Berenschot

Deelopdracht I: inventarisatie risico's

Van:	Daniël Huisman	Datum:	28 februari 2023
Aan:	Deelnemers overleg 23 februari	Status:	Intern vertrouwelijk
Cc:			
Onderwerp:	Inventarisatie risico's HUA		

Achtergrond van deze deelopdracht

Zoals beschreven in de Berenschot rapportage over de toekomstige organisatie van de gemeenschappelijke regeling HUA, is één van de deelnemers (namelijk OCW) van deze gemeenschappelijke regeling voornemens uit te treden. Tegelijkertijd blijft OCW duurzaam bijdragen aan de gemeenschappelijke regeling via een specifieke uitkering. Dit betekent dat - wanneer OCW dit voornemen tot uittreding doorzet –het niet langer deelnemer (eigenaar) is van de gemeenschappelijke regeling, maar alleen opdrachtgever.

Op dit moment deelt OCW als eigenaar mee in de risico's die horen bij het eigendom van een regionaal historisch centrum. Wanneer OCW inderdaad zou uittreden en niet langer eigenaar is, dan is het voor de achterblijvende partners belangrijk om inzicht te hebben in wat dit betekent voor de risicoverdeling.

Daarbij is de inzet van de achterblijvende partners dat in alle toekomstscenario's de risicoverdeling tussen OCW, provincie en gemeente gelijk blijft. Dit betekent dat – ook als OCW feitelijk de eigenaarsrol opgeeft – OCW in juridisch zin voor onbepaalde tijd in gelijke mate blijft delen in de risico's die horen bij het eigendom van een regionaal historisch centrum. Daar hoort ook bij dat OCW de eventuele kosten voor het vastleggen van afspraken om dit mogelijk te maken, voor zijn rekening neemt.

Doel en aanpak van deze deelopdracht

Het doel van deze opdracht is tweeledig:

1. te verkennen of de risico's die horen bij het eigendom van een regionaal historisch centrum op dit moment goed in beeld zijn, *en*
2. welk effect de keuze voor het voortzetten van de gemeenschappelijke regeling op basis van delegatie (zie ons eerdere rapport) heeft op de mogelijkheden van de achterblijvende partijen om op deze risico's te sturen.

Deze memo gaat in op deel 1 van deze deelopdracht, namelijk de beeldvorming over de risico's van HUA binnen de context van voortzetting van de GR.[1] Daartoe hebben we de volgende activiteiten uitgevoerd:

- expertbeoordeling van het risicoregister van HUA in de begroting: geïdentificeerde risico's en beheersingsmaatregelen

[1] Deel 1 van de opdracht gaat daarmee *niet* over het maken van afspraken met OCW over de risicoverdeling..

- (indien nodig) aanvullen risicoregister
- opstellen memo/ deelrapportage met beeldvorming over risico's HUA.

Deze memo is het resultaat van de uitgevoerde activiteiten.

Clustering van risico's in vier categorieën

Uitgangspunt van dit onderzoek is de risico-inventarisatie die jaarlijks door het bestuur van HUA wordt vastgesteld. Deze risico-inventarisatie resulteert in een risicoregister. Dit risicoregister is onderdeel van de P&C cyclus van HUA en wordt in de begroting en jaarrekening opgenomen. Bij de risico analyse hanteert HUA het BBV model[2]. De accountant ziet toe op het risicoregister van HUA en maakt hierbij gebruik van het COSO model[3].

Het meest recente risicoregister van HUA, uit de concept jaarrekening 2022, hebben we opgenomen in bijlage 1. [4] Het systeem (proces) van risicobeheersing wat HUA hanteert staat op hoofdlijnen beschreven in bijlage 2.

Bij deze risicoanalyse zijn we uitgegaan van de huidige (juridische) situatie van HUA, met continuering van het bestaande takenpakket. We hebben ons hierbij gefocust op de belangrijkste risico's die vanuit de externe omgeving van HUA of vanuit de bedrijfsvoering zouden kunnen komen.

Als we het risicoregister en de bedrijfsvoering van HUA analyseren dan constateren wij dat de belangrijkste risico's te clusteren zijn in de volgende -in willekeurige volgorde opgesomde- vier categorieën:

1. Inkomsten/ financiering HUA.
2. Personeel.
3. Huisvesting.
4. ICT.

Elke categorie bevat hieraan gerelateerde risico's. Deze werken we in het vervolg van deze memo uit. Bij de te bespreken risico's geven we inzicht in wat de belangrijkste genomen beheersingsmaatregelen zijn voor het voorkomen of mitigeren van deze risico's.

Ten aanzien van de in deze memo beschreven risico's merken we verder het volgende op:

- Een deel van de beschreven risico's, namelijk de risico's die voorzienbaar en hanteerbaar zijn, zijn geadresseerd in de begroting van HUA. Dit is in lijn met de beleidsnota Weerstandsvermogen en risicomanagement; zie bijlage 2 voor een toelichting.
- Overige risico's met mogelijke financiële consequenties staan vermeld in het risicoregister.
- Tot slot heeft een deel van de hierna te bespreken risico's een 'zacht' (niet-financieel) karakter.

1. Inkomsten/ financiering HUA

De eerste categorie risico's betreft mogelijk verlies van inkomsten door HUA.

