Gemeente Haarlem

Collegebesluit

Onderwerp Referentiekader voor volwassenheid van Informatiebeveiliging	
Nummer	2020/854267
Portefeuillehouder	Botter, J.
Programma/beleidsveld	6.2 Gemeentelijk bestuur
Afdeling	CC
Auteur	Hut, F.J.
Telefoonnummer	023-5114955
Email	fhut@haarlem.nl
Kernboodschap	De internationale standaard ISO 27001 zal worden gebruikt als referentiekader om over de volwassenheid van Informatiebeveiliging te rapporteren.
Behandelvoorstel voor commissie	Het college stuurt dit besluit ter informatie naar de commissie, omdat dit richting geeft aan een toegezegde rapportage, zoals benoemd in 2019/311846
Relevante eerdere besluiten	N.v.t.
Besluit College d.d. 6 oktober 2020	Het college van burgemeester en wethouders Besluit: 1. De internationale ISO 27001 standaard te gebruiken als referentiekader voor de toegezegde rapportage over Volwassenheid van informatiebeveiliging. de secretaris, de burgemeester,

1. Inleiding
Bij behandeling van het RKC rapport over informatiebeveiliging heeft de raad opdracht gegeven om periodiek te rapporteren over de volwassenheid van informatiebeveiliging.

Er is niet afgesproken welk referentiekader hierbij zal worden gebruikt. Deze notitie stelt de ISO 27001 als referentiekader voor.

2. Besluitpunten college
De internationale ISO 27001 standaard te gebruiken als referentiekader voor de toegezegde rapportage over Volwassenheid van informatiebeveiliging.

3. Beoogd resultaat
Als wordt gerapporteerd en gesproken over “Volwassenheid van informatiebeveiliging” dan gebruikt iedereen hetzelfde referentiekader: de internationale standaard ISO 27001.

4. Argumenten
Bij volwassen informatiebeveiliging is de bestuurder voor dit aspect “In Control”. Het is de bedoeling om de informatiebeveiliging in orde te maken en daarna structureel in orde te houden. Zoiets vereist een benadering via een aanpak waarin onder aansturing van de directie een continue Plan-Do-Check-Act cyclus wordt geïmplementeerd.

Voor informatiebeveiliging is de ISO 27001 de internationale standaard. Management processen en de uitkomsten daarvan staan hierin centraal. Van deze ISO 27001 is ook de Baseline Informatiebeveiliging Overheid (BIO) afgeleid, waaraan de hele overheid moet voldoen.

De BIO focust zich echter vooral op de maatregelen en minder op de management processen. Juist die management processen en hun uitkomsten tonen de volwassenheid, en daardoor is de BIO minder geschikt om als referentiekader voor volwassenheid te gebruiken.

Het voorstel is daarom om rapportages over volwassenheid van informatiebeveiliging te relateren aan de ISO 27001 als referentiekader.

Bijkomend voordeel hiervan is dat dit een gelijkvormige benadering mogelijk maakt waar op verschillende gebieden aan kwaliteit wordt gewerkt:

- Het kwaliteitssysteem van o.a. het klantcontactcentrum conform de ISO 9001 standaard.
- Ontwikkeling van beheer in de afdeling informatievoorziening dat zich beweegt richting de ISO 20000 standaard.
- Structureren van Privacy processen richting de ISO 27701 standaard, die is ontwikkeld als uitbreiding op de ISO 27001 standaard voor informatiebeveiliging.
- In een later stadium het opzetten van Business Continuïteit volgens de ISO 22301 standaard.

5. Risico's en kanttekeningen
Met ISO standaarden wordt impliciet een hoge ambitie gekozen, waarbij sterke management betrokkenheid, actief risico management en continue verbetering uitgangspunten zijn.

6. Uitvoering
In de voorgestelde begroting is professionaliseren van informatiebeveiliging reeds opgenomen. Dit voorstel is consistent met de keus van ISO 27001 als referentiekader.

De keus van ISO 27001 als referentiekader geeft vooral duidelijkheid in de communicatie, het veroorzaakt verder geen additionele kosten.

In december 2020 is de audit naar volwassenheid van informatiebeveiliging door een onafhankelijke auditor gepland.

7. Bijlagen
Er zijn geen bijlagen.