# <pagina>Quickscan DUTO-risicobeoordeling

De **Quickscan DUTO-risicobeoordeling** is een methode om snel op hoofdlijnen een beeld te krijgen van de risico’s die een overheidsorganisatie loopt door de manier waarop informatiebeheer binnen die organisatie is ingericht.

De quickscan bestaat uit de volgende stappen:

* Selecteer de belangrijkste bedrijfsprocessen
* Vul de vragenlijst in voor die processen
* Beoordeel de resultaten
* Deel je conclusies

Deze stappen kunnen door een informatieprofessional binnen een paar weken uitgevoerd worden. De precieze duur hangt er met name vanaf hoelang het duurt om de benodigde informatie te verzamelen.

## <kop>Voor wie is de quickscan bedoeld?

De quickscan is bedoeld voor organisaties die snel een globaal inzicht willen verwerven in de belangrijkste risico’s die ze lopen op het gebied van informatiebeheer. Het uitvoeren hiervan brengt globaal in kaart waar de prioriteiten liggen en wat het eerste opgepakt moet worden. En het kan helpen om binnen organisaties het gesprek op gang te brengen en bewustwording te creëren over het belang van duurzame toegankelijkheid.

De quickscan is *niet* geschikt voor organisaties die op het gebied van kwaliteitszorg en risicomanagement rondom DUTO al processen ingericht hebben en die op zoek zijn naar een meer gedetailleerde risicobeoordeling. Voor die situaties is er een uitgebreider <link> stappenplan beschikbaar. Dit stappenplan is verder uitgewerkt en gebruikers kunnen dit aanpassen om een risicobeoordeling uit te voeren die precies de inzichten oplevert waar ze naar op zoek zijn.

# Stap 1 – Selecteer de belangrijkste bedrijfsprocessen

De quickscan richt zich op de belangrijkste processen binnen je organisaties. Stel voor jezelf een korte lijst samen met een paar bedrijfsprocessen die ‘bedrijfskritisch’ zijn. Wat bedrijfskritisch is, wisselt per organisatie, al zijn er ook bedrijfsprocessen te noemen die in elke organisatie belangrijk zijn. Geen enkele organisatie kan bijvoorbeeld functioneren zonder degelijke financiële administratie.

Processen zijn bedrijfskritisch als ze voldoen aan een of meer van de volgende criteria:

* Er worden [bijzondere persoonsgegevens](https://www.autoriteitpersoonsgegevens.nl/themas/basis-avg/privacy-en-persoonsgegevens/wat-zijn-persoonsgegevens#bijzondere-persoonsgegevens)beheerd en gebruikt.
* De beheerde gegevens dienen als basis- of kernregistratie.
* Er wordt informatie beheerd waarin rechten en plichten van burgers zijn vastgelegd.
* Er wordt informatie beheerd over bestuurlijke besluitvorming van de organisatie.
* Er wordt informatie beheerd en gebruikt die vaak nodig is om informatievragen te beantwoorden en aan Woo-verzoeken te voldoen.
* Er wordt informatie beheerd en gebruikt die op grond van de Woo [actief openbaar](https://www.informatiehuishouding.nl/projecten/actieve-openbaarmaking-overheidsinformatie/documenten/publicaties/2024/10/22/handreiking-openbaar-maken-doe-je-zo---conceptversie) gemaakt moet worden.
* Er wordt informatie in beheerd en gebruikt die van hoge waarde is voor de bedrijfsvoering van de organisatie, bijvoorbeeld zoals in een juridisch, financieel of HRM-systeem.
* Het gaat om informatie die dusdanig gevoelig of vertrouwelijk is, dat een datalek grote schade veroorzaakt.
* Het gaat om een proces of een applicatie waarvan de impact van uitval groot is.

## <kop>Wat als er geen goed overzicht is van bedrijfsprocessen?

Bij een quickscan is het niet de bedoeling om eerst een eindeloze analyse uit te voeren om deze processen te identificeren. Werknemers die goed bekend zijn met hun organisatie, kunnen in de regel een lijstje met bedrijfskritische processen leveren. Je kunt hiervoor uitgaan van je eigen intuïtie en de kennis van ervaren collega’s.