Het grootste deel van de inkomsten is afkomstig van de volgende drie partners: de gemeente Utrecht, OCW en de provincie Utrecht. HUA loopt het risico dat één of meer van de partners de structurele bijdragen willen verlagen. Een belangrijke (bestaande) maatregel om dit risico te mitigeren is dat eens in de vier jaren een meerjarenbeleidsplan wordt vastgesteld door de deelnemers. Dit beleidsplan wordt voorbesproken met de ambtelijke contactpersonen en -na bespreking in het DB- vastgesteld door het AB.

---

[2] BBV staat voor Besluit begroting en verantwoording provincies en gemeenten.
[3] Zie voor meer informatie over het COSO model bijvoorbeeld https://nl.wikipedia.org/wiki/COSO.
[4] De jaarrekening is nog niet vastgesteld door het bestuur, dus het gaat om een concept versie. Dit risicoregister bouwt voort op risicoregisters uit de vastgestelde begroting 2023 en de jaarrekening 2021.

In de P&C documenten wordt gerapporteerd over in hoeverre de doelen van het meerjarenbeleidsplan zijn gerealiseerd. Deze categorie risico's is opgenomen in het risicoregister.

Verder noemen we nog als potentieel risico dat de investering in de Expo tentoonstelling in een aantal jaren is afgebouwd, waardoor er geen geld meer zou kunnen zijn voor aanpassingen. In de (concept) begroting 2024 is structurele ruimte gemaakt voor het aanpassen van deze permanente tentoonstelling. De jaarlijkse exploitatielasten van de Expo zijn eveneens structureel opgenomen in de begroting.

2. Personeel

De tweede categorie risico's heeft betrekking op het personeel. Deze categorie risico's hebben we onderverdeeld in de volgende subcategorieën:

- Aantrekken en behouden van medewerkers.
- (Langdurige) ziekte van medewerkers.
- Fraude door medewerkers.
- Integriteit en sociale veiligheid.

Aantrekken en behouden van medewerkers

HUA heeft medewerkers nodig met specifieke kennis op diverse terreinen. Om dit gespecialiseerde werk te kunnen doen is het aantrekken en behouden van de juiste medewerkers daarmee cruciaal.
Uit het concept jaarverslag 2022 valt af te leiden dat HUA (onder meer) de volgende activiteiten uitvoert om de juiste medewerkers te 'binden en te boeien':

- Een jaarlijks trainingsprogramma toegespitst op een van de vier kernwaarden van HUA: 2021 – Betrouwbaar, 2022 – Toegankelijk, 2023 – Verbindend, 2024 – Duurzaam. Dit trainingsprogramma is gericht op het toerusten van alle medewerkers qua vaardigheden en competenties op de impact van de digitale transformatie en de netwerksamenleving.
- Aanpassing van de wervingsprocedure om de organisatie diverser en inclusiever op te bouwen. De werving & selectieprocedure is daartoe zo ingericht dat alle kandidaten worden geselecteerd op dezelfde manier met dezelfde objectieve criteria.
- Het uitvoeren van een medewerkersonderzoek via een workshop waarbij 7 bronnen van arbeidsvreugde het uitgangspunt waren. De uitkomsten zijn begin 2023 bekend geworden en zijn vertaald in een actieplan. De separate bijlage bevat een samenvatting van het medewerkersonderzoek.

Bij vertrek van medewerkers is -zo blijkt uit het risicoregister- een belangrijke oplossing inhuur van tijdelijke medewerkers.

Ten aanzien van het thema 'aantrekken van nieuwe medewerkers' zijn de volgende citaten uit het concept jaarverslag 2022 nog van belang:

- *2022 is een jaar waarin we veel nieuwe medewerkers hebben binnengehaald. Er waren in de personeelsformatie gaten ontstaan vanwege pensioneringen en het wegvallen van de expo door de coronamaatregelen. Hierdoor was er geen werk voor bijvoorbeeld rondleiders, publieksmedewerkers, tentoonstellingmakers, etc. In 2022 kwamen er weer schoolklassen op bezoek, werden nieuw expo's geopend en activiteiten gestart zodat we daarvoor nieuwe medewerkers hebben geworven. Ondanks de krapte in de arbeidsmarkt is dat grotendeels gelukt.*
- *Er zijn nieuwe medewerkers aangetrokken voor het nieuwe team Digitale Archiefdiensten. Voor alle nieuwe functies (adviseur digitale informatie, e-conservator, specialist digitaal collectiebeheer en relatiebeheerder/coördinator) zijn goede kandidaten gevonden en in oktober ging het nieuwe team officieel van start.*

(Langdurige) ziekte van medewerkers

Ziekte en dan met name *langdurige* ziekte van medewerkers kan diverse risico's met zich brengen. We noemen de volgende risico's en beheersingsmaatregelen:

- Bij langdurige ziekte van medewerkers is HUA eigen risicodrager, waardoor HUA gedurende de ziekteperiode het salaris moet doorbetalen voor een maximum van 2 jaar. Een maatregel om langdurige ziekte op te vangen is inhuur; hiervoor is (extra) inhuurbudget nodig. Dit type risico's staat benoemd in het risicoregister (onderdeel 2, 3 en 17).
- Het is van belang dat medewerkers die taken over nemen weten hoe de processen lopen en specifiek de processen op het gebied van de interne controle. Er zijn diverse maatregelen genomen om dit risico te mitigeren. Het gaat dan om beschrijving van werkprocessen, het regelen van vervanging voor de essentiële functies en rollen binnen de organisatie, het minimaliseren van het aantal eenpitters en langlopende contracten met bureaus die inhuurkrachten kunnen leveren.

