DeNederlandscheBank
EUROSYSTEEM

Woordenlijst bij SBA-ORM

Woord	Betekenis, uitleg, toelichting
Assurancerapport	ISAE3402-rapport of ISAE3000-rapport of vergelijkbaar, dat inzicht geeft in de werking van beheersmaatregelen. Wij bedoelen hier geen ISO certificering, omdat deze betrekking heeft op werking van een 'managementsysteem' en niet direct assurance verschaft over de werking van specifieke beheersmaatregelen.
BCP	Business Continuity Plan
Bedrijfskosten	Het totaal aan personeels-, bestuurs- en governance-, administratie- en ICT-, vermogensbeheers-, advies- en controle-, uitbestedingskosten en afschrijvingen op bedrijfsmiddelen. Kosten die betrekking hebben op het sluiten van verzekeringsovereenkomsten (acquisitiekosten) en kosten die betrekking hebben op herverzekering zijn hier niet onder begrepen. De mate waarin de hier bedoelde kosten al dan niet verhaalbaar zijn op klanten of opdrachtgevers is voor deze opgaaf niet relevant.
Beleid	Document of samenstel van documenten met interne richtlijnen over de beheersing en/of uitvoering van een bepaald onderwerp. Elementen die typisch in het beleid over een onderwerp worden uitgewerkt zijn: doelstelling van het beleid; definities van de belangrijkste begrippen; reikwijdte van het beleid; datum en status van het beleid; inhoudelijke bepalingen over taken, verantwoordelijkheden en bevoegdheden, of verwijzingen daarnaar; instructies en/of richtlijnen en/of procesbeschrijvingen over uitvoering daarvan, of verwijzingen daarnaar; relevante indicatoren en normen, of verwijzingen daarnaar. Het beleid over een onderwerp kan zijn samengesteld uit meerdere documenten die elk een eigen reikwijdte hebben (bijvoorbeeld groepsbreed en uitwerkingen per bedrijfsonderdeel).
Bestuur (zie ook: Directie)	Het orgaan binnen de instelling dat eindverantwoordelijk is voor het dagelijkse bestuur ervan. Bij vezekeraars, ppi's en pensioenuitvoeringsorganisaties is dat in de regel de Raad van bestuur of Directie, bij pensioenfondsen is dat in de regel het pensioenfondsbestuur.
Compliancefunctie	De functie binnen de instelling die belast is met kaderstelling, facilitering, monitoring en rapportage op het gebied van compliance.
Data directory	Een bestand waarin (kritieke) data elementen op eenduidige wijze zijn beschreven, zoals bijvoorbeeld de definitie van het data element, de karakteristieken van de data, de bron en het doelbestand van de data, de data eigenaar en (indien van toepassing) verwijzing naar de QRT.
Data element	Gegevenseenheid die - in haar specifieke context - als ondeelbaar wordt beschouwd. Dit begrip wordt ook wel aangeduid met kenmerk, attribuut, of veld.
Datakwaliteit	De mate waarin de data aantoonbaar geschikt, accuraat en volledig is en voldoet aan intern en extern gestelde normen.
Directie (zie ook: Bestuur)	Het orgaan binnen de instelling dat eindverantwoordelijk is voor het dagelijkse bestuur ervan. Bij vezekeraars, ppi's en pensioenuitvoeringsorganisaties is dat in de regel de Raad van bestuur of Directie, bij pensioenfondsen is dat in de regel het pensioenfondsbestuur.

End Using Computing toepassingen	End User Computing toepassingen zijn applicaties die door eindgebruikers zijn gebouwd met behulp van bijvoorbeeld spreadsheet-programma's en/of rapportgeneratoren. End User Computing toepassingen vallen in de regel buiten het bereik van IT beheersingsmaatregelen.
GRC-applicatie	Een applicatie om de governance, risk management en compliance van de organisatie te ondersteunen.
Instelling	Een onder toezicht van DNB staande financiële onderneming zoals bedoeld in art.1.1 Wft danwel een onder toezicht van DNB staand pensioenfonds, algemeen pensioenfonds, bedrijfstakpensioenfonds of ondernemingspensioenfonds zoals bedoeld in artikel 1.1 Pw danwel een pensioenuitvoeringsorganisatie (die niet onder direct toezicht staat).
Interne auditfunctie	De Interne Auditfunctie is een onafhankelijke functie die zekerheid en advies verschaft aan het management van een organisatie teneinde waarde toe te voegen aan de organisatie en de processen in de organisatie te verbeteren. De functie helpt om de organisatie haar doelstelling te bereiken door middel van een systematische en gedisciplineerde benadering van het evalueren en verbeteren van de effectiviteit van risico management, interne beheersing en governance processen.
Interne Controle Systeem	Het samenstel van beleid, procedures, instrumenten en maatregelen waarmee een organisatie zekerheid tracht te verkrijgen over de effectiviteit en efficiëntie alsmede de risicobeheersing van de bedrijfsprocessen.
Key risico	Een risico dat als 'key' of belangrijk is aangemerkt. Typisch ligt aan de kwalificatie als key risico een analyse ten grondslag op basis van beleidsmatig vastgestelde criteria.
Key person risk	Het risico op directe of indirecte verliezen of niet-gerealiseerde voordelen als gevolg van verminderde beschikbaarheid van medewerkers met specifieke domeinkennis, -ervaring of -competenties. Key person risk treedt typisch op indien de instelling afhankelijk is van een beperkt aantal medewerkers wier kennis, ervaring of competenties cruciaal zijn voor het bereiken van organisatiedoelstellingen.
Kosten van uitbestedingen	De kosten van alle uitbestedingen (zie bij 'uitbesteding' voor de definitie van dat begrip) waaronder begrepen de door dienstverleners gefactureerde bedragen (vast en variabel, naar het verslagjaar gealloceerd) alsook de interne kosten voor beheersing van die uitbestedingen. Het gaat om de kosten van uitbestedingen (zowel kritieke als niet kritieke), niet om inkoop.
Kritiek bedrijfsproces	Bedrijfsproces dat als kritiek is aangemerkt voor de kwaliteit en continuïteit van de dienstverlening aan de klant, voor de financiële resultaten en/of voor de reputatie van de instelling. Een verstoring of onjuiste uitvoering van een kritiek bedrijfsproces zou een grote impact kunnen hebben op de dienstverlening, resultaten of reputatie. Typisch ligt aan de kwalificatie als kritiek bedrijfsproces een analyse ten grondslag op basis van beleidsmatig vastgestelde criteria.
Kritiek data-element	Data element dat als kritiek is aangemerkt voor de kwaliteit van de financiële rapportages of andere relevante informatie/ berekeningen/bedrijfsprocessen. Typisch ligt aan de kwalificatie als kritiek data-element een analyse ten grondslag op basis van beleidsmatig vastgestelde criteria.

