



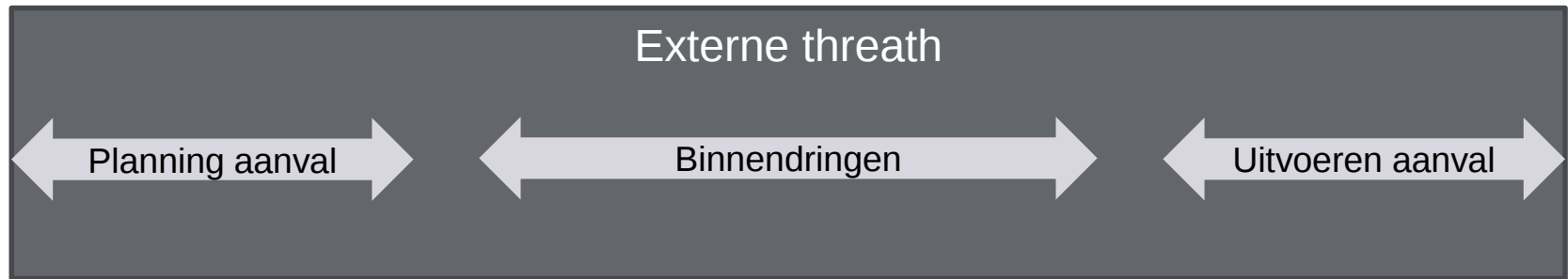
Digitaal veilig pensioenfonds Digitaal veilig uitbesteden

