvang en complexiteit van de bedrijfsactiviteiten;
- de mate waarin op adequate wijze verantwoordelijkheden zijn toegewezen aan individuele leden van het management (bestuur) en de mate waarin er sprake is van een adequate span of control;
- de mate waarin het management (bestuur) al dan niet een voorbeeldfunctie (waaronder het uitdragen van ethische normen en waarden) vervult;
- de leiderschapsstijl van het management (bestuur) en de mate waarin het management binnen de instelling gerespecteerd wordt.

Strategie
Dit betreft:
- de wijze waarop de strategie binnen een instelling totstandkomt;
- de mate waarin dit organisatiebreed wordt aangepakt;
- de transparantie van het proces;
- de inhoudelijkheid en eenduidigheid van de strategie;
- de mate van concreetheid alsmede;
- de mate waarin de strategie van de instelling voldoende eenduidig wordt gecommuniceerd.

Risico/control houding
Dit betreft:
- de mate waarin het management (bestuur) zich bewust is van, aandacht heeft voor, dan wel inzicht heeft in de risico's die de instelling loopt;
- de bereidheid van het verantwoordelijke management (bestuur) om adequate beheersingsmaatregelen (zowel intern als op basis van wettelijke voorschriften) in te zetten en hiervoor voldoende middelen beschikbaar te stellen;
- de mate waarin het management (bestuur) bereid is tot het nemen van risico's en hierbij een adequate risico-rendement-afweging maakt;
- de mate waarin het management (bestuur) zich houdt aan bestaande interne controlemaatregelen.

Besturing en besluitvorming
Dit betreft:
- de mate waarin het management (bestuur) voldoende actief en inhoudelijk betrokken is bij de operationele bedrijfsvoering en resultaten. Dit uit zich onder andere in de frequentie, inhoudelijkheid, intensiteit en actiegerichtheid van het managementoverleg;
- de effectiviteit van de delegatie van bevoegdheden aan (besluitvormende) organen (zoals risicocomités).

Beoordelingscriteria

1. Sterke beheersing	*2. Voldoende beheersing*
Management kwaliteit en structuur • Sterk, uitgebalanceerd, voldoende breed samengesteld en zeer ervaren top en middle management. • Hoge integriteit van management. • Kennis, ervaring en integriteit van top en middle-management uitstekend toegesneden op de instelling en verantwoordelijkheid. • Top en middle-management gaat op zeer ethische wijze om met medewerkers, klanten en andere derden. • Uitstekende track record wat betreft het opstellen en uitvoeren van strategieën en het oplossen van problemen. • Duidelijke structuur van subgroepen, open en opbouwende relatie binnen managementstructuur. Medewerkers en leidinggevenden zijn tevreden over aansturing en leiderschap • Sterk overzicht en betrokkenheid door ervaren hoger management • Middle-management voldoende onafhankelijk; durft beslissingen en voorstellen van hoger management te bekritiseren en/of ter discussie te stellen. Strategie • Alle relevante leidinggevenden en medewerkers zijn betrokken bij het opstellen van de ondernemingsstrategie (zeer ondernemingsbreed proces). • In de strategische planning zijn de bedrijfsdoelstellingen duidelijk geformuleerd. • Duidelijk, systematisch, transparant en goed beheerst proces van totstandkoming van de strategie. • In het strategisch planningsproces zijn voldoende checks en balances aangebracht ter toetsing van aannames, uitgangspunten en berekeningen. • Strategie geeft blijk van scherpe analyse van omgeving, concurrentiepositie, risico's, als mede interne sterkten en zwakten • Strategie geeft blijk van een realistische kijk (reële aannames en uitgangspunten). • Aannames zeer helder uiteengezet. • De strategie wordt instellingsbreed helder gecommuniceerd • De strategie is zeer concreet en bevat zeer concrete en reële doelstellingen.	Management kwaliteit en structuur • Competentie en ervaring van top en middle-management is acceptabel, doch niet optimaal. • Integriteit van management is acceptabel. • Kennis, ervaring en integriteit van top en middle-management voldoende toegesneden op de instelling en verantwoordelijkheid. • Top en middle-management gaat op voldoende ethische wijze om met medewerkers, klanten en andere derden. • Verbetering mogelijk wat betreft het opstellen en uitvoeren van strategieën en het oplossen van problemen. • Acceptabele structuur van subgroepen. Medewerkers en leidinggevenden zijn voldoende tevreden over aansturing en leiderschap. • Voldoende overzicht door redelijk ervaren hoger management • Middle-management redelijk onafhankelijk; durft beslissingen en voorstellen van hoger management te bekritiseren en/of ter discussie te stellen. Strategie • Bevredigende betrokkenheid van relevante leidinggevenden en medewerkers bij het opstellen van de ondernemingsstrategie (in redelijke mate ondernemingsbreed proces). • In de strategische planning zijn de bedrijfsdoelstellingen redelijk duidelijk geformuleerd. • Adequaat proces van strategische planning. Enigszins ad-hocproces en beperkte transparantie. • In het strategische planningsproces is slechts een beperkt aantal checks en balances aangebracht ter toetsing van aannames, uitgangspunten en berekeningen. • Strategie geeft blijk van toereikende analyse van omgeving, concurrentiepositie, risico's en interne sterkten en zwakten. • Strategie geeft blijk van een redelijk realistische kijk (aannames en uitgangspunten zijn acceptabel). • Aannames redelijk helder uiteengezet. • De strategie wordt alleen voor het hogere kader, maar wel instellingsbreed, helder gecommuniceerd. • De strategie is redelijk concreet en bevat redelijk concrete en reële doelstellingen.

1. Sterke beheersing (vervolg)	*2. Voldoende beheersing (vervolg)*
Risico/control houding • Risicobereidheid van management is in overeenstemming met de economische kracht en de algehele kwaliteit van de instelling. • Belang van een adequate risicoanalyse en adequate beheersing van risico's wordt krachtig ondersteund, uitgedragen en afgedwongen door het management. • Risicobewustzijn wordt actief gestimuleerd binnen de instelling. • Goede, open en respectvolle relatie met toezichthouders en onder andere eigen internal audit, risk management en compliancefunctie. • Management laat zich periodiek informeren over status van risico's, de kwaliteit van beheersing en de status van tekortkomingen en verbeterplannen. Er bestaan expliciete risicorapportages. • Bij het nemen van beslissingen is zichtbaar en ruim voldoende aandacht voor mogelijke risico's. • Management is zeer bereid om waar nodig adequate beheersingsmaatregelen in te zetten en hiervoor ruim voldoende middelen beschikbaar te stellen. • Zeer integriteitsbewuste cultuur; management is zich zeer bewust van het feit dat men integriteitsrisico´s loopt en op welke specifieke gebieden.	Risico/control houding • Risicobereidheid van management is voldoende in overeenstemming met de economische kracht en de algehele kwaliteit van de instelling. • Belang van een adequate risicoanalyse en adequate beheersing van risico's wordt voldoende ondersteund, uitgedragen en afgedwongen door het management. • Risicobewustzijn wordt beperkt gestimuleerd binnen de instelling. • Voldoende open relatie met toezichthouders en onder andere eigen internal audit, risk management en compliancefunctie. • Management laat zich in voldoende mate informeren over risico's en de beheersing daarvan alsmede de follow-up van aandachtspunten. Er bestaan risicorapportages. • Bij het nemen van beslissingen is aandacht voor mogelijke risico's. • Management is bereid om waar nodig adequate beheersingsmaatregelen in te zetten en hiervoor middelen beschikbaar te stellen. • Integriteitsbewuste cultuur; management is zich voldoende bewust van het feit dat men integriteitsrisico´s loopt en op welke specifieke gebieden.
Besturing en besluitvorming • Absoluut geen sprake van afhankelijkheid van sleutelfiguren. • Management ruim voldoende betrokken bij operationele bedrijfsvoering en belangrijke issues. • Frequentie en inhoud van top en middle-management-vergaderingen zeer goed toegesneden op de complexiteit van de activiteiten en risico's. • Management onderscheidt zich door sterke daadkracht en besluitvaardigheid. • Verantwoordelijkheden en 'accountability' duidelijk en eenduidig vastgelegd en gecommuniceerd. • Ruim voldoende intensief overleg binnen managementteams en tussen managementlagen op verschillende niveaus. • Zeer uitgebreide vastlegging inzake genomen besluiten.	Besturing en besluitvorming • Geen significante afhankelijkheid van sleutelfiguren. • Management voldoende betrokken bij operationele bedrijfsvoering en belangrijke issues. • Frequentie en inhoud van top en middle-management-vergaderingen voldoende toegesneden op de complexiteit van de activiteiten en risico's. • Management toont voldoende daadkracht en besluitvaardigheid. • Verantwoordelijkheden en 'accountability' adequaat vastgelegd en gecommuniceerd. • Voldoende overleg binnen managementteams en tussen managementlagen op verschillende niveaus. • Voldoende vastlegging inzake genomen besluiten.