Als je het bedrijfsproces voor deze risicobeoordeling hebt geselecteerd, is de volgende vraag: **wie zijn verantwoordelijk voor deze processen?** Hoe dat belegd is, verschilt van organisatie tot organisatie. Veel organisaties werken met proceseigenaren en/of procesbeheerders. Benader de juiste persoon met het voorstel om een snelle risicobeoordeling uit te voeren.

# Stap 2 - Vul de vragenlijst in

De vragenlijst voor de snelle risicobeoordeling bestaat uit twee delen.

* Het *eerste deel* kun je zelfstandig invullen. Hierbij gaat het om vragen over de manier waarop informatiebeheer organisatiebreed geborgd wordt. De antwoorden op deze vragen gelden voor alle bedrijfsprocessen. Deze vragen kun je zelf beantwoorden door bureauonderzoek te doen.
* Het *tweede deel* bevat vragen die specifiek over één bedrijfsproces gaan. Als je meerdere bedrijfsprocessen opneemt in de risicobeoordeling, dan vul je dit deel meer dan eens in. Bij het beantwoorden van deze vragen heb je mensen nodig die kennis hebben van het desbetreffende bedrijfsproces. Via de proceseigenaar of beheerder kom je bij deze specialisten terecht.

**<kop>Met de lijst de organisatie in**

In de communicatie met de proceseigenaar is het belangrijk om duidelijk te zijn over het doel van de quickscan. De quickscan is geen vorm van toezicht. Het doel van een risicobeoordeling is om de lijnorganisatie *in control* te brengen op het gebied van duurzame toegankelijkheid. De rol van de informatieprofessional is om te ontzorgen en mee te denken over mogelijke concrete oplossingen.

Je kunt de vragenlijst van te voren opsturen ter voorbereiding, maar plan altijd een gesprek in met de proceseigenaar om de vragenlijst samen door te lopen. De proceseigenaar kan eventueel inhoudelijke deskundigen aan laten schuiven. Daarmee voorkom je dat vragen verkeerd worden geïnterpreteerd en wordt de gelegenheid geboden om de zichtbaarheid van informatiebeheer te vergroten.

* Als het antwoord op een vraag ‘nee’ is, dan is dat het begin van een gesprek en een reden om verder door te vragen naar de oorzaken. Dat levert de informatieprofessional ook stof op om stap 4 van de quickscan realistische oplossingen te kunnen voorstellen.
* Maar ook als het antwoord ‘ja’ is, is het belangrijk om door te vragen om een goed beeld te krijgen van de situatie. Dat kan voorkomen dat er verschillende interpretaties bestaan bij een vraag. Bijvoorbeeld: Als er een procedure bestaat voor vernietiging, betekent dat niet dat er ook daadwerkelijk vernietigd wordt. En als er vernietigd wordt, wil dat niet zeggen dat dit ook *rechtmatig* is verlopen.

Bij iedere vraag is een toelichting beschikbaar: waarom is de vraag relevant? En: waar vinden we het antwoord? Je kunt de vragenlijst ook voor jezelf downloaden zodat je er makkelijker de organisatie mee in kunt.

* <Link naar download>

## <kop>Organisatiebrede vragen

1. Er is een **actueel overzicht** van welke informatie door welke bedrijfsprocessen en applicaties gebruikt wordt

|  |  |
| --- | --- |
| [] Ja | [] Nee |

Toelichting: Deze informatie is vaak vastgelegd in architectuur of in een documentair structuurplan, zaaktypecatalogus, verwerkingsregister of ordeningsstructuur. Heeft je organisatie een informatie-architect? Vraag die dan om informatie. Ook kun je aan specialisten op het gebied van privacy en informatiebeveiliging vragen of zij al beschikken over een overzicht.

Als het antwoord ‘nee’ is, dan kan je organisatie niet goed in beeld brengen welke kansen en risico’s er bestaan op het gebied van informatiebeheer. En hoe de organisatie op die kansen in kan spelen en eventuele risico’s kan verkleinen. Met als gevolg dat de organisatie dan kansen mist of overvallen wordt door onverwachte calamiteiten waarop niet geanticipeerd is.

