

Hoe digitaal weerbaar is de gemeente Raalte?

Offerte voor een rekenkameronderzoek bij de gemeente Raalte

2 maart 2022

Offertenummer 4321



Gemeente Raalte

PBLQ

Inhoud



- ▼ Aanleiding
- ▼ Onze visie op uw vraag
- ▼ Vraagstelling
- ▼ Voorgesteld normenkader
- ▼ Onze aanpak & resultaat
- ▼ Planning
- ▼ Het team
- ▼ Referenties
- ▼ Investering
- ▼ Overleg en procedures
- ▼ Slotbepalingen

PBLQ

verbinders in de
informatiesamenleving

Over PBLQ

PBLQ is een onafhankelijk adviesbureau voor de publieke sector. Wij zijn gecommitteerd aan een goed functionerende overheid in een moderne samenleving. Wij verbinden beleid, bestuur en uitvoering in het publieke domein. Opdrachtgevers schakelen ons in voor (rekenkamer-)onderzoek, advies, interim-management en opleidingen.

Met onze rekenkameronderzoeken leveren wij een belangrijke bijdrage aan de kwaliteit van het lokaal bestuur. Inzicht in de context en opbrengsten van beleid brengt raadsleden beter in positie om hun vertegenwoordigende, controlerende en kaderstellende verantwoordelijkheden waar te maken. In de praktijk blijkt dat een gedegen uitvoering van een rekenkameronderzoek zorgvuldige en deskundige ondersteuning vereist van bureaus die de bijzondere positie van rekenkamers begrijpen. Wij bieden die als geen ander.

In de afgelopen tijd hebben wij een groot aantal rekenkamers ondersteund bij een grote variëteit aan thema's, zoals privacybeleid en informatiebeveiliging, burgerparticipatie, subsidiebeleid, lokaal mediabeleid en de invoering van de Omgevingswet.

Aanleiding

Gemeenten, onderwijsinstellingen en andere organisaties in het publieke domein zijn steeds vaker doelwit van cybercriminaliteit. Een geslaagde cyberaanval kan een organisatie veel geld kosten, de dienstverlening in gevaar brengen en ten koste gaan van het imago en het vertrouwen van burgers. Er is publieke organisaties daarom veel aan gelegen de informatiebeveiliging goed op orde te hebben.

Ook bij gemeenten is de aandacht voor de beveiliging van informatie de laatste jaren sterk toegenomen. Gemeenten hebben de bedrijfsvoering steeds verder gedigitaliseerd en wisselen intern, met andere organisaties en met burgers en ondernemingen digitaal veel gegevens uit. Omdat het bij deze uitwisselingen vaak gaat om persoonsgegevens en andere gevoelige informatie, is het voor gemeenten van extra groot belang om de informatiebeveiliging goed op orde te hebben.

Cybercriminelen worden steeds slimmer en de techniek steeds geavanceerder. Er moet dus rekening worden gehouden met het daadwerkelijk plaatsvinden en eventueel slagen van digitale aanvallen. Omdat 100% veiligheid niet bestaat, heeft het de voorkeur om in een organisatie te kijken naar de digitale weerbaarheid. Een digitaal weerbare organisatie kan potentiële incidenten vroegtijdig signaleren, maar ook tijdig adequate maatregelen treffen om de gevolgen van een incident te beperken.

De Rekenkamercommissie van de gemeente Raalte heeft PBLQ gevraagd onderzoek te doen naar de digitale weerbaarheid, om mogelijke cyberaanvallen buiten de deur te kunnen houden en in geval van een daadwerkelijk incident adequaat te kunnen reageren. Wij voeren die opdracht graag voor u uit.

PBLQ

NIEUWS HACK BIJ GEMEENTE HOF VAN TWENTE

'Hello, need data back? Contact us fast.' Hackers eisen geld van gemeente Hof van Twente

De criminele groepering die de backsystemen van de gemeente Hof van Twente in gijzeling heeft, wil 750 duizend euro om de bestanden weer vrij te geven. De

hacke
geme
admi
burge

HvA en UvA getroffen door cyberaanval

Huib M

De Hogeschool van Amsterdam (HvA) en Universiteit van Amsterdam (UvA) zijn doelwit van een cyberaanval. Onbekenden hebben zich toegang verschaft tot de ICT-omgevingen van de HvA en UvA, schrijft de universiteit.