3. Onvoldoende beheersing

Management kwaliteit en structuur

- Ervaring en competentie van top en middle-management verdient verbetering. Management onvoldoende breed samengesteld.
- Integriteit van management twijfelachtig.
- Kennis, ervaring en integriteit van top en middle-management slechts in beperkte mate toegesneden op de instelling en verantwoordelijkheid.
- Top en middle-management gaat vaak op twijfelachtig ethische wijze om met medewerkers, klanten en andere derden.
- Het management toont onvoldoende bekwaamheden wat betreft het opstellen en uitvoeren van strategieën en het oplossen van problemen.
- Onduidelijke structuur van subgroepen. Medewerkers en leidinggevenden zijn ontevreden over aansturing en leiderschap.
- Hoger management niet sterk, onvoldoende betrokkenheid.
- Middle-management niet erg onafhankelijk; durft beslissingen en voorstellen van hoger management nauwelijks te bekritiseren en/of ter discussie te stellen.

Strategie

- Onbevredigende betrokkenheid van relevante leidinggevenden en medewerkers bij het opstellen van de ondernemingsstrategie. Strategie door zeer beperkte groep managers opgesteld (nauwelijks sprake van een ondernemingsbreed proces).
- In de strategische planning zijn de bedrijfsdoelstellingen onduidelijk geformuleerd.
- Onduidelijk en veelal ad hoc proces van strategische planning.
- In het strategisch planningsproces zijn nauwelijks checks en balances aangebracht ter toetsing van aannames, uitgangspunten en berekeningen.
- Strategie geeft onvoldoende blijk van analyse van omgeving, concurrentiepositie, risico's, alsmede interne sterkten en zwakten.
- Strategie geeft blijk van een te optimistische kijk (te positieve aannames en uitgangspunten).
- Aannames veelal niet duidelijk uiteengezet binnen de strategie.
- De strategie wordt nauwelijks binnen de instelling gecommuniceerd.
- De strategie is weinig concreet en bevat voornamelijk vage doelstellingen.

4. Zwakke beheersing

Management kwaliteit en structuur

- Competentie en ervaring van top en middle-management absoluut ontoereikend. Samenstelling van management ruim onder de maat.
- Integriteit van management staat ter discussie.
- Kennis, ervaring en integriteit van top en middle-management onvoldoende toegesneden op de instelling en verantwoordelijkheid.
- Omgang van top en middle-management met medewerkers, klanten en andere derden vaak onethisch.
- Het management toont gebrekkige bekwaamheden wat betreft het opstellen en uitvoeren van strategieën en het oplossen van problemen.
- Onacceptabele structuur van subgroepen. Medewerkers en leidinggevenden zijn in sterke mate ontevreden over aansturing en leiderschap.
- Hoger management niet betrokken en niet kritisch genoeg.
- Middle-management zeer afhankelijk van topmanagement; durft beslissingen en voorstellen van hoger management niet te bekritiseren en/of ter discussie te stellen. Voert slechts uit.

Strategie

- Veel relevante leidinggevenden en medewerkers zijn niet betrokken bij het opstellen van de ondernemingsstrategie (absoluut geen ondernemingsbreed proces).
- In de strategische planning zijn de bedrijfsdoelstellingen in sterke mate onduidelijk geformuleerd.
- Ongestructureerd, ad hoc en niet transparant proces van strategische planning.
- In het strategisch planningsproces zijn geen checks en balances aangebracht ter toetsing van aannames, uitgangspunten en berekeningen.
- Strategie geeft blijk van ontoereikende analyse van omgeving, concurrentiepositie, risico's, alsmede interne sterkten en zwakten
- Strategie geeft blijk van een onrealistische kijk (irreële aannames en uitgangspunten).
- Aannames absoluut niet duidelijk.
- De strategie wordt niet binnen de instelling gecommuniceerd.
- De strategie is niet concreet en bevat voornamelijk vage en veelal weinig reële doelstellingen.

3. Onvoldoende beheersing (vervolg)	*4. Zwakke beheersing (vervolg)*
Risico/control houding • Risicobereidheid van management is onvoldoende in overeenstemming met de economische kracht en de algehele kwaliteit van de instelling. • Belang van een adequate risicoanalyse en adequate beheersing van risico's wordt onvoldoende ondersteund, uitgedragen en afgedwongen door het management. • Risicobewustzijn wordt niet actief gestimuleerd binnen de instelling. • Zwakke, gesloten en defensieve relatie met toezichthouder en eigen internal audit, risk management en compliancefunctie. • Management informeert slechts op ad-hocbasis naar risico's en de wijze waarop deze worden beheerst en heeft onvoldoende aandacht voor follow-up van aandachtspunten. De instelling kent geen risicorapportages. • Bij het nemen van beslissingen is weinig zichtbaar of onvoldoende aandacht voor mogelijke risico's. • Management is slechts beperkt bereid om waar nodig adequate beheersingsmaatregelen in te zetten en stelt hier veelal onvoldoende middelen voor beschikbaar. • Slechts beperkte integriteitsbewuste cultuur; management is zich onvoldoende bewust van het feit dat men integriteitsrisico´s loopt en op welke specifieke gebieden.	Risico/control houding • Risicobereidheid van management is nauwelijks in overeenstemming met de economische kracht en de algehele kwaliteit van de instelling. • Belang van een adequate risicoanalyse en adequate beheersing van risico's wordt nauwelijks ondersteund, uitgedragen en afgedwongen door het management. • Risicobewustzijn wordt in het geheel niet gestimuleerd binnen de instelling. • Vrijwel geen bereidheid tot samenwerking met toezichthouder en eigen internal audit, risk management en compliance-functie. Erg veel discussie met en onbegrip voor toezicht-houders. • Management informeert nauwelijks naar risico's, de wijze waarop deze worden beheerst en de getroffen maatregelen ter verbetering. De instelling kent geen risicorapportages. • Bij het nemen van beslissingen is niet zichtbaar en/of absoluut onvoldoende aandacht voor mogelijke risico's. • Management is veelal niet bereid om waar nodig adequate beheersingsmaatregelen in te zetten en stelt hier veelal dan ook geen middelen voor beschikbaar. • Nauwelijks tot geen integriteitsbewuste cultuur; management is zich niet bewust van het feit dat men integriteitsrisico´s loopt en op welke specifieke gebieden.
Besturing en besluitvorming • Afhankelijkheid van een beperkt aantal sleutelfiguren. • Management onvoldoende betrokken bij operationele bedrijfsvoering en belangrijke issues. • Frequentie en inhoud van top en middle-management-vergaderingen niet voldoende toegesneden op de complexiteit van de activiteiten en risico's. • Management toont onvoldoende daadkracht en besluitvaardig-heid. • Verantwoordelijkheden en 'accountability' gebrekkig vastgelegd en gecommuniceerd. • Onvoldoende overleg binnen managementteams en tussen managementlagen op verschillende niveaus. • Gebrekkige vastlegging inzake genomen besluiten.	Besturing en besluitvorming • Sterke afhankelijkheid van een beperkt aantal sleutelfiguren, zonder dat opvolging of vervanging geregeld is. • Management vrijwel niet betrokken bij operationele bedrijfs-voering en belangrijke issues; erg afstandelijk. • Frequentie en inhoud van top en middle-management-vergaderingen slecht toegesneden op de complexiteit van de activiteiten en risico's. • Management niet daadkrachtig en besluitvaardig. • Verantwoordelijkheden en 'accountability' nauwelijks vast-gelegd en gecommuniceerd. • Vrijwel geen overleg binnen managementteams en tussen managementlagen op verschillende niveaus. • Slechte vastlegging inzake genomen besluiten.

D12: BEHEERSINGSCATEGORIE: ORGANISATIE

Beoordeel de risicomitigerende werking van de risico-overstijgende beheersingscategorie organisatie.
Kies de score die het beste de kwaliteit van de beheersingsmaatregelen weergeeft. Hierbij hoeft niet steeds aan alle geformuleerde criteria voldaan te worden. Het is aan de toezichthouder om te beoordelen welke criteria de doorslag geven bij de toekenning van een score.

Items van de beheersingscategorie organisatie:
- organisatiestructuur;
- managementinformatievoorziening;
- human resources;
- interne samenwerking en communicatie;
- auditmaatregelen.

Definitie van de items

Organisatiestructuur
De transparantie van de juridische of organisatorische structuur alsmede de geschiktheid ervan om op effectieve wijze invulling te geven aan de bedrijfsvoering.

Managementinformatievoorziening
De mate waarin relevante financiële en operationele informatie tijdig en betrouwbaar beschikbaar is teneinde verantwoordelijke medewerkers (waaronder het management) in staat te stellen om tijdig en geïnformeerd beslissingen te nemen alsmede tijdig bij te sturen waar de situatie daartoe aanleiding geeft.

Human resources
De mate waarin er sprake is van adequaat HR-beleid, deugdelijke HR-instrumenten alsmede een adequate kwalitatieve en kwantitatieve personele bezetting.

