Bijlage J – Aanpak en aansturing van de uitvoering van het Beveiligingsplan

Programmatisch sturen

De door te voeren verandering grijpt in de hele organisatie in:

- Risico Management is een belangrijk ingrediënt en de Business is eindverantwoordelijk.
  Bij informatiebeveiliging is de lijn nu nog weinig betrokken, en de huidige invulling van Risico Management is summier.
- Na een eerste grondige Risico Analyse zal blijken dat er veel werk te doen is. Heel veel werk voor mensen die al druk zijn. Er zal verstandig geprioriteerd moeten worden, met impact op andere projecten en activiteiten.
- Het high-level beleid moet op veel gebieden nader worden uitgewerkt, geoperationaliseerd en gehandhaafd. Ook bestaand beleid moeten worden gehandhaafd of aangepast. Voor de nadere uitwerking moet draagvlak gecreëerd worden. Handhaven vereist steun van de lijn omdat dit mensen gaat beperken en dwingen.
- Management Systemen – met strikte processen en continue verbetering – bewegen zichzelf uiteindelijk op of rond Maturity Level 4.
  Om zonder bovenmatige inspanning ook op termijn succesvol te kunnen zijn is het aan te raden dat de context (de gemeente) zich beweegt naar Maturity Level 3.

In verband met bovenstaande punten is het principieel dat de Business eigenaarschap neemt, en dat het onderwerp in samenhang met alle andere werk in de organisatie wordt aangestuurd.

Opdrachtgever en stuurgroep

De CIO is opdrachtgever.

Het directieteam is de stuurgroep. Hier worden besluiten genomen die een grote en organisatie-brede impact hebben. De stuurgroep vergadert eens per 3 maanden.

Operationele sturing gebeurt door het CIO team. Dit onderwerp staat eens per 4 weken op de agenda.

Gefaseerde aanpak

Fase 1

Betrekken van de Business, te beginnen bij CIO-team, Directieteam en Wethouder. Uitgangspunten vaststellen.

Belangrijk hier zijn

- Overeenstemming over de opdracht, de keus van het ambitieniveau en daarvoor nodige middelen.
- Overeenstemming over de aansturing
- Overeenstemming over de aanpak op hoofdlijnen
- Overeenstemming over gewenste rapportages
- Overeenstemming over de gewenste onafhankelijke assurance
- Procesafspraken voor het opstellen, vaststellen en in uitvoer brengen van aanvullend beleid inclusief de handhaving ervan. In het afgesproken proces moet de omschakeling plaatsvinden van de gemak-gerichte huidige situatie naar de gewenste risico-bewuste situatie.
- Afspraken omtrent de communicatie met afdelingsmanagers, personeel, college, gemeenteraad.

- Procesafspraken voor het stellen van prioriteiten bij strijdige belangen met onderwerpen buiten het programma.
- 2nd Opinion over de voorgestelde opdracht – ambitie – aanpak – organisatie – sturing

Fase 2

Sturing nemen. Opstellen en starten met de uitvoering van het eerste beveiligingsplan

In deze fase horen de volgende activiteiten:

- Direct vanaf het begin:
    - Sturing nemen op Security aspecten die worden opgeleverd door project Any.
    - Sturing nemen op de activiteiten rond "Niet testen met persoonsgegevens"
    - Sturing nemen op de voortgang van interne en externe verantwoordingsactiviteiten.
- Ankerpunten in de organisatie creëren:
    - Formele "Eigenaren" van informatie, processen en applicaties benoemen, en definiëren wat deze rol betekent, en hoe deze rol zich verhoudt tot de lijnmanagers als het gaat om Security en Privacy.
    - In iedere afdeling een contactpersoon aanwijzen die namens de afdelingsmanager actiehouder is als punten aan de orde komen.
- Voor het verlagen van risico's:
    - Activiteiten baseren op de beoordeelde Risico scenario's
- Voor Compliance:
    - Activiteiten baseren op het voorkomen van mogelijke issues:
        - In kaart brengen en aansturen van ingediende verbeterplannen en escalatieprocessen van toezichthouders.
        - In kaart brengen van bestaande Gaps ten opzichte van verplichte normen.
- Onderwerpen ordenen en prioriteren op basis van
    - Risico
    - Resources
    - Relaties / interactie met andere trajecten
    - Vrijheidsgraden van Haarlem om zelf de planning te bepalen
- Opstellen van het beveiligingsplan en fasering waarin risico's en resources worden geoptimaliseerd.
  (Eén van de onderdelen zal zijn om op veel terreinen snel te komen met aanvullend beleid.)
- Expliciete acceptatie van risico's die samenhangen met de gekozen fasering.
- 2nd Opinion over het opgestelde plan, de gemaakte keuzes en de vastlegging van de overwegingen bij deze keuzes.

Fase 3

Uitvoeren en zo nodig bijstellen van het plan. Sturen van programma en lijnissues in samenhang. Rapporteren.

Redenen om bij te stellen kunnen o.a. voortkomen uit:

- De root-cause analyses van incidenten.
- Bevindingen en aanbevelingen van audits
- Resultaten van self-assessments.
- Gewijzigde externe context, waaronder wet- en regelgeving
- Gewijzigde interne context, waaronder andere politieke prioriteiten.