Amsterdam sluit cruciale computersystemen uit angst voor hackers

Amsterdam heeft enkele cruciale computersystemen halsoverkop afgesloten, omdat ze nog altijd lek blijken te zijn. Ook andere gemeentes, waaronder Rotterdam en Den Haag, hebben ingegrepen.

Grote cyberaanval op gemeente Den Haag: parkeersystemen en websites liggen deels plat

Den Haag is sinds dinsdag de dupe van een grote, cyberaanval. Daarbij vallen onbekenden de servers en systemen van de gemeente van buitenaf aan om ze volledig plat te leggen. Op dit moment werken bijvoorbeeld gemeentelijke websites, de systemen van de balies in het stadhuis en de parkeersystemen niet goed.

Onze visie op uw vraag

Digitale veiligheid gaat in onze visie niet alleen over de beveiliging van de informatiesystemen van de gemeente. Het gaat over het geheel van maatregelen, processen en procedures die de beschikbaarheid, integriteit en vertrouwelijkheid van informatie en informatiesystemen waarborgen. Digitale weerbaarheid gaat niet alleen over de oorzaken en het voorkomen van mogelijke incidenten, maar ook over de respons en de wijze waarop de gemeente er van leert. We bekijken het vraagstuk dan ook integraal, waarbij we ons richten op de verschillende activiteiten die de gemeente Raalte moet uitvoeren om gegevens te beschermen, maar ook op de activiteiten die van belang zijn bij de respons op een daadwerkelijk incident.

We laten ons bij het onderzoek inspireren door het *NIST Framework for Improving Critical Infrastructure Cybersecurity*. Dit raamwerk identificeert verschillende kernactiviteiten die informatiebeveiligingsrisico's adresseren. Het biedt een kader waarmee de verschillende activiteiten ten behoeve van de digitale weerbaarheid geanalyseerd kunnen worden.

Door de kernactiviteiten uit het kader centraal te stellen, krijgen we inzicht in de voorbereiding van de gemeente op een incident, hoe het deze kan detecteren en hoe de gemeente er op kan reageren en ervan kan herstellen. Deze aanpak geeft een beeld van de samenhangende maatregelen die de gemeente heeft genomen.

The logo consists of the letters 'PBLQ' in a bold, dark blue, sans-serif font. The letters are closely spaced. To the right of the letters, there is a light blue triangular graphic element pointing towards the top right corner of the page.

verbinders in de
informatiesamenleving

In het onderzoek voor de gemeente Raalte zien wij nog een aantal belangrijke aandachtspunten die we betrekken in het onderzoek:

- **De bescherming van persoonsgegevens.** Voor gemeenten achten wij de bescherming van persoonsgegevens van groot belang omdat het gevoelige gegevens zijn en de bescherming daarvan een groot afbreukrisico voor een gemeente vormt.
- **De samenwerking van de gemeente Raalte** met de gemeenten Deventer en Olst-Wijhe op het gebied van bedrijfsvoering en ICT, en meer specifiek de onderlinge afspraken en afhankelijkheden in die samenwerking. De digitale weerbaarheid van de gemeente Raalte wordt namelijk deels ingevuld via deze samenwerking.
- **De rol van de gemeenteraad bij de digitale weerbaarheid.** Door het gemeentelijke beleid voor de bescherming van persoonsgegevens en andere informatie te toetsen op doeltreffendheid, doelmatigheid en rechtmatigheid, geeft de raad invulling aan haar controlerende rol. Vanuit de volksvertegenwoordigende rol is het voor de raad van belang de weerbaarheid tegen cybercriminaliteit te toetsen en daarbij het belang en perspectief van de inwoner mee te nemen en op basis hiervan eventueel nadere kaders te stellen. Wij betrekken de rol van de raad dan ook expliciet in ons onderzoek.

Vraagstelling

In de beoordeling van de digitale weerbaarheid ligt de nadruk vaak op het identificeren van bedreigingen en het nemen van maatregelen. Wij menen echter dat een digitaal weerbare gemeente ook adequaat handelt indien een incident zich daadwerkelijk voordoet.

Wij komen dan ook tot de volgende **hoofdvraag**:

Hoe is het gesteld met de beveiliging van persoonsgegevens en andere informatie en de voorbereiding op incidenten in de gemeente Raalte?