Interne samenwerking en communicatie
De mate waarin de interne communicatie en samenwerking tussen afdelingen en business units alsmede met groepsfuncties functioneert gericht op het effectief samenwerken ten einde de doelstellingen te kunnen realiseren.

Auditmaatregelen
De mate waarin interne en externe audits van accountants en actuarissen effectief bijdragen aan de identificatie, analyse, beheersing, monitoring en rapportering van risico's.

Beoordelingscriteria

1. Sterke beheersing	*2. Voldoende beheersing*
<u>Organisatiestructuur</u> • Uiterst transparante en inzichtelijke (juridische en organisatorische) structuur. • (Juridische en organisatorische) structuur is duidelijk, up-to-date en toegankelijk gedocumenteerd. • Complexiteit van de (juridische en organisatorische) structuur is uitermate goed toegesneden op behoeften en complexiteit van de business alsmede op de geografische oriëntatie. • Overwegingen die aan de juridische of organisatorische structuur ten grondslag liggen geven geen aanleiding tot kritische kanttekeningen. • Periodieke evaluatie van de organisatiestructuur. • Organisatiestructuur robuust en stabiel; weinig wijzigingen in de loop van de tijd. • Verdeling van rollen en verantwoordelijkheden tussen business units (i.c. lijnmanagement) en groepsstaven (centrale functies) is helder en eenduidig. • Goede balans tussen controlfunctie binnen business units/ divisies en controlfunctie op groepsniveau.	<u>Organisatiestructuur</u> • Transparantie en inzichtelijkheid van de (juridische en organisatorische) organisatiestructuur is adequaat. • (Juridische en organisatorische) structuur is in voldoende mate up-to-date gedocumenteerd. • Complexiteit van de (juridische en organisatorische) structuur is voldoende toegesneden op behoeften en complexiteit van de business alsmede op de geografische oriëntatie. • Overwegingen die aan de juridische of organisatorische structuur ten grondslag liggen geven geen grote aanleiding tot kritische kanttekeningen. • Periodieke evaluatie van de organisatiestructuur op hoofdlijnen. • Organisatiestructuur redelijk robuust en stabiel; slechts beperkte wijzigingen in de loop van de tijd. • Verdeling van rollen en verantwoordelijkheden tussen business units (i.c. lijnmanagement) en groepsstaven (centrale functies) is redelijk helder en eenduidig. • Balans tussen controlfunctie binnen business units/divisies en controlfunctie op groepsniveau is toereikend.
<u>Managementinformatievoorziening</u> • Rapportagelijnen en rapportage-inhoud volledig in overeenstemming met behoeften vanuit de organisatie en de verantwoordelijkheidsstructuur en zijn goed gedocumenteerd. • Het management ontvangt tijdige, nauwkeurige, volledige en relevante verslagen en rapportages. • Mate van detail (aggregatieniveau) van rapportages sluit zeer goed aan bij het betreffende managementniveau. • In rapportages wordt zeer helder en expliciet verslag gedaan van de belangrijkste stuurvariabelen, prestatie-indicatoren en kritische succesfactoren. • Rapportages worden voorzien van normcijfers en vergelijkende cijfers; afwijkingen en ontwikkelingen worden goed geanalyseerd en verklaard. • Het rapportageproces wordt goed beheerst; er is sprake van adequate kwaliteitswaarborgen. • Rapportages komen zeer snel beschikbaar voor verantwoordelijk management. Doorlooptijd van totstandkoming is derhalve zeer beperkt. • Rapportages worden tot stand gebracht door functies die onafhankelijk staan van de directe lijnverantwoordelijkheid. • Goede balans tussen financiële en operationele informatie. • Voor regulier benodigde informatie slechts zeer incidenteel gebruik van spreadsheets en dergelijke ter aanvulling op reguliere rapportages.	<u>Managementinformatievoorziening</u> • Rapportagelijnen en rapportage-inhoud in voldoende mate in overeenstemming met behoeften vanuit de organisatie en de verantwoordelijkheidsstructuur en zijn voldoende gedocumenteerd. • Het management ontvangt in voldoende mate tijdige, nauwkeurige en volledige verslagen en rapportages. • Mate van detail (aggregatieniveau) van rapportages sluit redelijk goed aan bij het betreffende managementniveau. • In rapportages wordt helder en expliciet verslag gedaan van de belangrijkste stuurvariabelen, prestatie-indicatoren en kritische succesfactoren. • Rapportages worden op hoofdlijnen voorzien van normcijfers en vergelijkende cijfers; afwijkingen en ontwikkelingen worden in zekere mate geanalyseerd en verklaard. • Het rapportageproces wordt voldoende beheerst; de kwaliteitswaarborgen zijn acceptabel. • Rapportages komen voldoende snel beschikbaar voor verantwoordelijk management. Doorlooptijd van totstandkoming is derhalve acceptabel. • Rapportages worden tot stand gebracht door functies die in redelijke mate onafhankelijk staan van de directe lijn-verantwoordelijkheid. • Acceptabele balans tussen financiële en operationele informatie. • Voor regulier benodigde informatie met enige regelmaat gebruik van spreadsheets en dergelijke ter aanvulling op reguliere rapportages.

1. Sterke beheersing (vervolg)	*2. Voldoende beheersing (vervolg)*
Human resources • Personeelsbeleid is goed ontwikkeld en in lijn met de strategie. • Sterke procedures voor aanname en screening van personeel. • Zeer gestructureerd proces van beoordeling en begeleiding van medewerkers. 'High potentials" worden onderkend en actief gemonitored. • Opleidings-, kennis- en ervaringseisen die aan functies worden gesteld zijn ruim voldoende in relatie tot de aard en complexiteit van de instelling. • Personeelsbezetting is goed. • Kennis- en ervaringsniveau optimaal in lijn met behoeften en complexiteit van de organisatie. • Geen substantieel deel tijdelijke krachten. • Zeer goed gedocumenteerde en actuele functiebeschrijvingen waarin taken, bevoegdheden en verantwoordelijkheden zijn uiteengezet.	Human resources • Personeelsbeleid is voldoende ontwikkeld en voldoende in lijn met de strategie. • Acceptabele procedures voor aanname en screening van personeel. • Gestructureerd proces van beoordeling en begeleiding van medewerkers. ´High potentials´ worden onderkend en actief gemonitored. • Opleidings-, kennis- en ervaringseisen die aan functies worden gesteld zijn voldoende in relatie tot de aard en complexiteit van de instelling. • Personeelsbezetting is voldoende. • Kennis- en ervaringsniveau voldoende in lijn met behoeften en complexiteit van de organisatie. • Geen substantieel deel tijdelijke krachten. • Redelijk actuele en adequaat gedocumenteerde functiebeschrijvingen waarin taken, bevoegdheden en verantwoordelijkheden zijn uiteengezet.
Interne samenwerking en communicatie • Intensieve samenwerking tussen lijn- en stafafdelingen alsmede tussen groep/holding en dochters. • Waar nodig vindt voldoende en effectief afdeling/business-unitoverstijgend overleg en communicatie plaats. • Afdelingsoverstijgende projecten worden adequaat beheerst. • Geen silomentaliteit. • Sterke en overtuigende beweegreden achter verbanden met zowel gecentraliseerde als gedecentraliseerde functies. • De aanwezige mate van samenwerking en afstemming is zeer adequaat en voorkomt daarmee suboptimale beslissingen, duplicatie van activiteiten en/of hiaten in bedrijfsvoering.	Interne samenwerking en communicatie • Voldoende samenwerking tussen lijn- en stafafdelingen alsmede tussen groep/holding en dochters. • Waar nodig vindt afdeling/businessunitoverstijgend overleg en communicatie plaats. • Afdelingsoverstijgende projecten worden redelijk goed beheerst. • Neiging naar silomentaliteit. • Voldoende overtuigende beweegreden achter verbanden met zowel gecentraliseerde als gedecentraliseerde functies. • De aanwezige mate van samenwerking en afstemming is adequaat en voorkomt daarmee suboptimale beslissingen, duplicatie van activiteiten en/of hiaten in bedrijfsvoering.
Auditmaatregelen • Internal audit besteedt ruim voldoende aandacht aan de kritische processen en risico's binnen de betreffende functionele activiteit. • Internal audit opereert zeer kritisch. • Internal audit verricht follow-up audits op het gebied van geconstateerde tekortkomingen. • Internal audit draagt zeer zichtbaar en effectief bij aan (verbetering dan wel bewaking van) de kwaliteit van de beheersing binnen de betreffende functionele activiteit. • Internal audit is volledig onafhankelijk, beschikt over uitstekende controleprogramma's en rapporteert rechtstreeks aan het hoger kader of de directie. • Externe accountants en externe actuarissen hebben strikte scheiding aangebracht tussen adviserende en controlerende/certificerende werkzaamheden. • Personeelsbezetting en kwaliteit van de medewerkers zijn goed.	Auditmaatregelen • Internal audit besteedt voldoende aandacht aan de kritische processen en risico's binnen de betreffende functionele activiteit. • Internal audit opereert kritisch. • Internal audit verricht follow-up audits op het gebied van belangrijke geconstateerde tekortkomingen. • Internal audit draagt zichtbaar bij aan (verbetering danwel bewaking van) de kwaliteit van de beheersing binnen de betreffende functionele activiteit. • Internal audit is onafhankelijk, beschikt over controle-programma's en rapporteert rechtstreeks aan het hoger kader of de directie. • Externe accountants en externe actuarissen hebben voldoende scheiding aangebracht tussen adviserende en controlerende/ certificerende werkzaamheden. • Personeelsbezetting en kwaliteit van de medewerkers zijn voldoende.