Hierbij merken we op dat -zo blijkt uit het concept jaarverslag 2022- het ziekteverzuim relatief laag is, namelijk zo'n 3% over 2022. . Deze categorie risico's is opgenomen in het risicoregister.

Fraude door personeel

Een ander personeelsgerelateerd risico is fraude. Er zijn een aantal maatregelen genomen om fraude tegen te gaan:

- De BBV systematiek[5] is onder meer gericht op het tegengaan van frauduleuze handelingen en de verantwoording hierover. Als uitvloeisel hiervan is het voor lokale overheden bijvoorbeeld verplicht om zogenaamde AO/ IC[6] handboeken op te stellen, inclusief mandaatregelingen. De AO/ IC handboeken van HUA worden eens in de vier jaar geaccordeerd door het bestuur.
- In aanvulling daarop zijn er organisatorische maatregelen genomen, de zogenaamde 'verdedigingslinies'. Zie bijlage 1 voor meer informatie. Onderdeel van de verdedigingslinies is het zogenaamde vierogenprincipe bij facturen en betalingen.
- De vierde verdedigingslinie wordt gevormd door de accountant. Deze houdt toezicht op de uitvoering; in bijlage 2 staat dit uitgewerkt. Ten aanzien van dit thema merkt de accountant het volgende op in het jaarverslag over 2021:

  Onze werkzaamheden tijdens de controle van de jaarrekening 2021 hebben geen fraudes of andere illegale handelingen, uitgevoerd door het bestuur, of andere medewerkers aan het licht gebracht. Hierbij merken wij overigens op dat onze werkzaamheden niet specifiek zijn gericht op het ontdekken van fraude en illegale handelingen.

Op basis van de geïmplementeerde regelgeving wordt dit risico adequaat afgedicht.

Integriteit en sociale veiligheid

Als gevolg van (recente) ontwikkelingen in de samenleving bestaat er een toenemende aandacht voor beheersing van risico's op het gebied van integriteit en sociale veiligheid. Het gaat hierbij om de meer 'zachte' aspecten van de beheersing van de bedrijfsprocessen, ook wel 'soft controls' genoemd. Dit is een

[5] Het Besluit Begroting en Verantwoording provincies en gemeenten (BBV) is de basis voor de gemeentelijke en provinciale financiële verslaglegging en planning en control cyclus.
[6] AO staat voor Administratieve Organisatie. Dit beschrijft een organisatie vanuit een controllers- of accountantsbril. Een accountant onderzoekt bedrijfsprocessen om te zien waar risico's verstopt zitten en controle en/of scheiding van functies nodig is (bijvoorbeeld om fraude of witwassen tegen te gaan).
IC staat voor interne controle. De interne controle is onderdeel van interne beheersingsmaatregelen.

verzamelbegrip voor diverse, uiteenlopende beheersings-maatregelen die als gemeenschappelijk kenmerk hebben dat ze gericht zijn op menselijke gedragsaspecten en moeilijk meetbaar zijn.

Het beleid van HUA ten aanzien van integriteit en sociale veiligheid is beschreven via het personeelshandboek:

- Artikel 1.a.7 Meldregeling Integriteitsschendingen en misstanden
- artikel 1.a.7.2 Vertrouwenspersoon integriteit. O.a. definitie en de procedure
- Artikel 1.a.7.6 Huis voor Klokkenluiders
- Artikel 1.a.8.2 Vertrouwenspersoon ongewenst gedrag. O.a. definitie en de procedure
- Artikel 1.a.8.5 Externe klachtenprocedure. Medewerkers kunnen hiervoor bij een externe vertrouwens- en integriteitspersoon terecht.

Bovenstaande artikelen leggen een formele basis voor een organisatie die streeft naar integriteit en sociale veiligheid. Aanvullend daarop zijn meer 'zachte' factoren van belang, zoals bijvoorbeeld voorbeeldgedrag van leidinggevenden.[7]

Naast de eerder genoemde meer formele controls hebben directie, MT en HRM van HUA een aantal 'soft controls' ontwikkeld om de sociale veiligheid van de medewerkers te kunnen monitoren. Naar aangeven van HUA gaat het om de volgende soft controls:

- Voorbeeldgedrag van de leidinggevenden is gericht op 'Practice what you preach'. Dit betreft onder meer het nakomen van afspraken, openheid en transparantie, vertrouwen geven en ontvangen, diversiteit en inclusie stimuleren en verwelkomen.
- Naast het actueel houden van de eerder genoemde formele controls, is er veel individuele aandacht voor het personeel. Er is sprake van relatief kleine teams met een eigen coördinator die dicht bij de medewerkers staat en de verbinding vormt met de leidinggevende.
- Het MT heeft de interne organisatie vast op de agenda staan van het tweewekelijkse management team overleg. Tijdens dit agendapunt wordt aandacht besteed aan zaken die spelen binnen afdelingen of bij individuele medewerkers alsook het ontwikkelen van de organisatie, de werksfeer etc.
- Tweewekelijks vindt er een digitaal 'Rondje HUA' plaats waarin directie, MT en medewerkers elkaar bijpraten over nieuwe ontwikkelingen en medewerkers vragen kunnen stellen over personeelsbeleid en andere zaken.
- Er is verder een zes wekelijks MT-Coördinatorenoverleg, waarin de leidinggeven en coördinatoren samen bespreken hoe het gaat met de interne organisatie en hoe ze kennis kunnen delen en elkaar kunnen helpen bij het oplossen van problemen.
- Er is een actieve rol van HRM voor integriteit en sociale veiligheid. Er is regelmatig contact tussen de vertrouwenspersoon, directie en HRM-adviseur, voor advies en overleg om bijtijds signalen te herkennen.
- Sociale veiligheid is opgenomen in het onboarding programma van nieuwe medewerkers.