Aan de hoofdvraag verbinden wij de volgende deelvragen:

1. Hoe weerbaar zijn de digitale systemen van de gemeente Raalte tegen cybercriminaliteit?
2. Hoe is de samenwerking van Raalte met Deventer en Olst-Wijhe van invloed op de informatiebeveiliging in de gemeente Raalte?
3. Hoe beveiligingsbewust zijn de medewerkers van de gemeente Raalte als het gaat om persoonsgegevens en andere informatie?
4. Hoe is de gemeente voorbereid in de respons op daadwerkelijke incidenten?
5. Waar liggen de grootste risico's en hoe kan de gemeente Raalte hierin verbeteringen aanbrengen?
6. Welke controle- en sturingsmogelijkheden heeft de gemeenteraad bij informatiebeveiliging en worden deze ook ingezet?

Voorgesteld normenkader

In onze werkwijze hanteren wij een normenkader dat bijdraagt aan het beantwoorden van de onderzoeksvragen. Het normenkader is ingedeeld op basis van het *NIST Framework for Improving Critical Infrastructure Cybersecurity*.

Activiteiten	Norm met betrekking tot weerbaarheid tegen cybercriminaliteit en bescherming van (persoons-)gegevens
Identificeer (Identify)	- De gemeente heeft een duidelijk beleid en uitvoeringskader bij hoe zij omgaat met cybersecurity risico's van/aan systemen, mensen, gegevens, informatie en middelen. - De gemeente heeft de belangrijkste processen, systemen en risico's in beeld. - De gemeente stelt dit risicobeeld periodiek bij op basis van (onder andere) informatie over dreigingen en veranderingen in processen en systemen.
Bescherm (Protect)	- De gemeente heeft maatregelen ontwikkeld en geïmplementeerd om te zorgen voor de continuïteit en bescherming van kritische processen en dienstverlening. - Medewerkers werken volgens de maatregelen en zijn bewust van eigen handelen en verantwoordelijkheid.
Detecteer/Ontdek (Detect)	- De gemeente heeft maatregelen ontwikkeld en geïmplementeerd om cybersecurity incidenten te detecteren. - Er is een procedure voor het melden van incidenten en medewerkers kennen en gebruiken deze procedure. - Er is een escalatieprocedure richting de directie, college en gemeenteraad.
Reageer (Respond)	- De gemeente heeft maatregelen/acties/processen geïmplementeerd om actie te (kunnen) ondernemen tegen/na potentiële cybersecurity incidenten. Het gaat bijvoorbeeld om een incidentrespons procedure en nood/continuïteitsplannen. - De gemeente toetst, oefent en evalueert deze maatregelen/acties/processen periodiek (zoals het oefenen van een cyberaanval). - De rollen en verantwoordelijkheden van functionarissen, directie en raad zijn vastgelegd en in de praktijk bekend.
Herstel (Recover)	- De gemeente werkt planmatig aan weerbaarheid en is voorbereid op activiteiten ten behoeve van herstellen van processen en dienstverlening. - Incidenten op het gebied van informatiebeveiliging of cybersecurity worden geëvalueerd en leiden tot structurele verbetermaatregelen.
Algemeen	- De raad wordt periodiek geïnformeerd over de digitale weerbaarheid van de gemeente en de ontwikkelingen op dat vlak. - De informatieverstrekking aan de raad biedt de raad voldoende mogelijkheden om de sturende en controlerende verantwoordelijkheden waar te maken. - De maatregelen die de gemeente neemt worden periodiek getoetst, geoefend en/of geëvalueerd.

Het is onze gewoonte om dit normenkader bij de start van het onderzoek te bespreken met de opdrachtgever en daarna het normenkader definitief vast te stellen.

Onze aanpak & resultaat

PBLQ

verbinders in de
informatiesamenleving



Startbijeenkomst



Inventarisatie feitelijke situatie



Verkenning van de praktijk



Raadsbijeenkomst



Eindrapportage

Activiteiten

PBLQ en de Rekenkamer-commissie bespreken onder meer het volgende:

- Vaststelling onderzoeksvragen, normenkader en processen die als casus onderzocht worden;
- Vaststellen te interviewen personen;
- Afspraken over de planning;
- Aansluiting op de raadsagenda.

Wij stellen voor om ook een startbijeenkomst te organiseren voor belangstellende raadsleden, betrokken medewerkers van de organisatie, alsmede de verantwoordelijk portefeuillehouder en secretaris.

We inventariseren de beleidsuitgangspunten en de bijbehorende ambities voor de bescherming van (persoons-)gegevens tegen cybercriminaliteit. We inventariseren de genomen maatregelen op de verschillende fasen van het *NIST* raamwerk door middel van bestudering van de relevante beleidsdocumenten en gesprekken met diverse sleutelpersonen.