3. Onvoldoende beheersing

Organisatiestructuur

- Gecompliceerde en moeilijk inzichtelijke (juridische en organisatorische) organisatiestructuur.
- (Juridische en organisatorische) structuur is niet up-to-date gedocumenteerd.
- Complexiteit van de (juridische en organisatorische) structuur onvoldoende toegesneden op behoeften en complexiteit van de business alsmede op de geografische oriëntatie.
- Overwegingen die aan de juridische of organisatorische structuur ten grondslag liggen geven aanleiding tot kritische kanttekeningen.
- Incidentele evaluatie van de organisatiestructuur op hoofd-lijnen.
- Organisatiestructuur beperkt robuust en stabiel; aanzienlijk aantal wijzigingen in de loop van de tijd.
- Verdeling van rollen en verantwoordelijkheden tussen business units (i.c. lijnmanagement) en groepsstaven (centrale functies) is enigszins onduidelijk.
- Matige balans tussen controlfunctie binnen businessunits/ divisies en controlfunctie op groepsniveau.

Managementinformatievoorziening

- Rapportagelijnen en rapportage-inhoud onvoldoende in overeenstemming met behoeften vanuit de organisatie en de verantwoordelijkheidsstructuur en zijn onvoldoende gedocumenteerd.
- Het management ontvangt in onvoldoende mate tijdige, nauw-keurige en volledige informatie.
- Mate van detail (aggregatieniveau) van rapportages sluit niet goed aan bij het betreffende managementniveau. Topmanagement wordt overladen met details.
- In rapportages wordt weinig helder noch expliciet verslag gedaan van de belangrijkste stuurvariabelen, prestatie-indicatoren en kritische succesfactoren.
- Rapportages zijn in onvoldoende mate voorzien van norm-cijfers en vergelijkende cijfers; afwijkingen en ontwikkelingen worden onvoldoende geanalyseerd en verklaard.
- Het rapportageproces wordt onvoldoende beheerst; de kwaliteitswaarborgen zijn zwak.
- Rapportages komen enigszins traag beschikbaar voor verantwoordelijk management. Doorlooptijd van totstandkoming is derhalve lang.
- Rapportages worden tot stand gebracht door functies die afhankelijk staan van de directe lijnverantwoordelijkheid.
- Zwakke balans tussen financiële en operationele informatie.
- Voor regulier benodigde informatie frequent gebruik van spreadsheets e.d. ter aanvulling op reguliere rapportages.

Human resources

- Personeelsbeleid is onvoldoende ontwikkeld en onvoldoende in lijn met de strategie.
- Essentiële tekortkomingen in de procedures voor aanname en screening van personeel.
- Geen gestructureerd proces van beoordeling en begeleiding van medewerkers. Geen actieve aandacht voor ‘high potentials’.
- Opleidings-, kennis- en ervaringseisen die aan functies worden gesteld zijn niet voldoende in relatie tot de aard en complexiteit van de instelling.
- Personeelsbezetting is onvoldoende, bijvoorbeeld sleutel-posities zijn niet goed opgevuld.
- Kennis- en ervaringsniveau onvoldoende in lijn met behoeften en complexiteit van de organisatie.
- Aanzienlijk deel tijdelijke krachten.
- Nauwelijks sprake van actuele functiebeschrijvingen waren taken, bevoegdheden en verantwoordelijkheden zijn uiteengezet.

4. Zwakke beheersing

Organisatiestructuur

- Juridische en organisatorische organisatiestructuur is uiterst gecompliceerd en niet inzichtelijk.
- (Juridische en organisatorische) structuur is vrijwel niet, of niet toegankelijk, alsmede niet up-to-date, gedocumenteerd.
- Complexiteit van de (juridische en organisatorische) structuur niet toegesneden op behoeften en complexiteit van de business alsmede op de geografische oriëntatie.
- Overwegingen die aan de juridische of organisatorische structuur ten grondslag zijn onduidelijk dan wel bieden aanleiding tot zeer kritische kanttekeningen.
- Geen evaluatie van de organisatiestructuur.
- Organisatiestructuur niet robuust en zeer instabiel; structuur wordt zeer frequent herzien.
- Verdeling van rollen en verantwoordelijkheden tussen business units (i.c. lijnmanagement) en groepsstaven (centrale functies) is zeer onduidelijk.
- Balans tussen controlfunctie binnen businessunits/divisies en controlfunctie op groepsniveau is slecht.

Managementinformatievoorziening

- Rapportagelijnen en rapportage-inhoud niet in overeen-stemming met behoeften vanuit de organisatie en de verant-woordelijkheidsstructuur en zijn nauwelijks gedocumenteerd.
- Het management ontvangt geen tijdige, nauwkeurige, volledige en relevante informatie.
- Mate van detail (aggregatieniveau) van rapportages sluit slecht aan bij het betreffende managementniveau. Topmanagement wordt overladen met details, waardoor sturen op hoofdlijnen wordt bemoeilijkt.
- In rapportages wordt nauwelijks tot geen verslag gedaan van de belangrijkste stuurvariabelen, prestatie-indicatoren en kritische succesfactoren.
- Rapportages zijn nauwelijks tot niet voorzien van normcijfers en vergelijkende cijfers; afwijkingen en ontwikkelingen worden slecht of niet geanalyseerd en verklaard.
- Het rapportageproces wordt slecht beheerst; nauwelijks kwaliteitswaarborgen.
- Rapportages komen zeer langzaam beschikbaar voor verantwoordelijk management. Doorlooptijd van totstand-koming is derhalve te lang.
- Rapportages worden tot stand gebracht door functies die zeer afhankelijk staan van de directe lijn verantwoordelijkheid.
- Scheve balans tussen financiële en operationele informatie.
- Voor regulier benodigde informatie continu gebruik van spreadsheets en dergelijke ter aanvulling op reguliere rapportages.

Human resources

- Personeelsbeleid is slecht ontwikkeld en niet in lijn met de strategie.
- Procedures voor aannames en screening van personeel zijn nauwelijks aanwezig dan wel bevatten essentiële tekort-komingen.
- Geen proces van beoordeling en begeleiding van medewerkers. Geen actieve aandacht voor ‘high potentials’.
- Opleidings-, kennis- en ervaringseisen die aan functies worden gesteld zijn onvoldoende in relatie tot de aard en complexiteit van de instelling.
- Personeelsbezetting is slecht.
- Kennis- en ervaringsniveau niet in lijn met behoeften en complexiteit van de organisatie.
- Zeer aanzienlijk deel tijdelijke krachten.
- Geen sprake van actuele functiebeschrijvingen waren taken, bevoegdheden en verantwoordelijkheden zijn uiteengezet.

3. Onvoldoende beheersing (vervolg)	*4. Zwakke beheersing (vervolg)*
Interne samenwerking en communicatie • Nauwelijks samenwerking tussen lijn- en stafafdelingen alsmede tussen groep/holding en dochters. • Noodzaak tot afdelings/businessunitoverstijgend overleg en communicatie wordt, zelfs in voorkomende gevallen, niet onderkend. • Afdelingsoverstijgende projecten worden slecht beheerst. • Beperkte silomentaliteit • Beweegreden achter verbanden met zowel gecentraliseerde als gedecentraliseerde functies is ontoereikend en overtuigend. • Gebrek aan samenwerking en afstemming leidt tot suboptimale beslissingen, duplicatie van activiteiten en/of hiaten in bedrijfsvoering. Auditmaatregelen • Internal audit besteedt onvoldoende aandacht aan de kritische processen en risico's binnen de betreffende functionele activiteit. • Internal audit opereert niet kritisch genoeg. • Internal audit verricht incidenteel follow-up audits op het gebied van belangrijke geconstateerde tekortkomingen. • Internal audit draagt matig bij aan (verbetering dan wel bewaking van) de kwaliteit van de beheersing binnen de betreffende functionele activiteit. • Internal audit is niet geheel onafhankelijk en rapporteert aan de business line of via de business line aan het management. • Externe accountants en externe actuarissen hebben onvoldoende scheiding aangebracht tussen adviserende en controlerende/certificerende werkzaamheden. • Personeelsbezetting en kwaliteit van de medewerkers zijn onvoldoende.	Interne samenwerking en communicatie • Geen samenwerking tussen lijn- en stafafdelingen alsmede tussen groep/holding en dochters. • Noodzaak tot afdelings/businessunitoverstijgend overleg en communicatie wordt, zelfs in voorkomende gevallen, niet onderkend. • Afdelingsoverstijgende projecten worden slecht beheerst. • Absolute silomentaliteit • Zwakke beweegreden achter en/of nauwelijks enige verbanden met zowel gecentraliseerde als gedecentraliseerde functies. • Gebrek aan samenwerking en afstemming leidt tot sub-optimale beslissingen, duplicatie van activiteiten en/of hiaten in bedrijfsvoering. Auditmaatregelen • Internal audit besteedt geen aandacht aan de kritische processen en risico's binnen de betreffende functionele activiteit. • Internal audit opereert niet kritisch. • Internal audit verricht standaard geen follow-up audits op het gebied van belangrijke geconstateerde tekortkomingen. • Internal audit draagt nauwelijks bij aan (verbetering dan wel bewaking van) de kwaliteit van de beheersing binnen de betreffende functionele activiteit. • Internal audit ontbreekt of is in sterke mate afhankelijk. Er vindt geen onafhankelijke rapportage plaats aan het management. • Externe accountants en externe actuarissen hebben geen scheiding aangebracht tussen adviserende en controlerende/certificerende werkzaamheden. • Personeelsbezetting en kwaliteit van de medewerkers zijn in sterke mate onvoldoende.