Gerrit Liefers

6 oktober 2020

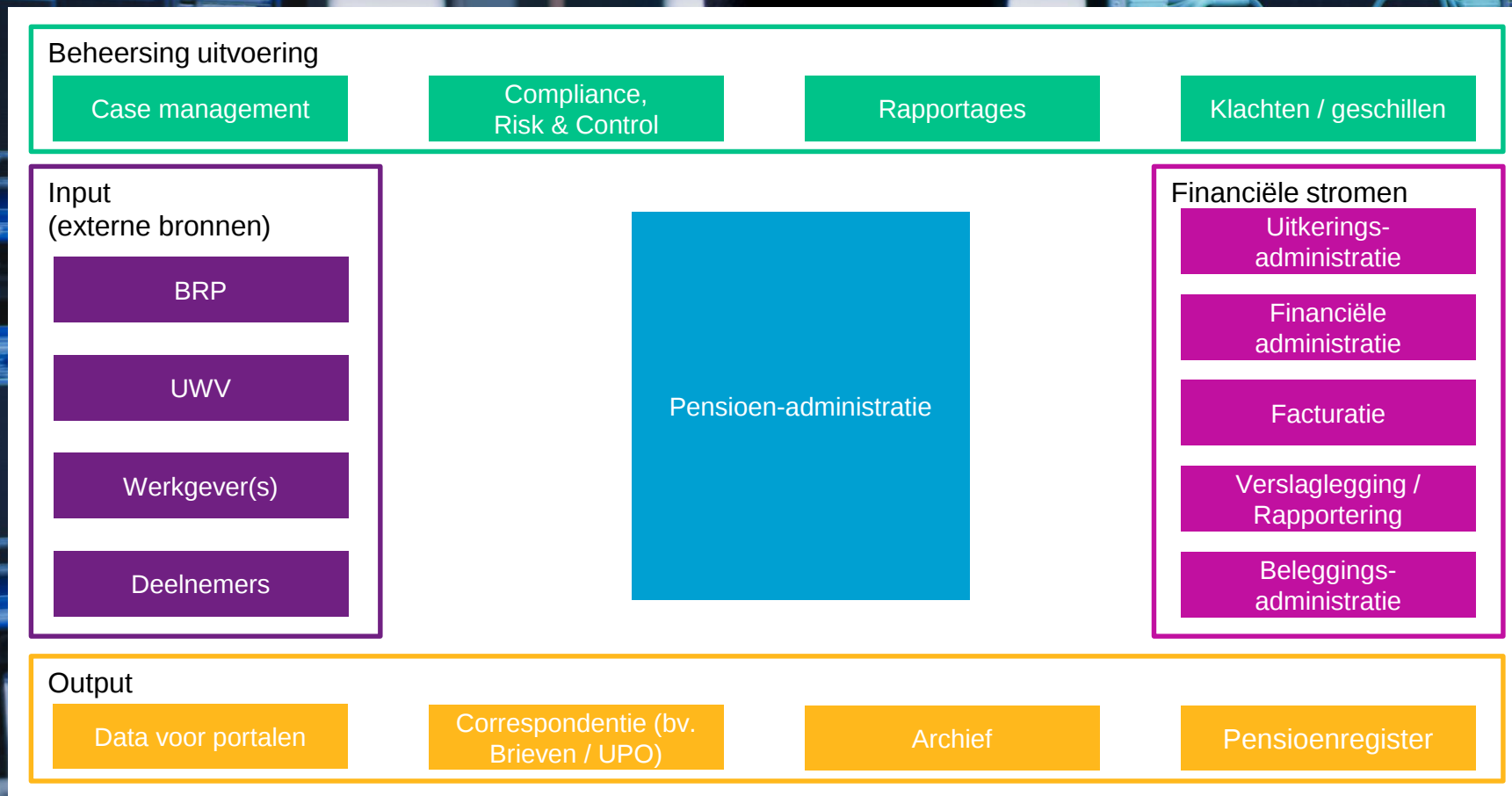
Achtergrond

Cyber security – beheersing



Uitbesteding: Voorbeeld van een keten pensioenbeheer

Gestileerd landschap en relaties naar “de buitenwereld”.