In deze stap verbreden en verdiepen we de inzichten die we hebben opgedaan bij het bestuderen van het beleid van de gemeente. We maken de koppeling van de 'papier situatie' van beleid en uitvoering naar de uitwerking in de praktijk, aan de hand van casuïstiek. Door middel van casusbesprekingen gaan we dieper in op de bescherming tegen cybercriminaliteit in praktijk. We gebruiken hiervoor het *NIST* raamwerk.

Aan het eind van deze fase verdiepen wij het inzicht in de ervaringen van alle betrokkenen door middel van een convergentiesessie.

Alhoewel het vraagstuk zich primair toespitst op de ambtelijke organisatie, is het ook belangrijk om de raad te betrekken. Immers, de raad stelt de kaders en voert de controle over het beleid uit. Middels een raadsbijeenkomst gaan we met raadsleden in gesprek aan de hand van (fictieve) casuïstiek hoe zij een goede rol kunnen pakken en wat dat betekent voor de bescherming van (persoons-)gegevens.

We leveren eerst een conceptrapport aan de Rekenkamercommissie.

We verwerken daarna de feedback van de Rekenkamercommissie en daarna maken wij een definitief rapport voor ambtelijk en bestuurlijk wederhoor.

Resultaat

Het onderzoek gaat goed voorbereid van start. Alle betrokkenen hebben inzicht in doel en onderliggend proces. Dit bevordert draagvlak en betrokkenheid bij het uitvoeringsproces

Op basis van relevante documenten en gesprekken krijgen wij een beeld van beleid en uitvoering en kunnen we gericht vragen stellen in de volgende fase.

Op basis van casussen wordt intensief aandacht besteed aan het beveiligingsbewustzijn en de ervaringen van deelnemers in de praktijk. Daarnaast wordt een inventarisatie gemaakt van de voorbereiding op incidenten. Door te reflecteren wordt aandacht besteed aan algemene lessen.

Inzicht in de opvattingen van raadsleden over hun rol en positie bij bescherming tegen cybercriminaliteit.

Bondige rapportage met de bevindingen, conclusies en aanbevelingen. Indien gewenst vervatten wij de bestuurlijke rapportage in een visueel aantrekkelijke folder.

1. Startbijeenkomst

- ▶ In alle rekenkameronderzoeken die we uitvoeren, beginnen we met een gezamenlijke startbijeenkomst. Tijdens de startbijeenkomst spreken we met de leden van de Rekenkamercommissie over het voorliggende onderzoek. Hierbij komen onder meer de volgende onderwerpen aan bod:
 - De specifieke onderzoeksvragen en het normenkader en een eventuele aanscherping daarvan;
 - De te onderzoeken processen t.b.v. casuïstiek en vaststelling te interviewen personen;
 - Afspraken over de planning;
 - Aansluiting op de raadsagenda. Wij streven naar een optimale doorwerking van het onderzoek en concrete aanbevelingen voor de raad om in de toekomst op te sturen.
- ▶ Wij stellen voor om ook een startbijeenkomst te organiseren voor belangstellende raadsleden, betrokken medewerkers van de organisatie, alsmede de verantwoordelijk portefeuillehouder en secretaris.
- ▶ Bovendien, zo is onze ervaring, versterkt een startbijeenkomst het draagvlak binnen de organisatie voor het onderzoek en daarmee de acceptatie van de bevindingen inclusief de daaraan verbonden conclusies en aanbevelingen.

2. Inventarisatie feitelijke situatie

- ▶ In een eerste fase van het onderzoek bestuderen wij de belangrijkste documenten in het kader van de bescherming tegen cybercriminaliteit. Wij zullen uit deze documenten een overkoepelend beeld distilleren en maken hierbij gebruik van het NIST raamwerk.
- ▶ Deze 'papieren informatie' wordt aangevuld met ca. acht interviews met medewerkers van de gemeente die betrokken zijn bij de bescherming tegen cybercriminaliteit. Wij denken hierbij aan gesprekken met:
 - De verantwoordelijk portefeuillehouder
 - De gemeentesecretaris
 - Hoofd Informatievoorziening
 - De beveiligingsfunctionaris / CISO
 - De functionaris gegevensbescherming
 - Enkele afdelingshoofden die verantwoordelijk zijn voor cruciale processen binnen de gemeente
 - Diverse betrokkenen bij de samenwerking met Deventer en Olst-Wijhe, zowel in Raalte zelf als bij de andere gemeenten.
- ▶ De gesprekspartners sturen wij vooraf informatie over het onderzoek en de onderwerpen die we in het interview zullen bespreken.