D13: BEHEERSINGSCATEGORIE: SOLVABILITEITSBEHEER

Beoordeel de risicomitigerende werking van solvabiliteitsbeheer.
Kies de score die het beste de kwaliteit van de beheersingsmaatregelen weergeeft. Hierbij hoeft niet steeds aan alle geformuleerde criteria voldaan te worden. Het is aan de toezichthouder om te beoordelen welke criteria de doorslag geven bij de toekenning van een score.

Items van de beheersingscategorie solvabiliteitsbeheer:
- beleid;
- risicomodellering;
- vermogensanalyse;
- toegang tot kapitaal.

Definitie van de items

Beleid
De mate waarin de instelling beleid heeft ontwikkeld ten aanzien van:
- risk appetite;
- gewenste solvabiliteitsniveau (berekening, omvang en samenstelling);
- de relatie hiervan met wettelijke eisen alsmede met een gewenste externe rating of interne ratio's;
- de wijze waarop men wenst te reageren in geval van (dreigende) solvabiliteitstekorten (contingency planning).

Voor pensioenfondsen wordt hier tevens onder verstaan het beleid ten aanzien van de financiële opzet (inclusief inzet van sturingsmiddelen indexatiebeleid en/of premiebeleid en/of beleggingsbeleid in geval van dreigende solvabiliteitstekorten).

Risicomodellering
De mate waarin en de wijze waarop sprake is van:
- adequate modellering van risico's;
- adequate scenario's (waaronder stress testing) ten aanzien van deze risico's;
- adequate en realistische aannames en uitgangspunten gericht op de berekening van een risk based vermogensbehoefte c.q. vermogenseis (economic capital).

Vermogensanalyse
De wijze waarop en de mate waarin de instelling de toekomstige ontwikkeling van haar activa en passiva prospectief in kaart brengt op basis van haar meerjarenplannen en -begrotingen (i.c. verwachtingen en doelstellingen ten aanzien van onder andere (des)investeringen, financieringen, omzetgroei, winstgevendheid) gericht op de inschatting van de verwachte ontwikkeling van de werkelijke solvabiliteitspositie.

Alsmede de wijze waarop en de mate waarin de ontwikkeling van de werkelijke solvabiliteitspositie ten opzichte van de gewenste/vereiste solvabiliteitspositie (beide zowel met betrekking tot het heden als met betrekking tot de toekomstverwachting) adequaat wordt bewaakt, eventuele signalen in deze tijdig worden afgegeven en waar nodig tijdig actie wordt ondernomen.

Toegang tot kapitaal
De mate waarin mogelijkheden aanwezig zijn om, indien nodig, tijdig en tegen acceptabele voorwaarden een (dreigend) solvabiliteitstekort af te wenden dan wel te corrigeren door bijvoorbeeld:
- voor de langere termijn vermogen te verwerven (kapitaal aan te trekken, bijvoorbeeld een achtergestelde lening van een sponsor van een pensioenfonds);
- inkomstenbronnen aan te boren;
- bezittingen te securitiseren.

Beoordelingscriteria

1. Sterke beheersing	*2. Voldoende beheersing*
<u>Beleid</u> • Heldere uiteenzetting op gedetailleerd niveau welk solvabiliteitsniveau aanvaardbaar geacht wordt. • Beleid niet alleen ingebed op groepsniveau maar ook op lagere organisatorische niveaus (vergunninghouders, product-groepen). • Het gewenste solvabiliteitsniveau wordt niet alleen afgeleid van de wettelijke norm, maar ook van eigen onderbouwde interne normen alsmede externe normen (van bijvoorbeeld rating agencies). Het gewenste solvabiliteitsniveau ligt ruimschoots boven de wettelijke norm. • Solvabiliteitsnormen worden altijd meegenomen bij prijsstelling van producten. • Gedetailleerde inkadering hoe te reageren in geval van (dreiging) van solvabiliteitstekorten (welke sturingsmiddelen, in welke mate, wanneer, effectiviteit van maatregelen). Hoog realiteitsgehalte van het kunnen toepassen van de maatregelen in de praktijk.	<u>Beleid</u> • Duidelijke uiteenzetting op hoofdlijnen welk solvabiliteits-niveau aanvaardbaar geacht wordt. • Beleid niet beperkt tot groepsniveau. • Het solvabiliteitsniveau wordt niet alleen afgeleid van de wettelijke norm, maar ook van eigen onderbouwde interne normen. • Solvabiliteitsnormen worden meegenomen bij prijsstelling van producten. • Inkadering op hoofdlijnen van hoe te reageren in geval (van dreiging) van solvabiliteitstekorten (welke sturingsmiddelen, in welke mate, wanneer, effectiviteit van maatregelen). Toepassing van de maatregelen in de praktijk is realistisch.
<u>Risicomodellering</u> • De instelling maakt gebruik van geavanceerde interne modellen ter berekening van haar benodigde solvabiliteit en/of economisch kapitaal om haar risico's te kunnen opvangen. • Inzichtelijke en gedegen systematiek voor de vaststelling van het gewenste solvabiliteitsniveau en/of economisch kapitaal. • In het risicomodel wordt rekening gehouden met alle significante risico's (ook niet-financieel) en alle facetten daarvan. • Risico's worden per organisatieonderdeel, per vergunning-houder gemodelleerd en geaggregeerd. • Het risicomodel is volgens best practice ontwikkeld en wordt frequent onderhouden, geëvalueerd en onafhankelijk gevalideerd. • In het risicomodel wordt veel aandacht besteed aan door-rekening van effecten van allerlei mogelijke scenario's, ook de scenario's met een kleine kans van optreden. • De voor de risicomodellering gehanteerde aannames en data zijn geheel gebaseerd op marktdata voor marktrisico's en interne ervaringscijfers voor andere risico's. • In het risicomodel wordt rekening gehouden met de (op grond van het beleid) in situaties van dreigende solvabiliteitstekorten toe te passen sturingsmiddelen (indexatiebeleid, premiebeleid, beleggingsbeleid). • Het model, voorzover afwijkend van de door DNB voor-geschreven parameters, is zeer uitgebreid gemotiveerd en door DNB getoetst en geaccepteerd. • De uitkomsten van de modelleringen worden in een risico-comité dan wel door de hoogste leiding goedgekeurd.	<u>Risicomodellering</u> • De instelling maakt gebruik van een eenvoudig intern model (of de door DNB voorgeschreven parameters) ter berekening van haar benodigde solvabiliteit en/of economisch kapitaal om haar risico's te kunnen opvangen. • Duidelijke systematiek voor de vaststelling van het gewenste solvabiliteitsniveau. • In het risicomodel wordt voldoende rekening gehouden met facetten van significante risico's. • Risico's zijn op instellingsniveau gemodelleerd. • Het risicomodel is volgens gebruikelijke methoden ontwikkeld en wordt periodiek geëvalueerd en onafhankelijk gevalideerd. • In het risicomodel wordt voldoende aandacht besteed aan doorrekening van effecten van allerlei mogelijke scenario's, ook de scenario's met een kleine kans van optreden. • De voor de risicomodellering gehanteerde aannames en data zijn gebaseerd op marktdata voor marktrisico en overwegend interne data; beperkt gebruik van externe data voor andere risico's. • In het risicomodel wordt voldoende rekening gehouden met de (op grond van het beleid) in situaties van (dreigende) solvabiliteitstekorten toe te passen sturingsmiddelen (indexatiebeleid, premiebeleid, beleggingsbeleid). • Het model, voorzover afwijkend van de door DNB voor-geschreven parameters, is door DNB getoetst en geaccepteerd. • De uitkomsten van de modelleringen worden door de hoogste leiding goedgekeurd.