1. Voor het vernietigen van informatie-objecten **bestaat een vastgestelde procedure**

|  |  |
| --- | --- |
| [] Ja | [] Nee |

Toelichting: De selectielijst legt per proces de bewaartermijnen vast die op verschillende categorieën overheidsinformatie van toepassing zijn. Na het verlopen van de bewaartermijn, moet informatie worden vernietigd. Om te kunnen vernietigen moeten zowel organisatorische als functionele en operationele maatregelen worden genomen. Een bewaartermijn kan bijvoorbeeld ingericht zijn in een applicatie, maar het kan onduidelijk zijn welke rollen en verantwoordelijkheden er zijn om het ten uitvoer te brengen. De organisatie moet daarom beschikken over een vastgestelde procesbeschrijving voor het vernietigen van overheidsinformatie.

Als het antwoord ‘nee’ is, dan weet de organisatie niet hoe het proces voor vernietiging van overheidsinformatie verloopt om te kunnen voldoen aan de wettelijke vernietigingsplicht. Hiermee wordt de kans vergroot dat vernietiging ongecontroleerd plaatsvindt en informatie te vroeg wordt vernietigd. Of dat het helemaal niet plaatsvindt omdat werknemers niet weten welk proces gevolgd moet worden. Het gevolg is dat ook niet aan verplichtingen uit andere wetgeving wordt voldaan, zoals de Woo, privacy en informatiebeveiliging. Als vernietiging uitblijft, wordt ook onnodig beslag gelegd op opslagcapaciteit. Dat leidt tot hogere kosten en grotere milieubelasting.

1. Blijvend te bewaren informatie-objecten worden **tijdig overgebracht** naar een archiefdienst

|  |  |
| --- | --- |
| [] Ja | [] Nee |

Toelichting: Onder de nieuwe Archiefwet moet blijvend te bewaren overheidsinformatie tien jaar na creatie of ontvangst overgebracht worden naar een archiefdienst. Onderzoek of overbrenging deel uitmaakt van beleid en/of er procedures zijn. Verklaringen van overbrengingen geven inzicht in de vraag of de organisatie voldoet aan het tijdig overbrengen.

Als het antwoord ‘nee’ is, kan het zijn dat de organisatie onterecht verantwoordelijk is voor het eigen beheer van overheidsinformatie. Afgezien van het niet voldoen aan wettelijke verplichting, is er grote kans dat de organisatie onnodige kosten maakt voor het beheer van informatie. Daarnaast blijft de informatie onder het regime van de Woo vallen en blijft de organisatie verantwoordelijk voor de verplichtingen en werkzaamheden die daaruit voortkomen.

1. Informatiebeheer is in een vroeg stadium betrokken bij **aanschaf en inrichting** van nieuwe applicaties

|  |  |
| --- | --- |
| [] Ja | [] Nee |

Toelichting: Overheidsinformatie moet gedurende hele levensduur duurzaam toegankelijk zijn. Het nemen van passende maatregelen voor duurzame toegankelijkheid begint dan ook in een zo vroeg mogelijk stadium bij het ontwerpen en inrichten van applicaties. We noemen dit archiveren by design. Het is daarom belangrijk om informatiebeheer te betrekken bij de aanschaf en ontwerp van applicaties zodat passende DUTO-maatregelen kunnen worden gerealiseerd.

Als het antwoord ‘nee’ is, dan zijn applicaties niet ingericht om overheidsinformatie duurzaam toegankelijk te houden. Het achteraf nemen van herstelmaatregelen kost veel tijd en geld. Als er bijvoorbeeld bij de vervanging van een applicaties niet meteen goed nagedacht wordt over migratie, kan het leiden tot de noodzaak om de oude applicaties in de lucht te houden, met als gevolg onnodige beheerkosten. En wanneer er niet wordt vooraf nagedacht over maatregelen om de authenticiteit van informatie te borgen kan deze abusievelijk worden gewijzigd met gevolg dat deze onbetrouwbaar wordt.

1. Er is **actieve sturing** op strategisch niveau op informatiebeheer

|  |  |
| --- | --- |
| [] Ja | [] Nee |

Door op strategisch niveau actief te sturen op informatiebeheer wordt aan de organisatie duidelijk gemaakt welke spelregels er gelden voor informatiebeheer en wie welke verantwoordelijkheden heeft. Daarnaast wordt het informatiebeheer van de organisatie structureel verbeterd door het vaststellen en uitvoeren van een cyclisch kwaliteitssysteem. Aan de hand daarvan worden verbetermaatregelen geprioriteerd en worden mensen en middelen ter beschikking gesteld.