Volgens opgave vanuit HUA spelen op dit moment geen casussen inzake integriteit en sociale veiligheid. Er lopen geen trajecten bij de vertrouwenspersoon of OR en er zijn geen signalen van komende issues op het gebied van integriteit en sociale veiligheid. Dit wordt gebaseerd op de volgende indicatoren:

- Er is sprake van een laag ziekteverzuim (3%).[8]

[7] Naast voorbeeldgedrag van leidinggevenden, gaat het bijvoorbeeld ook om een beheersbare werkdruk, een gevoel van verbondenheid van medewerkers met de organisatie, transparantie, bespreekbaarheid van deze thema's en handhaving door het management bij ongewenst gedrag.
[8] Bron: ziekteverzuim overzichten Bureau People & payment.

- In 2022 zijn er geen meldingen bij de vertrouwenspersoon ongewenst gedrag & integriteit geweest; er zijn ook geen signalen vanuit deze functionaris.[9]
- De OR is tevreden over de organisatieontwikkeling en personeelsbeheer.[10]
- Een positieve uitkomst van het medewerkersonderzoek is dat er geen aandachtspunten op het gebied van integriteit en sociale veiligheid naar boven zijn gekomen. Ook komt naar voren dat 'oud zeer' verdwijnt en plaats maakt voor een goede sfeer in de organisatie.[11] Er is een grote opkomst bij het tweewekelijkse digitale Rondje HUA en andere personeelsbijeenkomsten.

Mocht dit risico optreden en een financiële vertaling krijgen bij een arbeidsconflict met een medewerker, dan is dit risico geadresseerd in het risicoregister (punt 18).

3. Huisvesting

HUA maakt gebruik van de volgende twee panden:

- Het pand Hamburgerstraat 28 te Utrecht, dat gehuurd wordt van een particuliere organisatie. Hierin is het Publiekscentrum gehuisvest.
- Het pand Alexander Numankade 199 -201 te Utrecht, waarin de depots en studiezaal zijn gehuisvest. Ook dit pand wordt door HUA gehuurd. Het is deels eigendom van de gemeente Utrecht (kantoren en studiezaal) en deels van het Rijk (depots). Het beheer van de depots is per 1 januari 2019 overgegaan van het Rijk naar HUA.

De risico's ten aanzien van huisvesting hebben we onderverdeeld in de volgende twee subcategorieën:

- Bescherming van de archieven.
- Continuering van de huurcontracten.

Daarnaast is ten aanzien van huisvesting een actuele ontwikkeling met financiële impact de sterke stijging van de energiekosten. HUA heeft een aantal maatregelen genomen om dit risico te adresseren. Het gaat dan onder meer om een bestemmingsreserve "Energie en indexatie" en maatregelen zoals -uiteraard voor zover mogelijk bij een Archiefdienst- "De thermostaat op maximaal 19 graden".
Deze categorie risico's is opgenomen in het risicoregister.

Bescherming van de archieven

Van de HUA website komt het volgende citaat: *Het Utrechts Archief verwerft en bewaart de bronnen van de Utrechtse geschiedenis, om ze beschikbaar te stellen aan het publiek.* Voor HUA is het daarmee cruciaal dat deze bronnen beschermd worden voor bijvoorbeeld brand, wateroverlast of diefstal.

Om de archieven te beschermen tegen deze risico's is er een variëteit aan beheersingsmaatregelen genomen. We noemen de volgende maatregelen:

- Er zijn voor beide panden meerjarenonderhoudsplannen (MJOP) gemaakt voor de komende 30 jaar. Voor het opstellen van het MJOP maakt HUA gebruik van het HUMBLE programma. Dit wordt gecontroleerd door de accountant.

[9] Bron: jaarverslag externe vertrouwenspersoon.
[10] Bron: notulen, memo bestuursvergadering 15 november 2022.
[11] Bron: verslag medewerkersonderzoek.

- HUA maakt gebruik van een volledig gecontroleerd klimaatbeheersingssysteem voor de kantoren, de achiefdepots en de expositieruimtes.
- Er zijn verschillende maatregelen genomen inzake (het voorkomen van) brandschade:
  - Voldoen aan wetgeving op dit gebied, bijvoorbeeld brandwerende deuren
  - Compartimentering: 120 minuten brandwerend
  - Directe afschakeling van de stroom in de depot's buiten bedrijfstijd
  - Volledige bewaking door de brandmeldinstallatie, met directe doormelding naar de brandweer
  - Afspraken met de brandweer over onder meer de aanvliegroute.
- Maatregelen om diefstal te voorkomen zitten op het niveau Borg 4.[12] Dit is een combinatie van beveiligingsmaatregelen en afspraken op het gebied van organisatie, elektronische beveiliging, bouwkundige beveiliging en responstijd van de beveiliging en inschakelen van de politie.
- Om waterschade te voorkomen zijn er geen watergedragen leidingen in de depot's, zijn er detectiesystemen en dergelijke.
- Voor eventuele schade zijn passende verzekeringen bij eventuele schade.