1. Sterke beheersing (vervolg)	*2. Voldoende beheersing (vervolg)*
Vermogensanalyse • De meerjarenraming van de toekomstige financiële positie wordt frequent uitgevoerd. • De raming van de toekomstige financiële positie sluit volledig aan op meerjarenplannen en begrotingen en is gedetailleerd uitgevoerd. • De ontwikkeling van de werkelijke financiële positie ten opzichte van de gewenste en de vereiste solvabiliteitspositie wordt op maandbasis gevolgd. • Er wordt gesignaleerd indien sprake is van ongewenste ontwikkelingen en er wordt in een vroegtijdig stadium actie ondernomen. • Bij de analyse wordt gebruik gemaakt van diverse niveaus van urgentie teneinde de solvabiliteitspositie te karakteriseren. • Het hoogste management wordt direct geïnformeerd in geval van (toekomstig) dreigende solvabiliteitstekorten. • In de vermogensanalyse wordt rekening gehouden met grote/bijzondere transacties (fusies, overnames en dergelijke).	Vermogensanalyse • De meerjarenraming van de toekomstige financiële positie wordt met voldoende frequentie uitgevoerd. • De raming van de toekomstige financiële positie is op hoofdlijnen in lijn met meerjarenplannen en begrotingen. • De ontwikkeling van de werkelijke financiële positie ten opzichte van de gewenste en de vereiste solvabiliteitspositie wordt periodiek gevolgd. • Er wordt gesignaleerd indien sprake is van ongewenste ontwikkelingen en er wordt tijdig actie ondernomen. • Bij de analyse wordt gebruik gemaakt van een beperkt aantal niveaus van urgentie teneinde de solvabiliteitspositie te karakteriseren. • Het hoogste management wordt tijdig geïnformeerd in geval van (toekomstig) dreigende solvabiliteitstekorten. • In de vermogensanalyse wordt rekening gehouden met grote/bijzondere transacties (fusies, overnames en dergelijke).
Toegang tot kapitaal • Additionele middelen zijn op zeer korte termijn en tegen acceptabele voorwaarden aan te trekken. • Portefeuillesamenstelling is zodanig dat bezittingen gemakkelijk gesecuritiseerd kunnen worden. • Ruimschoots expertise aanwezig om proces van securitisatie adequaat uit te voeren. • Instelling voert frequent onderzoek uit naar mogelijkheden voor aanvullende financiering. • Binnen de groep is ruimschoots kapitaal aanwezig om dreigende solvabiliteitstekorten bij individuele vergunning-houders aan te vullen. • Kredietwaardigheid van de instelling is, exceptionele omstandigheden daargelaten, goed. • Uitstekende relaties met (potentiële) investeerders. • (Potentiële) investeerders zijn zeer kapitaalkrachtig.	Toegang tot kapitaal • Additionele middelen zijn op korte termijn en tegen acceptabele voorwaarden aan te trekken. • Portefeuillesamenstelling is zodanig dat bezittingen gesecuritiseerd kunnen worden. • Expertise aanwezig om proces van securitisatie adequaat uit te voeren. • Instelling voert periodiek onderzoek uit naar mogelijkheden voor aanvullende financiering. • Binnen de groep is voldoende kapitaal aanwezig om dreigende solvabiliteitstekorten bij individuele vergunninghouders aan te vullen. • Kredietwaardigheid van de instelling is, exceptionele omstandigheden daargelaten, voldoende. • Prima relatie met (potentiële) investeerders. • (Potentiële) investeerders zijn kapitaalkrachtig.

3. Onvoldoende beheersing	*4. Zwakke beheersing*
Beleid • Onduidelijk welk solvabiliteitsniveau aanvaardbaar geacht wordt. • Beleid grotendeels beperkt tot groepsniveau. • Het gewenste solvabiliteitsniveau wordt slechts afgeleid van de wettelijke norm, met inachtneming van een intern bepaalde beperkte veiligheidsmarge. • Solvabiliteitsnormen worden onvoldoende meegenomen bij prijsstelling van producten. • Summiere uitwerking van hoe te reageren in geval (van dreiging) van solvabiliteitstekorten (welke sturingsmiddelen, in welke mate, wanneer, effectiviteit). Geringe aandacht voor uitvoerbaarheid in de praktijk. Risicomodellering • De instelling maakt gebruik van een zeer eenvoudig intern model (of de door DNB voorgeschreven parameters) ter berekening van haar benodigde solvabiliteit en/of economisch kapitaal om haar risico's te kunnen opvangen. • Systematiek voor de vaststelling van het gewenste solvabiliteitsniveau en/of economisch kapitaal is op onderdelen onduidelijk. • In het risicomodel wordt soms geen rekening gehouden met (facetten van) significante risico's. • Risico's zijn grotendeels op groepsniveau gemodelleerd (derhalve nauwelijks op instellingsniveau). • Voor modellering wordt gebruik gemaakt van vuistregels of professional judgement, geen onafhankelijke validatie. • In het risicomodel wordt onvoldoende aandacht besteed aan doorrekening van effecten van allerlei mogelijke scenario's (ook scenario's met een kleine kans van optreden). • De voor de risicomodellering gehanteerde aannames en data zijn gebaseerd op marktdata voor marktrisico en overwegend externe data voor andere risico's. • In het risicomodel wordt onvoldoende rekening gehouden met de (op grond van het beleid) in situatie van (dreigende) solvabiliteitstekorten toe te passen sturingsmiddelen (indexatiebeleid, premiebeleid, beleggingsbeleid). • Het model, voorzover afwijkend van door DNB voorgeschreven parameters, is niet ter toetsing aan DNB voorgelegd dan wel niet goedgekeurd. • De uitkomsten van de modelleringen worden nauwelijks door de hoogste leiding goedgekeurd.	Beleid • Geen dan wel summier onderbouwd beleid inzake acceptabel geacht solvabiliteitsniveau. • Beleid uitsluitend op groepsniveau. • Het gewenste solvabiliteitsniveau wordt slechts afgeleid van de wettelijke norm, zonder inachtneming van een intern bepaalde veiligheidsmarge. • Bij prijsstelling producten wordt geen rekening gehouden met solvabiliteitsnormen. • Geen visie hoe te reageren in geval (van dreiging) van solvabiliteitstekorten.(welke sturingsmiddelen, in welke mate, wanneer, effectiviteit). Risicomodellering • De instelling maakt gebruik van een zeer eenvoudig intern model (of de door DNB voorgeschreven parameters) ter berekening van haar benodigde solvabiliteit en/of economisch kapitaal om haar risico's te kunnen opvangen. • Systematiek voor de vaststelling van het gewenste solvabiliteitsniveau en/of economisch kapitaal is onduidelijk. • In het risicomodel wordt onvoldoende rekening gehouden met significante risico's. • Risico's zijn uitsluitend op groepsniveau gemodelleerd, er wordt geen rekening gehouden met risico's op instellingsniveau. • Het risicomodel is niet volgens gebruikelijke methoden ontwikkeld dan wel wordt niet geëvalueerd en gevalideerd. • In het risicomodel wordt geen aandacht besteed aan doorrekening van effecten van allerlei mogelijke scenario's (ook scenario's met een kleine kans van optreden). • De voor de risicomodellering gehanteerde aannames en data zijn gebaseerd op marktdata en externe data, geen gebruik van interne data. • In het risicomodel wordt geen rekening gehouden met de (op grond van het beleid) in situaties van (dreigende) solvabiliteitstekorten toe te passen sturingsmiddelen. • Het gehanteerde model is niet door DNB getoetst dan wel geaccepteerd. • Uitkomsten van modelleringen worden niet door de hoogste leiding goedgekeurd.

