Gemeente Haarlem

Informatienota

Onderwerp Rapportage volwassenheid Informatiebeveiliging januari 2021	
Nummer	2021/55774
Portefeuillehouder	Botter, J.
Programma/beleidsveld	6.2 Gemeentelijk bestuur
Afdeling	CC
Auteur	Hut, F.J.
Telefoonnummer	023-5114955
Email	fhut@haarlem.nl
Kernboodschap	Het resultaat van het volwassenheidsonderzoek Informatiebeveiliging wordt in deze nota met de raadscommissie gedeeld. Haarlem krijgt op dit moment de score 2. Er is duidelijk gewerkt aan het opzetten van een pragmatische basis, maar veel aspecten zijn nog informeel of hebben nog niet de grondigheid die door een ISO-norm wordt verwacht. Aanbevelingen worden opgepakt. Jaarlijks wordt het onderzoek herhaald zodat voortgang gevolgd kan worden.
Behandelvoorstel voor commissie	Het college stuurt de informatienota ter kennisname naar de commissie Bestuur. Bij de behandeling van de Informatienota Informatiebeveiliging najaar 2020 (2020/948418) in december is toegezegd dat deze informatie zal worden nagezonden.
Relevante eerdere besluiten	Informatienota Informatiebeveiliging najaar 2020 (2020/948418) Referentiekader voor volwassenheid van Informatiebeveiliging (2020/854267)
Besluit College d.d. 23 maart 2021	1. Het college stelt de informatienota aan de commissie vast. 2. Op de bij deze nota behorende bijlage 1 geheimhouding op te leggen aan de commissie Bestuur op grond van artikel 86 van de Gemeentewet, vanwege de bescherming van de economische of financiële belangen van de gemeente, als bedoeld in artikel 10, tweede lid, aanhef en onder van de Wet Openbaarheid van Bestuur. de secretaris, de burgemeester,

Inleiding
Het resultaat van het volwassenheidsonderzoek Informatiebeveiliging wordt hierbij met de raadscommissie gedeeld. Dit is nagekomen informatie zoals is aangekondigd bij de informatienota informatiebeveiliging najaar 2020 (2020/948418)

Volgens collegebesluit (2020/854267) is de internationale ISO 27001 standaard bij deze beoordeling het referentiekader. Hiervoor is gekozen omdat de Baseline Informatiebeveiliging Overheid (BIO) vooral bestaat uit een serie maatregelen waaraan wel of niet wordt voldaan, maar dat de BIO veel minder stil staat bij alle processen die er nodig zijn om continu de aandacht te blijven richten op de domeinen met de actuele risico's. De ISO standaard voorziet hier wel in, en geeft daarom een goed aangrijpingspunt om te rapporteren over volwassenheid.

Schematisch is de relatie tussen BIO en de ISO 27001 standaard als volgt te duiden:

	BIO	ISO27001
Management processen	Beperkt	Uitgebreid, daardoor is het mogelijk om "In Control" te zijn.
Beheersmaatregelen die getroffen zijn	Dit is de kern van de BIO	Deze zijn gerelateerd aan de uitkomsten van de management processen.

Alle ISO standaarden gaan uit van het beheersen van risico's. Een organisatie met het hoogste volwassenheidsniveau (5) heeft alle risico's – of het nu gaat om informatiebeveiliging of niet – in kaart en zorgt dat deze integraal worden gemanaged.

Het niveau daaronder (4) staat voor continue verbetering, wat verder gaat dan normen als de BIO vereisen.

Daaronder komt niveau 3 waar wordt voldaan aan de ISO 27001 standaard. Dit betekent dat aan alle normen formeel voldaan wordt op een herhaalbare manier. Als het meerwaarde heeft dan kan de organisatie zich onafhankelijk laten certificeren.

Lang niet altijd wordt voor zo'n onafhankelijke certificering gekozen, omdat extra inspanning nodig is om alle vereiste overhead (verplichte processen, verplichte documenten, bewijsmateriaal) gedetailleerd in orde te hebben en te houden zonder dat dit direct tot betere veiligheid leidt.

Een pragmatische ambitie is om op termijn qua beveiliging te groeien naar niveau 3, maar dan zonder de overhead als deze slechts van geringe waarde is.

2. Kernboodschap
Haarlem krijgt op dit moment de score 2. Er is duidelijk gewerkt aan het opzetten van een pragmatische basis, maar veel aspecten zijn nog informeel of hebben nog niet de grondigheid die door een ISO-norm wordt verwacht.

De belangrijkste adviezen van de auditor zijn:

- Versterk de structuur door eigenaarschap te benoemen, effectief in te richten en de resultaten daarvan te monitoren.
- Maak informele en impliciete normen expliciet.
- Werk het beveiligingsplan voor 2021 concreet uit en rapporteer regelmatig over de voortgang.

3. Consequenties
Naast de grote lijnen van de management processen is bij de audit ook gekeken naar de inhoudelijke domeinen. De geconstateerde punten waren bekend en zijn meegewogen bij de inschattingen van kans en impact in de risicoanalyse die bij de informatienota in december 2020 met de commissie is gedeeld.

Risico's zijn hoger waar maatregelen zwak zijn of ontbreken. De financieel substantiële risico's zijn reeds opgenomen bij de begroting.

4. Vervolg
De adviezen en opmerkingen van de auditor worden meegenomen in het plan van 2021. Over de voortgang daarvan wordt volgens afspraak gerapporteerd in de informatienota's van juni en van december.

Prioriteit wordt gegeven aan maatregelen die grote incidenten helpen voorkomen.

Volgens planning wordt de volwassenheid jaarlijks opnieuw gemeten in september, zodat het resultaat daarvan kan worden meegenomen in de informatienota van december.

5. Bijlage
Bijlage 1 GEHEIM Volwassenheidsbepaling ISO 27001 Gemeente Haarlem