Aanpak

Onze aanpak op hoofdlijnen:

1. **Kick-off met stakeholders** (fysiek of online) In deze bijeenkomst stellen de onderzoekers zich voor, lichten zij de opdracht nader toe en beantwoorden eventuele vragen. Bij voorkeur is de opdrachtgever hierbij aanwezig. De kick-off kan zowel fysieke als online plaatsvinden, de ervaring leert dat deelname het grootst is als deze online wordt aangeboden. De ervaring leert dat de planning uitdagend kan zijn. Daarom stellen wij voor om een kick-off per gemeente te organiseren.

2. **Opvragen & analyseren documentatie** Wij vragen documentatie op waaruit blijkt op welke manier de gemeente informatieveiligheid borgt in haar organisatie. Wij voeren een eerste analyse hierop uit en vragen eventueel aanvullende informatie op. De ontvangen informatie zal tijdens de interviews gebruikt worden om het 'bestaan' en de 'werking' van beheersmaatregelen steekproefsgewijs te toetsen. Aanvullend op het analyseren van de documentatie zal op basis van een openbaar bronnen onderzoek (open source intelligence) vastgesteld worden of er informatiebeveiligingsrisico's bekend zijn.
3. **Technisch onderzoek** (optioneel) In overleg en nader te bepalen. Voor een technisch onderzoek dient afhankelijk van het type onderzoek, diepgang en doorlooptijd rekening gehouden te worden met k€ 6 tot 12, exclusief btw per onderzoek.

4. **Schouw** Wij voeren een schouw op de hoofdlocatie (gemeentehuis/stadskantoor) per gemeente uit om een indruk te krijgen van enerzijds de fysieke (toegangs)beveiliging en anderzijds om het (on)veilig gedrag van medewerkers te kunnen observeren. Het doel van de schouw is het identificeren van risico's in relatie tot de fysieke omgeving (BIO eis).

5. **Interviews** Wij interviewen verschillende stakeholders op strategisch, tactisch en operationeel niveau om aanvullend op de ontvangen informatie een goed beeld te kunnen vormen van het volwassenheidsniveau ten aanzien van informatieveiligheid. Wij willen graag per gemeente spreken met (niet-limitatief): portefeuillehouder informatiebeveiliging, directeur bedrijfsvoering, security team (CISO, ISO, TISO, etc.), domeinmanagers / management (cluster), IT-manager, IT-beheerders (cluster), medewerkers (cluster), HRM en Facilitair. Waar mogelijk worden interviews gecombineerd, ook kan tijdens het onderzoek blijken dat er nog andere medewerkers geïnterviewd moeten worden om het beeld te completeren. Wij gaan uit van acht interviews per gemeente.

6. **Rapporteren** DMC levert een totaalrapport op voor MSSW en per gemeente een afzonderlijke rapport. Wij zullen in een bijlage van de respectievelijke rapportages de namen en rol/functie van gesproken medewerkers opnemen en verder geen naar personeel herleidbare informatie verwerken, zoals het citeren van uitspraken of interview verslagen. Verder nemen wij per gemeente een overzicht van alle ontvangen documentatie op.
7. **Presenteren** Indien gewenst kunnen de onderzoekers de bevindingen digitaal of fysiek op locatie nader toelichten.

In onderstaande tabel is indicatief uitgewerkt welke activiteiten (niet-limitatief) er door de rekenkamer/gemeente en DMC geleverd moeten worden om het onderzoek binnen een redelijke termijn te kunnen uitvoeren en afronden, inclusief een uren inschatting op basis van onze ervaring met

vergelijkbare opdrachten. Op basis van deze activiteiten kan indicatief de doorlooptijd worden afgeleid, rekening houdend met afzeggingen, vakanties en dergelijke.

Planning & uitvoering

U heeft aangegeven de werkzaamheden graag op korte termijn te willen laten starten. Wij willen graag aan uw verzoek te voldoen en maximale flexibiliteit bieden. Wij houden voor dit onderzoek rekening met een doorlooptijd van drie tot vier maanden. Bij een start begin juli vindt de oplevering eind november plaats, rekening houdend met het zomerreces. Hieronder een de indicatieve planning:

Activiteit	Jul	Aug	Sep	Okt	Nov	Dec
Kick-Off	■					
Opstellen overzicht te analyseren documenten	■					
Aanleveren verzamelde documenten	■	■				
Analyseren opgevraagde en aangeleverde documenten		■	■			
Aanleveren overzicht stakeholders	■					
Inplannen afspraken (interviews, managementsessie en eindpresentatie)	■	■				
Interviews (8x per gemeente)		■	■	■		
Schouw op locatie		■				
Technisch assessment (optioneel)			■	■	■	
Opstellen rapportage en bespreking concept met opdrachtgever					■	■
Eindpresentatie rapport aan opdrachtgever en stakeholders						■

Wat levert het op?

- Inzicht in de volwassenheid t.a.v. informatiebeveiliging per gemeente;
- Inzicht in kwetsbaarheden en daaraan verbonden risico's per gemeente;
- Aanbevelingen voor het (beter) beveiligen van de informatie(systemen) van de gemeente;
- Aanbevelingen voor het verbeteren van de informatieveiligheid per gemeente;
- Rapport per gemeente met daarin alle feiten en concrete aanbevelingen;
- Presentatie en mondelinge toelichting op locatie aan de stakeholders.