3. Verkenning van de praktijk



PBLQ

verbinders in de
informatiesamenleving

- ▶ In deze fase kijken we hoe het beleid zoals dat in de vorige fase is geïnventariseerd in de praktijk wordt uitgevoerd. We selecteren daarvoor in overleg met de rekenkamercommissie twee casussen. Voor deze casussen maken wij een analyse aan de hand van de processtappen (volgens het NIST raamwerk) die in het normenkader zijn opgenomen. De casussen zijn processen waar bijvoorbeeld de bescherming van (persoons-)gegevens en/of continuïteit van dienstverlening essentieel is. Suggesties voor te onderzoeken casuïstiek zijn bijvoorbeeld het betalen van uitkeringen, de gemeentelijke belastingen (eventueel in een samenwerkingsverband), diensten zoals afvalverwerking en beheer van sluizen en verkeerslichten, de loketten (publieke zaken en/of dienstverlening) of de gemeentelijke taak bij de verkiezingen. In de context van het onderzoek is het zinvol dat tenminste één van die casussen ook betrekking heeft op de samenwerking met Deventer en Olst-Wijhe.
- ▶ We verkennen de casuïstiek aan de hand van workshops met sleutelpersonen (betrokken medewerkers van de gemeente en eventueel ook medewerkers van Deventer en/of Olst-Wijhe en ketenpartners). Zo verdiepen we ons inzicht en toetsen we de bevindingen uit de documentstudie aan de praktijk. De workshop biedt ook de mogelijkheid om intensief aandacht te besteden aan het beveiligingsbewustzijn van de medewerkers van de gemeente Raalte en expliciet aandacht te besteden aan de voorbereiding op mogelijke incidenten.
- ▶ De verkregen informatie relateren we aan de onderzoeksvragen en het normenkader, waardoor we tot een beredeneerde en onderbouwde beoordeling van de praktijk van de bescherming tegen cybercriminaliteit (rond de casussen) te kunnen komen. Daardoor ontstaat ook een meer algemeen inzicht in en een basis voor de beoordeling van de weerbaarheid.
- ▶ Om het inzicht in de ervaringen van alle betrokkenen te verdiepen ronden wij deze fase af met een zogenaamde convergentiebijeenkomst. Voor deze bijeenkomst nodigen wij de betrokkenen bij de bestudeerde processen uit. In die bijeenkomst leggen wij eerst aan alle deelnemers enkele van de opgedane inzichten voor en verzoeken hen daarop te reflecteren. Vervolgens zullen wij de deelnemers verzoeken om na te denken over algemene lessen en verbeterpunten die uit de ervaringen kunnen worden getrokken.

4. Bijeenkomst met de raad



- De raad heeft vanuit de kaderstellende, controlerende en volksvertegenwoordigende verantwoordelijkheden een belangrijke rol, ook op het gebied van informatiebeveiliging. Het is voor ons een gebruikelijke aanpak om de raad binnen het onderzoek te betrekken. Daarbij houden wij nadrukkelijk rekening met de drukbezette agenda van raadsleden en in het bijzonder de gemeenteraadsverkiezingen zowel door middel van de werkvorm als door een eventuele afstemming met een reeds geplande vergadering binnen de raadsagenda.
- Om raadsleden uit te dagen om hun sturende en controlerende ambities te formuleren, leggen wij hen een fictieve casus uit onze eigen 'gemeente Fonkelveen' voor. Deze werkvorm maakt het mogelijk om uit de dagelijkse politieke context te stappen.
- In de nabespreking van de casus worden de door de raadsleden geformuleerde inzichten en adviezen gerelateerd aan de bestaande praktijk en zo worden de verschillen tussen de huidige en gewenste situatie duidelijk.
- De bijeenkomst ronden we dan af met een gesprek over hoe de huidige situatie dichterbij de buurt van de gewenste situatie kan worden gebracht. Daaruit leiden wij voor het onderzoek relevante conclusies en aanbevelingen af.