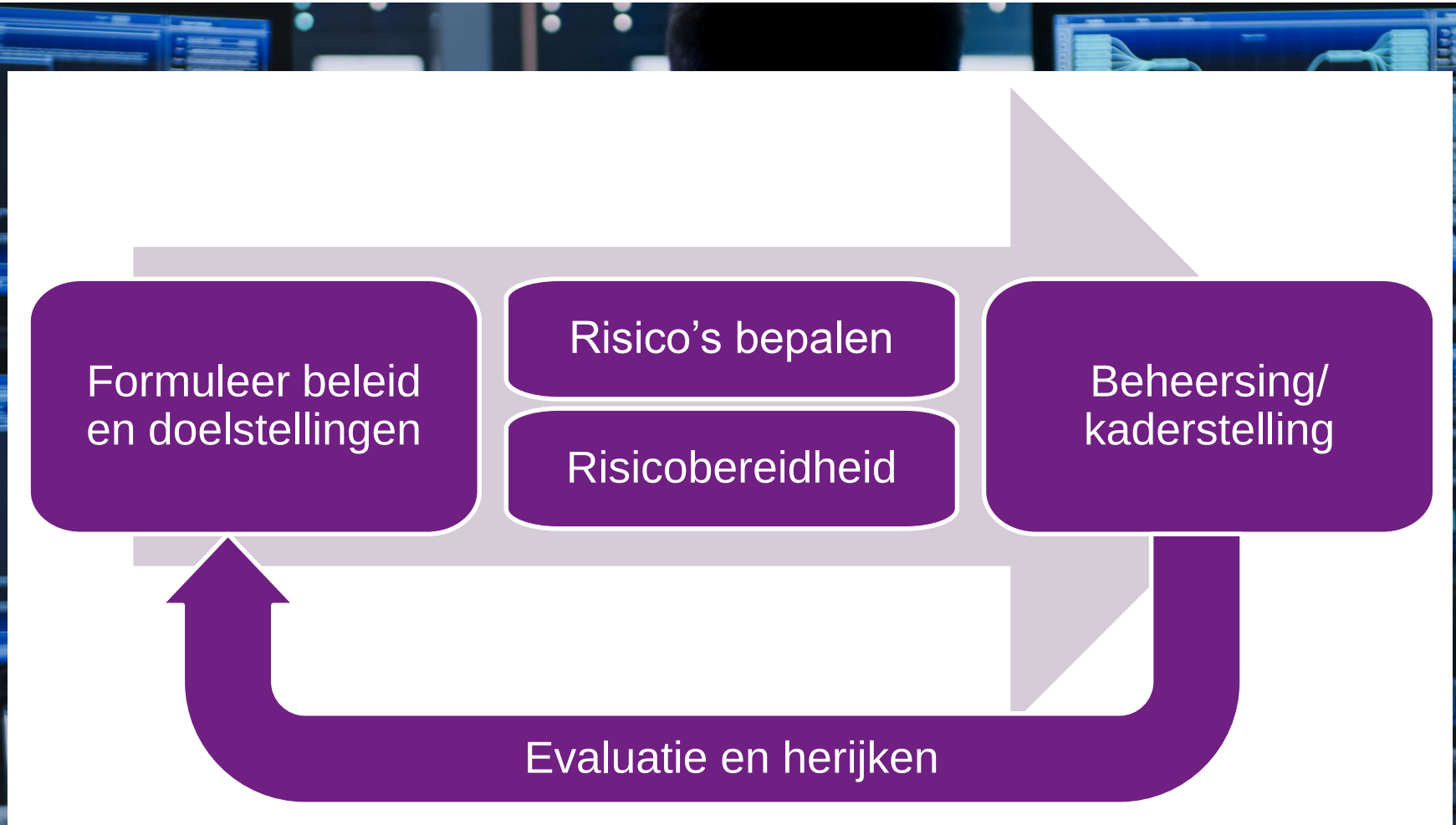
Agenda

Stappen bij uitbesteding



Uitbesteding en risicobeheersing

Samenhang tussen stappen 1 t/m 3



Stap 2 risicobeeld: Doelstellingen en risicobereidheid IT (1)

Voorbeeld a.d.h.v. BIV classificatie

BIVA	Classificatie
Beschikbaarheid Availability	0 - Niet nodig
	1 - Belangrijk
	2 - Noodzakelijk
	3 - Essentieel
Integriteit Accuracy	0 - Niet zeker
	1 - Beschermd
	2 - Hoog
	3 - Absoluut
Vertrouwelijkheid Access	0 - Openbaar
	1 - Bedrijfsvertrouwelijk
	2 - Vertrouwelijk
	3 - Geheim
Aanpasbaarheid Agility	0 - Standaard
	1 - Innovatief
	2 - Onderscheidend
	3 - Compliance

Stap 2 risicobeeld: Doelstellingen en risicobereidheid IT (2)

Voorbeeld risicobereidheid; beschikbaarheid

Onderdeel administratie	Score	Risicobereidheid
Deelnemersadministratie	1	De deelnemersadministratie is belangrijk, maar kan er even uitliggen
Uitkeringsadministratie	2	De uitkeringsadministratie is een geval apart; op de dagen dat moet worden uitgekeerd moet deze beschikbaar zijn
Handelssysteem vermogensbeheerder, actief beleid	3	Dit systeem is essentieel tijdens de handelsuren; mag er eigenlijk nooit uitliggen