De genoemde maatregelen behoren tot de risico's die kunnen worden afgedekt via de werkprocessen. Ze zijn daarom opgenomen in de reguliere begroting van HUA (en niet in het risicoregister).

Continuering huurcontracten

Een andere bron van risico's ten aanzien van huisvesting is dat de huurcontracten opgezegd zouden kunnen worden door de verhuurders. We achten de kans dat dit risico zich voordoet uitermate klein, om de volgende redenen:

- Voor de huisvesting op de Numankade geldt dat het Rijk en de gemeente Utrecht de verhuurder zijn. Specifiek aan het huurcontract met het Rijk is dat deze het contract niet kan opzeggen. Het contract met de gemeente Utrecht voor het kantoordeel betreft een contract met oneindige looptijd en stilzwijgende verlenging.
- Het pand op de Hamburgerstraat wordt verhuurd door een stichting. Dit betreft een huurcontract met oneindige looptijd en stilzwijgende verlenging. Volgens het bestemmingplan heeft dit pand een museale bestemming. Dit beperkt de verhuurmogelijkheden van dit pand. Een andere factor die de verhuurmogelijkheden beperkt is dat het pand beschikt over een grote kelder. Voor HUA heeft deze kelder wél meerwaarde omdat hierin een deel van de Expo tentoonstelling is ondergebracht.
- . Deze categorie risico's is opgenomen in het risicoregister.

4. ICT

Onze beschrijving van de risico's ten aanzien van ICT hebben we als volgt onderverdeeld:

- Ransomware en virusaanvallen.
- Storingen ICT systemen.
- Implementatie van nieuwe applicaties voor het primair proces.
- Faillissement van softwareleveranciers.
- Gegevensmisbruik door medewerkers van HUA.

Ransomware en virusaanvallen

De eerste subcategorie betreft ransomware en virusaanvallen.

[12] Borgklasse 4 is het hoogste risicoklasse niveau. Zie voor meer informatie bijvoorbeeld: https://hetccv.nl/keurmerken/vrki-bedrijven/.

In de eerste plaats merken we hierbij op dat de impact van dergelijke risico's voor de bedrijfsprocessen van HUA relatief beperkt is. In tegenstelling tot bijvoorbeeld een bank, een vliegtuigmaatschappij of een universiteit is er geen acute noodzaak om gegevens te kunnen leveren. In vergelijking met deze drie voorbeelden zijn de HUA bedrijfsprocessen van HUA dus over het algemeen niet tijdkritisch. Het zou daardoor enige weken kunnen duren voordat de systemen weer in de lucht moeten zijn. Ten tijde van de ransomware aanval in 2021 lag het IT systeem er bijvoorbeeld 6 weken uit. Specifiek benodigde archiefstukken, zoals bouwdossiers, werden in deze periode met de hand gelicht en aan het publiek ter beschikking gesteld.

Dat neemt niet weg dat HUA diverse maatregelen heeft genomen om dergelijke aanvallen tegen te gaan. HUA werkt met de BIO[13] systematiek om de volgende stappen te zetten. HUA werkt -als onderdeel van dit uitgebreide maatregelenpakket- bijvoorbeeld met een gedifferentieerde back-up strategie, waarbij back-up tapes op verschillende locaties liggen.

Dit is overigens ook een thema waar de accountant toezicht op houdt, zie bijlage 2.

. Deze categorie risico's is opgenomen in het risicoregister.

Storingen ICT systemen

Een tweede subcategorie risico's is dat het ICT systeem door hardware defecten of software problemen niet meer zou werken. Deze problemen zouden bijvoorbeeld veroorzaakt kunnen worden door een gebrek aan ICT medewerkers of ICT medewerkers met onvoldoende deskundigheid.

In aanvulling op de hiervoor genoemde maatregelen bij ICT en Huisvesting heeft HUA de volgende maatregelen ingezet om dit type risico's te mitigeren. Voor Afas en Microsoft wordt gewerkt met cloudoplossingen. Het technisch beheer van de ICT infrastructuur wordt in 2023 geoutsourced aan een externe partij. Het volgende citaat uit het concept jaarverslag 2020 licht deze ontwikkeling richting een ICT-regie organisatie nader toe:

> *De kern hierbij is om de huidige ICT-organisatie om te vormen naar een ICT-regie organisatie, organisatie brede ICT-functies te benoemen en in de formatie te beleggen en de huidige ICT omgevingen uit te besteden. Daarmee komt de focus van HUA te liggen op enerzijds het digitaal specialisme in het primaire proces voor collectiebeheer, verrijking, ontsluiting en nieuwe ontwikkelingen (als een e-depot) en anderzijds de ICT-regieorganisatie HUA breed gestuurd vanuit een CIO-rol met een ICT-regisseur, ICT beveiligingsverantwoordelijke en eigen HUA functioneel applicatiebeheerders voor de kernapplicaties.*

Ten aanzien van dit thema doet de accountant in het jaarverslag over 2021 een aanbeveling om bij de overgang naar de nieuwe infrastructuur en applicatielandschap een monitoringtool te implementeren. Deze aanbeveling is inmiddels geïmplementeerd door HUA.