Als het antwoord ‘nee’ is, dan weet de organisatie niet hoe zij in hun organisatie uitvoering moeten geven aan wet-en regelgeving op het gebied van informatiebeheer, hoe de verantwoordelijkheden zijn belegd en op welke wijze daarop wordt gestuurd. Met als gevolg dat er geen actie wordt ondernomen wordt omdat onduidelijk is hoe of door wie dat georganiseerd moet worden.

1. De organisatie gebruikt een **metagegevensschema** om de duurzame toegankelijkheid van overheidsinformatie te realiseren.

|  |  |
| --- | --- |
| [] Ja | [] Nee |

Toelichting: een metagegevensschema zoals bedoeld in NEN-ISO 23081-1, zoals MDTO, beschrijft het verband tussen metagegevens in een logische structuur. Er worden daarin regels vastgelegd over gebruik en beheer van metagegevens. Bijvoorbeeld welke metagegevens verplicht zijn. Door een metagegevensschema vast te stellen en te gebruiken, worden metagegevens op eenduidige wijze in informatiesystemen ingericht en gebruikt.

Als het antwoord ‘nee’ is, dan is het voor de gehele organisatie onduidelijk welke metagegevens moeten worden gebruikt in informatiesystemen en wat het doel daarvan is. Met als gevolg dat er essentiële metagegevens kunnen ontbreken. Dat kan leiden tot slechte vindbaarheid van informatie door gebruikers en maakt het moeilijk om te voldoen aan informatiewet- en regelgeving, zoals de Woo. Ook bestaat er grote kans dat gegevens niet correct kunnen worden geïnterpreteerd. Dit heeft gevolgen voor de kwaliteit van de informatie die je beschikbaar stelt in ketenprocessen en aan externen in het kader van hergebruik.

1. De organisatie voert **actief preserveringsbeleid** om de duurzame toegankelijkheid van overheidsinformatie met een lange bewaartermijn veilig te stellen.

|  |  |
| --- | --- |
| [] Ja | [] Nee |

Toelichting: Hoe langer de overheidsinformatie moet worden bewaard, hoe belangrijker het wordt om goed na te denken over de maatregelen die genomen moeten om overheidsinformatie duurzaam toegankelijk te houden. De levensduur van overheidsinformatie kan bijvoorbeeld veel langer zijn dan die van een applicatie. En bestandsformaten zijn niet in gelijke mate toekomstbestendig. Een organisatie moet daarom over preserveringsbeleid beschikken, waarin uitgewerkt wordt hoe de organisatie omgaat met zaken zoals vervanging, migratie, conversie en emulatie. Dit beleid heeft alleen waarde als het ook actief wordt uitgevoerd.

Als het antwoord ‘nee’ is, dan wordt het moeilijk voor medewerkers in de organisatie om consistent de juiste maatregelen te bepalen en uit te voeren voor de toekomstbestendigheid van overheidsinformatie. Met als gevolg dat overheidsinformatie door technische veroudering op termijn niet meer leesbaar is.

## <kop>Vragen over het bedrijfsproces

Neem samen met de proceseigenaar de volgende vijf stellingen door voor iedere applicatie die het bedrijfsproces ondersteunt.

Tip: Raadpleeg eerst het overzicht van applicaties, als dat er is. In veel gevallen zijn applicaties namelijk aan elkaar gekoppeld. Bijvoorbeeld om onderling informatie uit te wisselen. Soms zorgt een applicatie er dan voor dat bepaalde functionaliteit (bijvoorbeeld: een zoekfunctie) ook binnen andere applicaties werkt.

1. De applicatie wordt gebruikt om overheidsinformatie te **registreren**

|  |  |  |
| --- | --- | --- |
| [] Ja | [] Nee, maar een andere applicatie zorgt hiervoor | [] Nee, en er is ook geen andere applicatie die hiervoor zorgt |

Toelichting: met ‘registreren’ bedoelen we de activiteiten die nodig zijn voor het vastleggen van overheidsinformatie in een informatiesysteem. Denk aan het toebedelen van essentiële metagegevens en het bepalen van de vindplaats waar informatie ook na verloop van tijd terug te vinden is.