Classificatie
0 - Niet nodig
1 - Belangrijk
2 - Noodzakelijk
3 - Essentieel

Stap 2 risicobeeld: Bepaling risico's; voorbeeld incidenten

Beheersing bij uitbesteding



Stap 3: Kaderstelling

Maak gebruik van de Good Practice IB DNB

Good Practice

Informatiebeveiliging 2019/2020

DeNederlandscheBank

EUROSYSTEEM

Voorbeeld onderwerpen kader Governance

1.1 Information Security plan

1.2 IT Policies Management

2.1 Enterprise Information Architecture Model

2.2 Data classification scheme

3.1 Monitor future trends and regulations

3.2 Technology standards

Stap 4 en 5: Contract, SLA en Monitoring uitbesteding

Beheersingsmaatregelen



Supplier risk management



Internal control at third parties

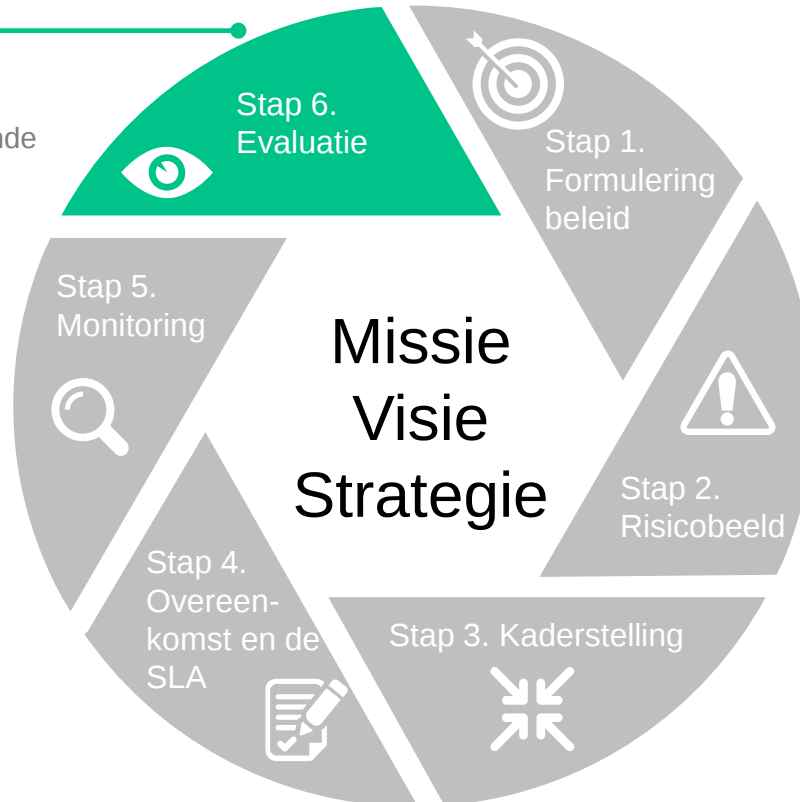


Monitoring and reporting of Service Level Achievements

Samenvatting en vragen

Stap 6 - Evaluatie:

Evalueer (jaarlijks) grondig (veranderende omgeving, veranderende organisatie etc.) Loop alle stappen door.