5. Eindrapportage



- In de 'feitenrapportage' beschrijven wij de gevolgde werkwijze in het onderzoek en de op deze wijze verkregen bevindingen. Deze feitenrapportage leggen wij, na vaststelling door de rekenkamercommissie, voor aan de organisatie ten behoeve van 'ambtelijk hoor en wederhoor'.
- Conform gebruikelijke procedures kan er hiervoor sprake zijn van een schriftelijke reactie, ook kan er gekozen worden voor een bijeenkomst met betrokkenen. Op basis van onze ervaringen geven wij de voorkeur aan een bijeenkomst. Na verwerking van de ambtelijke reacties maken wij de feitenrapportage definitief.
- Vervolgens stellen wij een bestuurlijke rapportage op, waarin de bevindingen worden beoordeeld en de onderzoeksvragen worden beantwoord. Deze bestuurlijke rapportage wordt na vaststelling door de rekenkamercommissie voor bestuurlijk wederhoor voorgelegd aan de colleges van B&W. Desgewenst bieden wij ondersteuning bij het opstellen van een eventueel bestuurlijk nawoord.

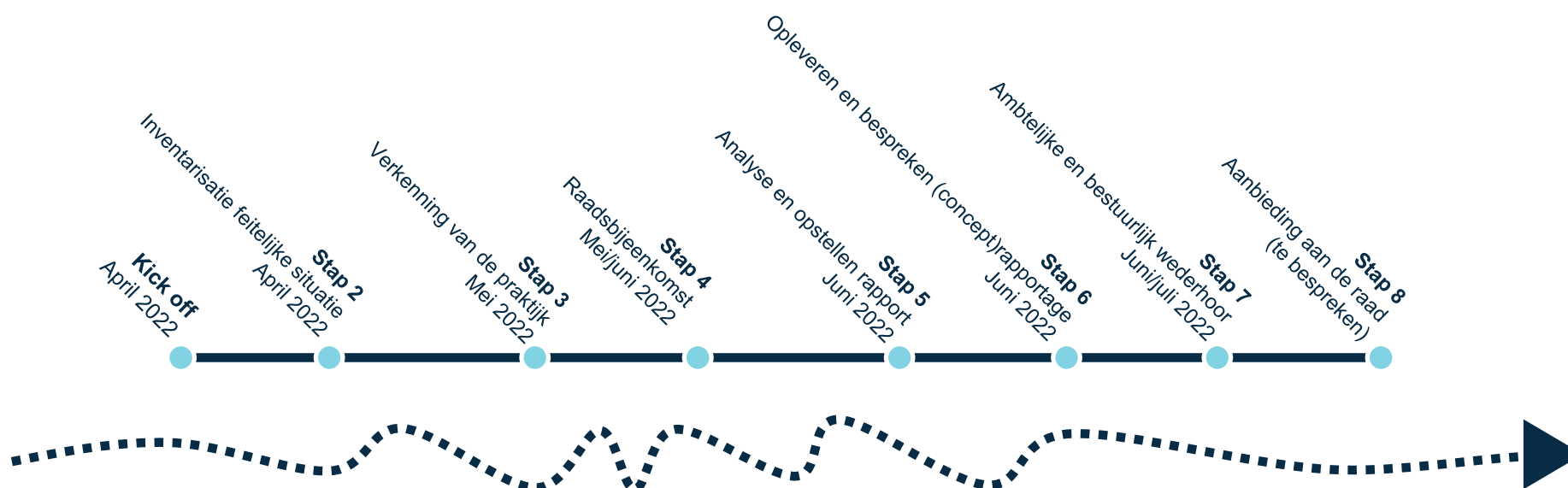
PBLQ

verbinders in de
informatiesamenleving

Planning

PBLQ

verbinders in de
informatiesamenleving



Bovenstaande planning is een indicatie van de doorlooptijd. Het startmoment dient in nader overleg samen vastgesteld te worden.

Of de planning haalbaar is hangt niet alleen af van het startmoment, maar ook van de vraag of er, gezien de gemeenteraadsverkiezingen in maart, het aantreden van een nieuwe raad en de belasting van de (nieuwe) raadsleden vanwege hun inwerkprogramma, voor de zomer een inhoudelijk gesprek met de raad kan plaatsvinden.

Wij hebben ondertussen, vanwege de Corona-omstandigheden, de nodige ervaring opgedaan met alternatieve vormen van overleg (video-conferencing e.d.) en digitale vormen van informatieverzameling en -deling. Bij voorkeur zetten wij deze in voor interviews. De bijeenkomsten voor de casussen en raadsbijeenkomst vinden bij voorkeur op locatie plaats (maar kunnen ook digitaal).