. Deze categorie risico's is opgenomen in het risicoregister.

Implementatie van nieuwe applicaties voor het primair proces

Een volgende bron van risico's zijn (mislukte) aanbestedingen en implementaties van nieuwe applicaties voor het primair proces.

[13] Baseline Informatiebeveiliging Overheid. Zie voor meer informatie bijvoorbeeld: https://bio-overheid.nl/.

In het concept jaarverslag 2022 is terug te vinden dat er op dit gebied diverse ontwikkelingen zijn geweest. Een belangrijke mijlpaal was de afronding van de aanbesteding van het e-depot. Deze bewaarplaats voor digitaal gevormd archief zal in de loop van 2023 operationeel zijn. Nadat het bestuur hiervoor groen licht had gegeven, is in samenwerking met specialisten van de gemeente Utrecht en de provincie Utrecht een plan van eisen opgesteld. Daarna is het aanbestedingstraject met hulp van een gespecialiseerd adviesbureau op het gebied van aanbestedingen doorlopen en is de beoogde voorziening gegund aan de leverancier Preservica.

De risico's van (een mislukte of vertraagde) implementatie van dit systeem zijn in onze visie beperkt, omdat:

- Het 'proven technology' is. Ruim 10 Nederlandse archieforganisaties werken reeds met dit systeem. [14]
- Het niet gaat om tijdkritische bedrijfsprocessen, zoals hiervoor al aangegeven.
- . Deze categorie risico's is opgenomen in het risicoregister.
-

Faillissement softwareleveranciers

Een ander risico ten aanzien van softwareleveranciers is dat deze failliet zouden kunnen gaan.

Hierbij merken we op dat HUA voor de bedrijfsvoering werkt met software van gerenommeerde marktpartijen, zoals Microsoft (voor de kantoorautomatisering) en Afas (voor de financiële en de personeelsadministratie). Het risico dat de leveranciers van deze, breed door de markt geadopteerde, systemen failliet gaan achten wij heel klein.

Voor het primair proces werkt HUA met software van kleinere (Nederlandse) marktpartijen. HUA bevindt zich namelijk in een niche markt, waar relatief beperkte vraag is naar automatiseringsoplossingen. Het risico is daardoor groter dat deze partijen failliet zouden kunnen gaan. Voor de belangrijkste gebruikte applicaties heeft HUA de volgende beheersingsmaatregelen genomen:

- Er is een escrow[15] overeenkomst afgesloten met de leverancier van het MAIS-Flexis systeem. Dit systeem wordt gebruikt voor het beheren en beschrijven van de archieven in de depots.
- Met Preservica, een Engelse softwareleverancier, is de afspraak gemaakt dat bij een eventueel faillissement HUA de eigen data uit het systeem kan halen.
  . Deze categorie risico's is opgenomen in het risicoregister.
-

Gegevensmisbruik door medewerkers HUA

Tot slot bestaat het risico dat medewerkers van HUA ongeautoriseerd toegang zouden kunnen krijgen tot (persoons)gegevens.

Ten aanzien van de beheersingsmaatregelen voor dit risico noemen we het volgende:

- De maatregelen die genomen worden tegen fraude zijn ook van toepassing op het risico van gegevensmisbruik. Het gaat dan om de uitwerking van de BBV systematiek in onder meer mandatering (bijvoorbeeld beperking van toegang tot systemen) en het vierogenprincipe.
- In de afgelopen periode zijn de rollen van CISO en functionaris gegevensbescherming (FG) ingevuld door externe, onafhankelijke experts. Deze functionarissen hebben -conform wetgeving- direct toegang

[14] Zie voor meer informatie: https://preservica.com/resources/press-releases/netherlands-e-depots-choose-preservica-to-future-proof-government-records.
[15] Een escrow overeenkomst is een overeenkomst tussen de maker van software, zijn klanten en een escrow-agent. De overeenkomst garandeert dat de klant in bepaalde gevallen, bijvoorbeeld faillissement van de software leverancier, kan beschikken over de laatste broncode van het softwarepakket waarvoor de overeenkomst gesloten is.

tot de directie van HUA, bijvoorbeeld met rapportages. Vergelijkbaar met de control functie kunnen ze bij specifieke gevallen ook het bestuur benaderen.
- De accountant controleert of de principes van functiescheiding, toegangsbeveiliging, wachtwoorden en dergelijke adequaat zijn ingericht bij HUA. Deze controles zijn in de afgelopen periode steeds strenger geworden.
- . Deze categorie risico's is opgenomen in het risicoregister.

Reflectie risico's HUA

Onze reflectie ten aanzien van de (belangrijkste) risico's van HUA is dat deze in beeld zijn en dat er een breed pakket aan beheersingsmaatregelen is genomen om deze risico's te voorkomen of te mitigeren.