Kritieke (onder)uitbesteding / kritieke of belangrijke (onder)uitbesteding	(Onder)uitbesteding van bedrijfsactiviteiten die als belangrijk en/of kritiek zijn aangemerkt conform de beschrijving in de Good Practice Uitbesteding verzekeraars. Het betreffen die activiteiten die fundamenteel zijn voor het vermogen van de instelling om haar kernactiviteit uit te kunnen oefenen. Zie ook richtsnoer 60 EIOPA Guidelines on system of Governance.
Management Letter	Rapport van de certificerend externe accountant waarin aandachtspunten ten aanzien van de interne beheersing, die geconstateerd zijn bij de jaarrekeningcontrole, aan het management van de organisatie worden gerapporteerd.
Operationeel risico / Operationele risico's	Het risico op directe of indirecte verliezen of niet-gerealiseerde voordelen als gevolg van het falen of tekortschieten van mensen, processen , systemen en technologie, en/of als gevolg van onverwachte externe gebeurtenissen
Operationeel stress scenario	Een hypothetisch ingrijpend maar plausibel (severe but plausible) scenario waarin één of meerdere operationele risico's met grote impact manifest worden.
Registraties / registratiesystemen	Geordende opsomming waarin gegevens over zaken of begrippen worden bijgehouden. De verschijningsvorm is niet relevant. In de context van deze Vragenlijst kan bijvoorbeeld gedacht worden aan een risicoregister of een incidentenregister of een register van bedrijfsprocessen.
Risicobeheerfunctie of risicomanagementfunctie	De functie binnen de instelling die belast is met kaderstelling, facilitering, monitoring en rapportage op het gebied van risicomanagement.
Risicobereidheid	De risicobereidheid gaat over de aard, omvang en mate waarin een organisatie bereid is risico's te lopen bij het realiseren van haar doelstellingen. Dit begrip wordt ook wel aangeduid met de Engelse term Risk Appetite.
Risicocategorie	Algemene typering en/of classificatie van op elkaar gelijkende risico's bijvoorbeeld (maar niet beperkt tot) op basis van (i) min-of-meer vergelijkbare oorzaken en/of (ii) min-of-meer vergelijkbare vergelijkbare beheersingstechnieken, (iii) typisch voorkomen in dezelfde bedrijfsfunctie.
Risicomanagementfunctie of risicobeheerfunctie	De functie binnen de instelling die belast is met kaderstelling, facilitering, monitoring en rapportage op het gebied van risicomanagement.
Risicotaxonomie	Opsomming en (mogelijk hiërarchische) ordening van onderling uitsluitende en gezamenlijk omvattende (MECE: mutually exclusive and collectively exhaustive) risicocategorieën.
Security agreement	Een overeenkomst tussen een uitbestedende instelling en een dienstverlener over het gewenste beveiligingsniveau dat de dienstverlener dient in te regelen voor de beveiliging van data, netwerk, infrastructuur en systemen van de uitbestedende instelling.
Service Level Agreement	Een schriftelijke overeenkomst tussen de aanbieder en de afnemer van welbepaalde diensten en/of producten, waarin afspraken zijn gemaakt tussen beide partijen omtrent het niveau van dienstverlening en/of de kwaliteitsaspecten van het product.
SLA	Service Level Agreement

Uitbesteding	Het verlenen van een opdracht aan een derde tot het ten behoeve van die financiële onderneming verrichten van werkzaamheden (1) die deel uitmaken van of voortvloeien uit het uitoefenen van haar bedrijf of het verlenen van financiële diensten; of (2) die deel uitmaken van de wezenlijke bedrijfsprocessen ter ondersteuning daarvan