Gerrit Liefers

Senior consultant
M +31 (0)65 129 2768
gerrit.liefers@willistowerswatson.com



Jobine Kersseboom

Senior consultant
M +31 (0)65 182 9730
jobine.kersseboom@willistowerswatson.com

Bijlage bij stap 2 risicobeeld: Risicobereidheid IT

Voorbeeld a.d.h.v. BIV classificatie

BIVA	Classificatie	Criteria
Beschikbaarheid Availability Het binnen een redelijke tijdstermijn kunnen raadplegen of wijzigen van gegevens wanneer dit bij het uitvoeren van werkzaamheden nodig is, ofwel het draaiend houden van bestaande processen en het herstellen van verstoringen, waarbij de negatieve gevolgen van incidenten (uitval, beveiligingslekken) worden beperkt.	0 - Niet nodig	De informatie of het bedrijfsproces kan zonder gevolgen langere tijd niet beschikbaar zijn. Schending van beschikbaarheid heeft geen gevolgschade.
	1 - Belangrijk	De informatie of het bedrijfsproces staat incidentele uitval toe. De continuïteit zal op redelijke termijn moeten worden hervat. Schending van deze classificatie kan enige schade toebrengen aan de bedrijfsvoering en/of het imago (reputatie) van de organisatie en/of haar klanten en betrokkenen.
	2 - Noodzakelijk	De informatie of het bedrijfsproces zou niet mogen uitvallen; uitval is nauwelijks toegestaan. De beschikbaarheid zal snel moeten worden hervat. Schending van deze classificatie kan serieuze schade toebrengen aan de bedrijfsvoering en/of het imago (reputatie) van de organisatie en/of haar klanten en betrokkenen.
	3 - Essentieel	De informatie of het bedrijfsproces staat eigenlijk geen uitval toe. De beschikbaarheid zal zeer snel moeten worden hervat. Schending van de classificatie kan zeer grote schade toebrengen aan de bedrijfsvoering en/of het imago (reputatie) van de organisatie en/of haar klanten en betrokkenen.
Integriteit Accuracy Het in overeenstemming zijn van gegevens met het afgebeelde deel van realiteit en dat niets ten onrechte is achtergehouden of verdwenen, i.c. de aspecten juistheid, volledigheid en tijdigheid, ofwel het opleveren van juiste, tijdige en volledige informatie aan alle relevante belanghebbenden.	0 - Niet zeker	Deze informatie mag worden veranderd. Geen extra bescherming van integriteit noodzakelijk. Schending van integriteit heeft geen gevolgschade.
	1 - Beschermd	De informatie of het bedrijfsproces heeft geen directe hinder van (integriteits)fouten. Een basisniveau van bescherming is voldoende. Schending van de classificatie kan enigen (in)directe financiële en/of reputatieschade tot gevolg hebben voor de organisatie en/of haar klanten en betrokkenen.
	2 - Hoog	De informatie of het bedrijfsproces staat zeer weinig (integriteits)fouten toe. Bescherming van integriteit is belangrijk. Schending van de classificatie kan serieuze financiële schade of en/of reputatieschade tot gevolg hebben voor de organisatie en/of haar klanten en betrokkenen.
	3 - Absoluut	De informatie of het bedrijfsproces staat geen (integriteits)fouten toe. Bescherming van integriteit is absoluut noodzakelijk. Schending van integriteit kan zeer grote financiële schade en/of reputatieschade tot gevolg hebben voor de organisatie en/of haar klanten en betrokkenen.
Vertrouwelijkheid Access De beperking van bevoegdheid en mogelijkheid tot uitlezen, kopiëren of kennisnemen van informatie en van andere systeemcomponenten tot een gedefinieerde groep van gerechtigden, ofwel het waarborgen dat de juiste mensen toegang hebben tot de juiste informatie en anderen niet.	0 - Openbaar	Alle informatie die algemeen toegankelijk is voor ieder. Er is geen schending in de classificatie mogelijk.
	1 - Bedrijfsvertrouwelijk	Informatie die toegankelijk mag of moet zijn voor alle medewerkers van de eigen organisatie(s). Vertrouwelijkheid is gering. Schending van de classificatie kan enige (in)directe schade toebrengen aan de organisatie en/of haar klanten en betrokkenen.
	2 - Vertrouwelijk	Informatie die alleen toegankelijk mag zijn voor een beperkte groep gebruikers. De informatie wordt ter beschikking gesteld op basis van vertrouwen. Schending van deze classificatie kan serieuze (in)directe schade toebrengen aan de organisatie en/of haar klanten en betrokkenen.
	3 - Geheim	Dit betreft gevoelige informatie die alleen toegankelijk mag zijn voor de direct geadresseerde. Schending van deze classificatie kan zeer grote (in)directe schade toebrengen aan de organisatie en/of haar klanten en betrokkenen.
Aanpasbaarheid Agility Verandering in bedrijfsvoering die benodigd kan zijn als gevolg van interne en externe oorzaken, zoals acquisities of nieuwe regelingen, tegen acceptabele kosten of acceptabele risico's	0 - Standaard	Deze applicatie ondersteunt een proces dat als standaard voor de dienstverlening wordt beschouwd. Dit proces is evengoed onder te brengen in een andere applicatie. De behoefte aan aanpasbaarheid is derhalve laag.
	1 - Innovatief	Deze applicatie ondersteunt een proces waarvan verwacht wordt dat op korte of middellange termijn sprake is van veranderingen als gevolg van ontwikkelingen in de markt. De behoefte aan aanpasbaarheid wordt als gemiddeld beschouwd.
	2 - Onderscheidend	Deze applicatie ondersteunt een proces waarmee het pensioenfonds en/of de uitvoerder onderscheidend is ten opzichte van andere fondsen en/of uitvoerders. De behoefte aan aanpasbaarheid is derhalve hoog.
	3 - Compliance	Deze applicatie ondersteunt een proces welke onderhevig is aan het voldoen aan verplichtingen vanuit wet- en regelgeving waar het pensioenfonds en/of de uitvoerder aan moet voldoen. De behoefte aan aanpasbaarheid is derhalve cruciaal.

Bijlage: Evaluatie

Evaluatie vraagt om het totale overzicht