3. Onvoldoende beheersing (vervolg)	*4. Zwakke beheersing (vervolg)*
Vermogensanalyse • De meerjarenraming van de toekomstige financiële positie wordt met een te lage frequentie uitgevoerd. • De raming van de toekomstige financiële positie is op belangrijke onderdelen niet in lijn met meerjarenplannen en begrotingen. • De ontwikkeling van de werkelijke financiële positie ten opzichte van de gewenste en de vereiste solvabiliteitspositie wordt met een lage frequentie gevolgd. • Er wordt niet tijdig gesignaleerd of er sprake is van ongewenste ontwikkelingen. • Bij de analyse wordt vrijwel geen gebruik gemaakt van een aantal niveaus van urgentie teneinde de solvabiliteitspositie te karakteriseren. • De hoogste leiding wordt te laat geïnformeerd in geval van (toekomstig) dreigende solvabiliteitstekorten. • In de vermogensanalyse wordt geen rekening gehouden met grote/bijzondere transacties (fusies, overnames en dergelijke).	Vermogensanalyse • Geen dan wel op ad-hocbasis een meerjarenraming van de toekomstige financiële positie. • De raming van de toekomstige financiële positie sluit niet goed aan op meerjarenplannen en begrotingen. • De ontwikkeling van de werkelijke financiële positie ten opzichte van de gewenste en de vereiste solvabiliteitspositie wordt niet dan wel op ad-hocbasis gevolgd. • Er wordt niet of veel te laat gesignaleerd of er sprake is van ongewenste ontwikkelingen. • Bij de analyse wordt geen gebruik gemaakt van een aantal niveaus van urgentie teneinde de solvabiliteitspositie te karakteriseren. • De hoogste leiding wordt niet of veel te laat geïnformeerd in geval van (toekomstig) dreigende solvabiliteitstekorten. • In de vermogensanalyse wordt rekening gehouden met grote/ bijzondere transacties (fusies, overnames en dergelijke).
Toegang tot kapitaal • Additionele middelen zijn niet op redelijk korte termijn aan te trekken en tegen deels ongunstige condities. • Portefeuillesamenstelling is zodanig dat bezittingen moeilijk gesecuritiseerd kunnen worden. • Onvoldoende expertise aanwezig om proces van securitisatie adequaat uit te voeren. • Instelling voert incidenteel onderzoek uit naar mogelijkheden voor aanvullende financiering. • Binnen de groep is in beperkte mate kapitaal aanwezig om dreigende solvabiliteitstekorten bij individuele vergunninghouders aan te vullen. • Kredietwaardigheid van de instelling is, exceptionele omstandigheden daargelaten, onvoldoende. • Relatie met (potentiële) investeerders voor verbetering vatbaar. • Onduidelijkheid over vermogenspositie (potentiële) investeerders.	Toegang tot kapitaal • Additionele middelen zijn niet of pas op lange termijn aan te trekken en tegen ongunstige condities. • Bezittingen kunnen niet gesecuritiseerd worden. • Geen expertise aanwezig om proces van securisatie adequaat uit te voeren. • Instelling verricht geen onderzoek naar mogelijkheden voor aanvullende financiering. • Binnen de groep is geen kapitaal aanwezig om dreigende solvabiliteitstekorten bij individuele vergunninghouders aan te vullen. • Kredietwaardigheid van de instelling is onvoldoende. • Slechte relatie met (potentiële) investeerders. • (Potentiële) investeerders zijn niet kapitaalkrachtig.

D14 BEHEERSINGSCATEGORIE: LIQUIDITEITSBEHEER

Beoordeel de risicomitigerende werking van liquiditeitsbeheer.
Kies de score die het beste de kwaliteit van de beheersingsmaatregelen weergeeft. Hierbij hoeft niet steeds aan alle geformuleerde criteria voldaan te worden. Het is aan de toezichthouder om te beoordelen welke criteria de doorslag geven bij de toekenning van een score.

Items van de beheersingscategorie liquiditeitsbeheer:
- beleid;
- modellering;
- positiemonitoring;
- crisismanagement;
- toegang tot de geldmarkt.

Definitie van de items:

Beleid
De mate waarin de instelling beleid heeft ontwikkeld ten aanzien van:
- het gewenste liquiditeitsniveau (omvang en samenstelling);
- de relatie van het gewenste liquiditeitsniveau met wettelijke eisen;
- de wijze waarop men wenst te reageren in geval van (dreigende) liquiditeitstekorten (contingency planning).

Modellering
De mate waarin en de wijze waarop sprake is van:
- adequate modellering van risico's;
- adequate scenario's (waaronder stress testing) ten aanzien van deze risico's;
- adequate en realistische aannames en uitgangspunten gericht op de berekening van de liquiditeitsbehoefte als mede de analyse van deze liquiditeitsbehoefte versus de aanwezige liquiditeit.

Positiemonitoring
De wijze waarop en de mate waarin de ontwikkeling van de werkelijke liquiditeitspositie ten opzichte van de gewenste/vereiste liquiditeitspositie (beide zowel met betrekking tot het heden als met betrekking tot de toekomstverwachting) adequaat wordt bewaakt, eventuele signalen in deze tijdig worden afgegeven en waar nodig tijdig actie wordt ondernomen.

Crisismanagement
De mate waarin de instelling adequate maatregelen heeft getroffen die in werking treden bij een (dreigend) liquiditeitstekort.

Toegang tot de geldmarkt
De mate waarin de instelling mogelijkheden heeft om, indien nodig, tijdig en tegen acceptabele voorwaarden liquide middelen voor de korte termijn aan te trekken, teneinde in de reguliere liquiditeitsbehoefte te kunnen voorzien dan wel om de aanwezige liquiditeit te kunnen sturen.

Beoordelingscriteria

1. Sterke beheersing	*2. Voldoende beheersing*
<u>Beleid</u> • Heldere uiteenzetting op gedetailleerd niveau welk liquiditeitsprofiel aanvaardbaar geacht wordt. • Beleid afgestemd op de complexiteit van de organisatie (in termen van internationale vertakkingen, off balance sheet activiteiten, rol in CP-conduits en securitisatieverhikels, liquiditeitmismatch per valuta, vergunninghouders, productgroepen, et cetera). • Het gewenste liquiditeitsprofiel wordt niet alleen afgeleid van de wettelijke norm, maar ook van eigen onderbouwde interne normen (in termen van risk governance, richtlijnen, limieten, gewenste liquiditeitspositie, concentraties, stress events, risicotolerantie, et cetera). • Gedetailleerde inkadering contingencyplanning: hoe te reageren in geval (van dreiging) van liquiditeitstekorten (welke sturingsmiddelen, in welke mate, wanneer, effectiviteit van maatregelen). • Gedetailleerde inkadering van intraday liquiditeitmanagement (inzichtelijkheid belangrijkste bronnen en lekken van liquiditeit).	<u>Beleid</u> • Duidelijke uiteenzetting op hoofdlijnen welk liquiditeitsprofiel aanvaardbaar geacht wordt. • Beleid voldoende afgestemd op de complexiteit van de organisatie. • Het gewenste liquiditeitsprofiel wordt niet alleen afgeleid van de wettelijke norm, maar ook van eigen onderbouwde interne normen. • Inkadering contingency planning op hoofdlijnen. Toepassing van de maatregelen in de praktijk is realistisch. • Inkadering intraday liquiditeitmanagement op hoofdlijnen.
<u>Modellering</u> • De liquiditeitsraming en stressscenario's zijn gebaseerd op goed onderbouwde aannames en uitgangspunten en omvatten alle on/off balance activiteiten van de instelling. • De liquiditeitsraming en stressscenario's zijn volgens gebruikelijke methoden ontwikkeld en worden frequent onderhouden, geëvalueerd en gevalideerd. • De voor de liquiditeitsraming en stressscenario's gehanteerde aannames en data zijn grotendeels gebaseerd op eigen ervaringscijfers en benchmarks (peers). • De uitkomsten van de liquiditeitsraming en stressscenario's vormen een adequate afspiegeling voor de liquiditeitsbuffers van de instelling. • De uitkomsten van de liquiditeitsraming en stressscenario's zijn in een risicocomité dan wel door de hoogste leiding goedgekeurd.	<u>Modellering</u> • De liquiditeitsraming en stressscenario's zijn gebaseerd op redelijk onderbouwde aannames en uitgangspunten en omvatten alle belangrijke on/off balance activiteiten van de instelling. • De liquiditeitsraming en stressscenario's zijn volgens gebruikelijke methoden ontwikkeld en worden periodiek onderhouden, geëvalueerd en gevalideerd. • De voor de liquiditeitsraming en stressscenario's gehanteerde aannames en data zijn gebaseerd op eigen ervaringscijfers en marktdata. • De uitkomsten van de liquiditeitsraming en stressscenario's vormen een redelijke afspiegeling voor de liquiditeitsbuffers van de instelling. • De uitkomsten van de liquiditeitsraming en stressscenario's zijn door de hoogste leiding goedgekeurd.
<u>Positiemonitoring</u> • De raming van de toekomstige liquiditeitspositie wordt op maandbasis uitgevoerd. • De instelling rekent periodiek stressscenario's (onderscheiden naar marktbrede liquiditeitscrisis en instellingspecifieke crisis) door. • De ontwikkeling van de werkelijke liquiditeitspositie ten opzichte van de gewenste en de vereiste liquiditeitspositie wordt op dagbasis gevolgd. • Er wordt gesignaleerd indien sprake is van ongewenste ontwikkelingen en er wordt in een vroegtijdig stadium actie ondernomen. • Bij de signalering wordt gebruikgemaakt van diverse niveaus van urgentie teneinde het liquiditeitsprofiel te karakteriseren. • Het hoogste management wordt direct geïnformeerd in geval van (toekomstig) dreigende liquiditeitstekorten.	<u>Positiemonitoring</u> • De raming van de toekomstige liquiditeitspositie wordt meestal op maandbasis uitgevoerd. • De instelling rekent periodiek stressscenario's door. • De ontwikkeling van de werkelijke liquiditeitspositie ten opzichte van de gewenste en de vereiste liquiditeitspositie wordt meestal op dagbasis gevolgd. • Er wordt gesignaleerd indien sprake is van ongewenste ontwikkelingen en er wordt tijdig actie ondernomen. • Bij de signalering wordt gebruikgemaakt van een beperkt aantal niveaus van urgentie teneinde het liquiditeitsprofiel te karakteriseren. • Het hoogste management wordt tijdig geïnformeerd in geval van (toekomstig) dreigende liquiditeitstekorten.