Hierbij een korte resumé van de belangrijkste potentiële risico's:

- Het grootste deel van de *inkomsten* van HUA komt van overheidsorganisaties die deelnemer zijn in de GR of waarmee meerjarige overeenkomsten zijn afgesloten. Deze organisaties hebben zelf volledige beheersing van het risico dat de inkomsten van HUA verminderen.
- Wat betreft *huisvesting* is voor de bescherming van de archieven een uitgebreid pakket aan maatregelen genomen.
- De bedrijfsprocessen van HUA zijn beperkt tijdkritisch, waardoor *uitval van ICT systemen* (door bijvoorbeeld ransomware) en *langdurige ziekte of vertrek van medewerkers* op de korte termijn een relatief beperkte impact heeft. Bovendien is -zoals hiervoor beschreven- een breed pakket aan maatregelen ingevoerd om dit type risico's te voorkomen.
- Om risico's op het gebied van *integriteit en sociale veiligheid* te monitoren en te voorkomen zijn maatregelen genomen op zowel formele als op soft controls.

Bijlage 1. Risicoregister HUA

Deze bijlage bevat het (meest recente) risicoregister van HUA uit de concept jaarrekening 2022.

De opzet van dit risicoregister is in overeenstemming met hetgeen beschreven staat in de nota “211103 – Beleidsnota Weerstandsvermogen en risicomanagement 2022”. Zie de volgende bijlage voor een toelichting op deze nota.

#	Thema	Gebeurtenis	Oorzaak	Gevolg	Mogelijke oplossingen	Financieel effect	Eens in de jaren	Kans	Benodigde weerstandcapaciteit
1	Calamiteit	Brand of natuurramp depot's	Calamiteit	Delen archieven ernstig beschadigd	Grootschalig conserveren en restauratie toepassen en alternatieve opslag	200.000	25	4	8.000
2	Calamiteit	Corona en andere epidemien	Calamiteit	Mogelijke uitval van cruciale functies op	Inhuur interim medewerkers	200.000	10	10	20.000
3	Calamiteit	Corona en andere epidemien	Calamiteit	Uitval relevante functies en daardoor achterstanden in	Inhuur expertise	75.000	10	10	7.500
4	Calamiteit	Corona en andere epidemien	Calamiteit	Exposities worden uitgesteld en dit leidt	Planningen opschuiven	30.000	10	10	3.000
5	Calamiteit	Corona en andere epidemien	Calamiteit	Exposities moeten worden uitgesteld en	Planningen opschuiven	20.000	10	10	2.000
6	Partners	Uittreding Rijk	Veranderde visie OCW en NA op samenwerking RHC's	Zorg voor en huidige financiering van analoge collectie Rijk is blijvend toegezegd	Binding partners aan RHC's	2.532.748	25	4	101.310
7	Partners	Bezuinigingen bij partners	Herprioritering beschikbare	Vermindering van vaste bijdrage van	Bezuinigen bij HUA na eerste jaar	662.284	10	10	66.228
8	Partners	Andere inrichting inhoudelijke samenwerking partners	Veranderde visie partners op inhoudelijke samenwerking	Deelname wijzigt en daarmee 25% van de bijdrage	Migreren en andere voorziening realiseren	1.655.710	25	4	66.228
9	Partners	Uittreding DVO, andere samenwerking	Veranderde visie DVO partijen op samenwerking	Deelname wijzigt of stopt	Migreren en andere voorziening realiseren	311.000	5	20	62.200
10	Buitenwereld	Ransomware	Hacken van database	Data niet meer toegankelijk	Backup bestanden terugzetten	200.000	10	10	20.000
11	Buitenwereld	Exit traject leverancier van digitaal depot	Diverse faillissement leverancier etc	Uitfaseren huidige applicatie en migratie naar nieuwe aan te besteden omgeving	Contracten herzien en migratie naar nieuwe aan te besteden omgeving	200.000	10	10	20.000
12	Buitenwereld	Claim auteursrechten	Onvolledige registratie	Claims van derden	Schikking sluiten	50.000	10	10	5.000
13	Buitenwereld	Exit traject leverancier van basiscomponent digitaal collectiebeheer	Diverse waaronder faillissement leverancier	Uitfaseren huidige applicatie en migratie naar nieuwe aan te besteden omgeving	Contracten herzien en migratie naar nieuwe aan te besteden omgeving	200.000	10	10	20.000
14	Buitenwereld	Claim datalek	Onvolledige registratie	Claims van derden / boete	Schikking sluiten	50.000	10	10	5.000
15	Buitenwereld	Opzeggen huur HBS	Conflict met verhuurder	EXPO kan niet doorgaan op deze	Andere locatie of andere vorm zoeken	250.000	20	5	12.500
16	Buitenwereld	Opzeggen huur HBS	Conflict met	Verhuizen	Verhuizen naar ANK	150.000	20	5	7.500
17	Intern	Afwezigheid medewerkers	Vertrek en ziekte van medewerkers	Missen kennis en sturing	Inhuren van tijdelijke medewerkers	100.000	10	10	10.000
18	Intern	Arbeidsconflict	Verschillen van inzicht	Verstoorde arbeidsrelatie	Wachtgeldvoorziening incl juridische ondersteuning	250.000	7	14	35.714
	Totaal								**472.181**

Bijlage 2. Systeem van risicobeheersing

Deze bijlage gaat op hoofdlijnen in op het systeem (proces) van risicobeheersing bij HUA.