Als het antwoord ‘nee’ is, en er is ook geen applicatie die hiervoor zorgt, dan wordt overheidsinformatie niet vastgelegd op een manier die het mogelijk maakt om naast registreren de overige DUTO-processen in te richten. Door vanaf creatie of ontvangst meteen de juiste maatregelen te nemen zoals het vastleggen van benodigde metagegevens, wordt de vindbaarheid en beheerbaarheid van informatie vergroot. Dat is efficiënter dan het achteraf handmatig vastleggen van informatie omdat bij creatie van informatie in een bedrijfsproces veel van de benodigde metagegevens bekend zijn en meteen automatisch toegekend kunnen worden.

1. In de applicatie wordt overheidsinformatie **vernietigd conform bewaartermijnen.**

|  |  |  |
| --- | --- | --- |
| [] Ja | [] Nee, maar een andere applicatie zorgt hiervoor | [] Nee, en er is ook geen andere applicatie die hiervoor zorgt |

Toelichting: met ‘vernietigen’ bedoelen we de activiteiten die nodig zijn om ervoor te zorgen dat overheidsinformatie, na verstrijken van de bewaartermijn in een applicatie volgens de regels wordt vernietigd. Dat betekent onder andere dat er een selectie gemaakt wordt van informatie waarvan de bewaartermijn is verlopen en die vernietigd moet worden. Na het vernietigen is deze informatie niet meer kenbaar, vindbaar of reconstrueerbaar.

Als het antwoord ‘nee’ is, en er is ook geen applicatie die hiervoor zorgt, dan wordt overheidsinformatie langer bewaard dan wettelijk is toegestaan. Met als gevolg dat er bij beveiligingsincidenten of als gevolg van Woo-verzoeken gevoelige informatie kan opduiken die al vernietigd had moeten zijnMet imagoschade als gevolg. Daarnaast leidt onnodige opslag van overheidsinformatie tot hogere kosten.

1. In de applicatie wordt overheidsinformatie **op passende manier bewaard.**

|  |  |  |
| --- | --- | --- |
| [] Ja | [] Nee, maar een andere applicatie zorgt hiervoor | [] Nee, en er is ook geen andere applicatie die hiervoor zorgt |

Toelichting: met ‘bewaren’ bedoelen we de activiteiten die nodig zijn om overheidsinformatie te behouden op een dusdanige manier dat er gedurende de gehele levensduur geen onaanvaardbaar informatieverlies optreedt, de authenticiteit wordt gewaarborgd en de leesbaarheid is gegarandeerd.

Als het antwoord ‘nee’ is, en er is ook geen applicatie die hiervoor zorgt, dan is overheidsinformatie in een applicatie niet duurzaam toegankelijk gedurende de levensduur. Met als gevolg dat de overheidsinformatie in toenemende mate onbruikbaar wordt omdat informatiedragers- en omgevingen verouderen, informatie onvoldoende beschermd is tegen ongewenste wijzigingen en de betrouwbaarheid moeilijk gecontroleerd en gegarandeerd kan worden.

1. De applicatie is in staat om overheidsinformatie **te migreren**

|  |  |  |
| --- | --- | --- |
| [] Ja | [] Nee, maar een andere applicatie zorgt hiervoor | [] Nee, en er is ook geen andere applicatie die hiervoor zorgt |

Toelichting: met ‘migreren’ bedoelen we de activiteiten die nodig zijn om overheidsinformatie te verplaatsen naar een andere applicatie, platform of informatiedrager. Dat kan zijn in het kader van de vervanging van een oude applicatie, het overbrengen naar een e-depot of conversie als onderdeel van preservering. In het geval van migratie naar een andere applicatie of platform betekent het dat een export gemaakt kan worden van informatie die een toekomstige doelapplicatie kan importeren. Dat betekent een export in een bruikbaar en algemeen geaccepteerd formaat, waarbij geen onaanvaardbaar informatieverlies plaatsvindt en onderlinge relaties tussen gegevens nog steeds gelegd kunnen worden.

Als het antwoord ‘nee’ is, en er is ook geen applicatie die hiervoor zorgt, dan kan overheidsinformatie bij vervanging van de applicatie niet gemigreerd worden naar een nieuwe oplossing, blijvend te bewaren overheidsinformatie niet worden overgebracht naar een e-depot en informatie niet worden gemigreerd naar nieuwe dragers als de oorspronkelijke verouderd raken. Dit leidt tot extra beheerkosten, als beheer überhaupt nog mogelijk is.