1. Sterke beheersing (vervolg)	*2. Voldoende beheersing (vervolg)*
Crisismanagement • De instelling beschikt over een goed gedocumenteerd en geïmplementeerd liquidity contingency draaiboek. • Een adequaat en actueel communicatiedraaiboek is voorhanden. • De instelling beschikt over ruim voldoende beleenbare activa ter belening bij liquiditeitsverschaffers. • In productvoorwaarden zijn aanzienlijke uitstroombeperkende maatregelen opgenomen ter beperking van de opvraagbaarheid van door de instelling aangetrokken gelden. • In de leningvoorwaarden (hypotheken, creditcardvorderingen) zijn clausules opgenomen voor eventuele doorverkoop aan derde partijen • De noodprocedures worden frequent getest en geëvalueerd.	Crisismanagement • De instelling beschikt over een redelijk gedocumenteerd en geïmplementeerd liquidity contingency draaiboek • Een redelijk actueel communicatiedraaiboek is voorhanden. • De instelling beschikt over voldoende beleenbare activa ter belening bij liquiditeitsverschaffers. • In productvoorwaarden zijn meestal uitstroombeperkende maatregelen opgenomen ter beperking van de opvraagbaarheid van door de instelling aangetrokken gelden. • In de leningvoorwaarden (hypotheken, creditcardvorderingen) zijn meestal clausules opgenomen voor eventuele doorverkoop aan derde partijen • De noodprocedures worden periodiek getest en geëvalueerd.
Toegang tot de geldmarkt • Instelling voert frequent analyse uit naar gebruik van verschillende fundingbronnen. • Sprake van aanzienlijke spreiding van de fundingbehoefte over liquiditeitsverschaffers, instrumenten en markten en regio's. • Goede mate van disclosure en reputatie-opbouw naar liquiditeitverschaffers (banken, beleggers, tegenpartijen) en ratingagencies. • Additionele middelen zijn op korte termijn en tegen gunstige voorwaarden aan te trekken.	Toegang tot de geldmarkt • Instelling voert periodiek analyse uit naar gebruik van verschillende fundingbronnen. • Sprake van voldoende spreiding van de fundingbehoefte over liquiditeitsverschaffers, instrumenten en markten en regio's. • Redelijke mate van disclosure en reputatie-opbouw naar liquiditeitverschaffers (banken, beleggers, tegenpartijen) en ratingagencies. • Additionele middelen zijn op korte termijn en tegen acceptabele voorwaarden aan te trekken.

3. Onvoldoende beheersing	*4. Zwakke beheersing*
Beleid • Onduidelijk welk liquiditeitsprofiel aanvaardbaar geacht wordt. • Beleid onvoldoende afgestemd op de complexiteit van de organisatie. • Het gewenste liquiditeitsprofiel slechts afgeleid van de wettelijke norm, met inachtneming van een intern bepaalde beperkte veiligheidsmarge. • Summiere inkadering contingency planning. Geringe aandacht voor uitvoerbaarheid in de praktijk. • Summiere inkadering intraday liquiditeitmanagement.	Beleid • Geen dan wel summier onderbouwd beleid inzake acceptabel geacht liquiditeitsprofiel. • Beleid nauwelijks afgestemd op de complexiteit van de organisatie. • Het gewenste liquiditeitsprofiel slechts afgeleid van de wettelijke norm, zonder inachtneming van een intern bepaalde veiligheidsmarge. • Geen inkadering contingencyplanning. • Geen inkadering intraday liquiditeitmanagement.
Modellering • De liquiditeitsraming en stressscenario's zijn gebaseerd op onvoldoende onderbouwde aannames en uitgangspunten. • Voor liquiditeitsraming en stressscenario's wordt gebruik-gemaakt van vuistregels of professional judgement.. • De voor de liquiditeitsraming en stressscenario's gehanteerde aannames en data zijn grotendeels gebaseerd op marktdata. • De uitkomsten van de liquiditeitsraming en stressscenario's vormen in onvoldoende mate een afspiegeling voor de liquiditeitsbuffers van de instelling. • De uitkomsten van de liquiditeitsraming en stressscenario's worden nauwelijks door de hoogste leiding goedgekeurd.	Modellering • De liquiditeitsraming en stressscenario's zijn gebaseerd op slecht onderbouwde aannames en uitgangspunten. • Liquiditeitsraming en stressscenario's zijn niet volgens gebruikelijke methoden ontwikkeld dan wel worden niet geëvalueerd. • De voor de liquiditeitsraming en stressscenario's gehanteerde aannames en data zijn gebaseerd op marktdata. • De uitkomsten van de liquiditeitsraming en stressscenario's vormen een slechte afspiegeling voor de liquiditeitsbuffers van de instelling. • De uitkomsten van de liquiditeitsraming en stressscenario's worden niet door de hoogste leiding goedgekeurd.
Positiemonitoring • De raming van de toekomstige liquiditeitspositie wordt met een te lage frequentie uitgevoerd. • De instelling rekent incidenteel stressscenario's door. • De ontwikkeling van de werkelijke liquiditeitspositie ten opzichte van de gewenste en de vereiste liquiditeitspositie wordt met een te lage frequentie gevolgd. • Er wordt niet tijdig gesignaleerd of er sprake is van ongewenste ontwikkelingen. • Bij de signalering wordt vrijwel geen gebruik gemaakt van een aantal niveaus van urgentie teneinde het liquiditeitsprofiel te karakteriseren. • Het hoogste management wordt te laat geïnformeerd in geval van (toekomstig) dreigende liquiditeitstekorten.	Positiemonitoring • Geen dan wel op ad-hocbasis een raming van de toekomstige liquiditeitspositie. • De instelling rekent geen stressscenario's door. • De ontwikkeling van de werkelijke liquiditeitspositie ten opzichte van de gewenste en de vereiste liquiditeitspositie wordt niet dan wel op ad-hocbasis gevolgd. • Er wordt niet of veel te laat gesignaleerd of er sprake is van ongewenste ontwikkelingen. • Bij de signalering wordt geen gebruik gemaakt van een aantal niveaus van urgentie teneinde het liquiditeitsprofiel te karakteriseren. • Het hoogste management wordt niet of veel te laat geïnformeerd in geval van (toekomstig) dreigende liquiditeits-tekorten.

3. Onvoldoende beheersing (vervolg)	*4. Zwakke beheersing (vervolg)*
Crisismanagement • De instelling beschikt over een in onvoldoende mate gedocumenteerd en geïmplementeerd liquidity contingency draaiboek. • Een verouderd communicatiedraaiboek is voorhanden. • De instelling beschikt over onvoldoende beleenbare activa ter belening bij liquiditeitsverschaffers. • In productvoorwaarden zijn incidenteel uitstroombeperkende maatregelen opgenomen ter beperking van de opvraagbaarheid van door de instelling aangetrokken gelden. • In de leningvoorwaarden (hypotheken, creditcardvorderingen) zijn incidenteel clausules opgenomen voor eventuele door-verkoop aan derde partijen • De noodprocedures worden incidenteel getest en geëvalueerd.	Crisismanagement • De instelling beschikt over slecht gedocumenteerd en geïmplementeerd liquidity contingency draaiboek. • Een communicatiedraaiboek is niet voorhanden. • De instelling beschikt vrijwel niet over beleenbare activa ter belening bij liquiditeitsverschaffers. • In productvoorwaarden zijn geen uitstroombeperkende maatregelen opgenomen ter beperking van de opvraagbaarheid van door de instelling aangetrokken gelden. • In de leningvoorwaarden (hypotheken, creditcard vorderingen) zijn geen clausules opgenomen voor eventuele doorverkoop aan derde partijen • De noodprocedures worden niet getest en geëvalueerd.
Toegang tot de geldmarkt • Instelling voert incidenteel analyse uit naar gebruik van verschillende fundingbronnen. • Sprake van onvoldoende spreiding van de fundingbehoefte over liquiditeitsverschaffers, instrumenten en markten en regio's. • Onvoldoende sprake van disclosure en reputatie-opbouw naar liquiditeitverschaffers (banken, beleggers, tegenpartijen) en ratingagencies. • Additionele middelen zijn moeilijk op korte termijn en tegen acceptabele voorwaarden aan te trekken.	Toegang tot de geldmarkt • Instelling voert geen analyse uit naar gebruik van verschillende fundingbronnen. • Nauwelijks sprake van spreiding van de fundingbehoefte over liquiditeitsverschaffers, instrumenten en markten en regio's. • Nauwelijks sprake van disclosure en reputatie-opbouw naar liquiditeitverschaffers (banken, beleggers, tegenpartijen) en ratingagencies. • Additionele middelen zijn niet op korte termijn en tegen acceptabele voorwaarden aan te trekken.