Beleidsnota Weerstandsvermogen en risicomanagement

Het risicomanagementproces staat beschreven in de nota “211103 - Beleidsnota Weerstandsvermogen en risicomanagement 2022”. Deze nota wordt per beleidsperiode geactualiseerd en vastgesteld door het AB en gaat in op de manier waarop binnen HUA risico’s geïnventariseerd, gewogen en beheerst worden. Ook wordt aangegeven welk vermogen nodig is om gebeurtenissen financieel het hoofd te bieden. Aan de orde komen de spelregels en richtlijnen op het gebied van weerstandsvermogen en risicomanagement.

Deze nota vindt zijn weerslag in de risicoparagraaf van de jaarverslag en de begroting en is conform de BBV wetgeving en de PDCA-cyclus. Zie de vorige bijlage voor het meest actuele risicoregister.

Proces van totstandkoming en vaststelling risicoregister

Het risicoregister c.q. de risicoparagraaf uit de begroting en jaarrekening (P&C documenten) komt als volgt tot stand:

- In een aparte jaarlijkse sessie neemt het MT van HUA alle risico’s door, actualiseert en evalueert deze. De risicoparagraaf wordt door de accountant gecontroleerd voor het jaarverslag. Vervolgens bespreekt de accountant zijn bevindingen met de directie (en vervolgens met het DB).
- Voorafgaand aan de bestuursvergaderingen vindt een ambtelijk vooroverleg plaats van HUA met de contactpersonen (beleidsmedewerkers) van de gemeente Utrecht en de provincie. In dit overleg worden alle vergaderstukken in concept besproken en reacties opgehaald. In dit overleg wordt onder meer de risicoparagraaf besproken.
- De volgende stap is dat de P&C documenten worden besproken met het DB.
- Daarna worden de P&C documenten met de risicoparagraaf vóór 15 april naar het Rijk, de gemeenteraad van Utrecht en Provinciale Staten gestuurd in het kader van de zienswijzeprocedure.
- Tot slot wordt het risicoregister -samen met een goedkeurende verklaring van de accountant- vastgesteld door het AB in de juni vergadering.
- Gedurende het jaar vindt tussentijdse controle en sturing plaats via de bestuursrapportages (Beraps).

De verantwoordelijkheid voor het risicomanagementproces ligt bij de directie in samenspraak met het MT en waar nodig de OR. De onafhankelijke interne controle is geregeld via de controller.

Toezichthouder HUA

Het ministerie van BZK is toezichthouder op HUA. HUA valt onder de lichtste vorm van toezicht (repressief toezicht.). Vóór 15 juli van elk jaar stuurt HUA het jaarverslag van het voorgaande jaar en de begroting van het komende jaar naar BZK.

Risicomanagementorganisatie: verdedigingslinies

Hiervoor zijn we ingegaan op het risicomanagement*proces*. We gaan nu kort in op de risicomanagement*organisatie*. Op hoofdlijnen zijn de zogenaamde verdedigingslinies ('lines of defense')[16] als volgt georganiseerd bij HUA:

1. Het lijnmanagement is verantwoordelijk voor haar eigen processen en de risicobeheersing.
2. De controller van HUA ondersteunt, adviseert en bewaakt of het management zijn verantwoordelijkheden ook daadwerkelijk neemt. De controller bereidt ook het beleid voor en organiseert de risico-sessies.
3. De rollen van FG en CISO zijn ingevuld door externe onafhankelijke experts. Deze hebben conform wetgeving direct toegang tot de directie en -in specifieke gevallen- het bestuur van HUA.
4. Bestuur, accountant en de (ambtelijke vertegenwoordiging van de) deelnemers in de GR houden vervolgens toezicht op dit hele proces.
5. BZK is de formele toezichthouder.

Rol accountant

Hiervoor gingen we reeds kort in op de rol van de accountant in het risicomanagementproces. De accountant kijkt in de controleaanpak naar de volgende risico's:

- Het onterecht onttrekken van gelden aan de GR [Getrouwheid].
- Onjuiste mutaties in PA/SA waardoor personeelskosten niet nauwkeurig zijn verantwoord [Getrouwheid].
- De bezoldiging en de verantwoording WNT voldoen niet aan de eisen die daaraan zijn gesteld [Getrouwheid].
- Prestaties worden gefactureerd aan de GR welke niet zijn ontvangen [Getrouwheid].
- Investeringen en afschrijvingen vinden plaats in strijd met de nota investerings- en afschrijvingsbeleid [Rechtmatigheid].
- Dotaties en onttrekkingen vinden plaats in strijd met de nota reserves en voorzieningen [Rechtmatigheid].
- Inkopen worden ten onrechte niet Europees aanbesteed [Rechtmatigheid].
- Bestedingen vinden plaats boven de goedgekeurde begroting [Rechtmatigheid].

In het jaarverslag doet de accountant aanbevelingen om het risicomanagementproces te verbeteren. In de memo hebben wij voorbeelden gegeven van dergelijke aanbevelingen.

Hierbij merken we op dat er per 2023 een verandering in de systematiek van rechtmatigheidscontrole is. Vanaf dit jaar moet namelijk het DB van HUA een 'in control statement' afgeven. De betreffende stukken worden in maart 2023 in het bestuur besproken.

[16] De kern van dit principe is dat er verschillende -elkaar versterkende- beheersingsfuncties zouden moeten bestaan, die onafhankelijk van elkaar functioneren. Elke functie levert een eigen bijdrage aan de kwaliteit van het interne beheersingssysteem.