1. De applicatie stelt overheidsinformatie **ter beschikking aan rechthebbenden.**

|  |  |  |
| --- | --- | --- |
| [] Ja | [] Nee, maar een andere applicatie zorgt hiervoor | [] Nee, en er is ook geen andere applicatie die hiervoor zorgt |

Toelichting: met ‘ter beschikking stellen’ bedoelen we de activiteiten die nodig zijn om overheidsinformatie te leveren aan gebruikers ten behoeve van (her)gebruik. Het kan daarbij gaan om een medewerker van een overheidsorganisatie die overheidsinformatie raadpleegt voor de uitvoer van zijn taken en informatie die mogelijk gedeeld wordt in een ketenproces. Het kan ook gaan om het ter beschikking stellen van overheidsinformatie in het kader van de wet hergebruik overheidsinformatie (Who).

Als het antwoord ‘nee’ is, en er is ook geen applicatie die hiervoor zorgt, dan kan er door medewerkers of andere rechthebbenden geen gebruik worden gemaakt van de overheidsinformatie. Met als gevolg dat medewerkers van een overheidsorganisatie hun taken niet kunnen uitvoeren en kansen op het gebied van hergebruik niet worden benut

# Stap 3 – Beoordeel de resultaten

Neem de resultaten door met de proceseigenaar. Het is niet de bedoeling om met een opgeheven vinger de proceseigenaar te confronteren met de tekortkomingen. Het gesprek moet de proceseigenaar helpen om inzicht te geven in de risico’s en deze gezamenlijk te wegen en te beoordelen. Door de proceseigenaar mee te nemen in de beoordeling van de resultaten draag je ook bij aan een grotere bewustwording op het gebied van duurzame toegankelijkheid. Door met de proceseigenaar mee te denken en begrip te tonen voor zijn positie, laat je ook zien dat je als informatieprofessional een serieuze gesprekspartner bent die begrijpt dat er keuzes gemaakt moeten worden.

* Als het antwoord op iedere stelling ‘ja’ luidt, dan is dat goed nieuws. Op hoofdlijnen wordt dit proces ondersteund door informatiebeheer dat goed ingericht is. De risicobeoordeling kan een bepaalde zorg wegnemen.
* Wanneer je op specifieke stellingen reageert met ‘nee’, kan er een risico bestaan. De volgende vraag is: hoe **ernstig** is dat risico? Een **ernstig risico** is er als het **waarschijnlijk** is dat een bepaalde gebeurtenis plaatsvindt en dat de **impact** groot is wanneer dat gebeurt.
  + Soms gaat het om risico’s waarbij de waarschijnlijkheid laag is en de eventuele impact gering. In zulke gevallen is het een legitieme keuze om een bepaald risico te accepteren.
  + Als je vaststelt dat er ernstige risico’s bestaan, is het tijd om actie te ondernemen. De antwoorden op de vragenlijst laten zien waar de meest dringende actie nodig is. Het kan bijvoorbeeld gaan om een organisatiebreed probleem dat onder de verantwoordelijkheid van de directie valt. Of om een applicatie-specifiek probleem dat een actie vereist van de proceseigenaar.

# Stap 4 – Deel je conclusies

Stel een risicorapportage op waarin je de resultaten van de vragenlijst samenvat en ook de mogelijke oplossingen voor ernstige risico’s beschrijft.

Een risicobeoordeling is een instrument dat helpt bij het prioriteren van maatregelen. Bij een quickscan geldt in nog sterkere mate dat je alleen focust op de belangrijkste risico’s. Niet elke risico hoeft in detail te worden beschreven en niet alles hoeft te worden aangepakt. Beperk je bij de uitwerking van oplossingen tot een selectie van de grootste risico’s.

Voor deze risico’s stel je vervolgens haalbare oplossingen voor, daarbij past een zeker pragmatisme. Als bijvoorbeeld blijkt dat er een grote achterstand is bij het vernietigen, kun je een pragmatische aanpak voorstellen door van verschillende bewaartermijnen de langste als uitgangspunt te nemen bij vernietiging (in afstemming met toezichthouder). Of bij het toevoegen van ontbrekende functionaliteit aan een applicatie kan wellicht worden gewacht tot de aanschaf van de vervangende applicatie.