Toelichting CISO diverse rapportages, resultaten zelfevaluatie en audit ENSIA 2024
Documentnummer : bijlage 1, kenmerk D-139786.

Toelichting CISO Verantwoordingsrapportages informatiebeveiliging; resultaten zelfevaluatie en ENSIA (audit) 2024

Het college legt jaarlijks verantwoording af over de informatiebeveiliging (IB). Dit gebeurt door de zelfevaluatie en de ENSIA-audit. Het betreft twee verantwoordingsprocessen, te weten:
1. Horizontaal proces: verantwoording aan de Raad.
2. Verticaal proces: verantwoording aan de rijksoverheid/toezichthouders.

De daarbij gehanteerde rapportages en collegeverklaring met bijlagen zijn in overeenstemming met de formats zoals landelijk zijn voorgeschreven/aangeleverd.

Ad 1 Horizontaal proces: verantwoording aan de Raad.

Rapportage Zelfevaluatie en ENSIA 2023 2024 (bijlage 2, D-139447 geheim)
De informatiebeveiliging over 2024 is met behulp van de Eenduidige Normatiek Single Information Audit (ENSIA) getoetst. De ENSIA is een zelfevaluatie op basis van de Baseline Informatiebeveiliging Overheid (BIO).
De Baseline informatiebeveiliging Overheid (BIO) is het basisnormenkader voor informatiebeveiliging binnen **alle** overheidslagen (Rijk, gemeenten, provincies en waterschappen). De BIO heeft risicomanagement als uitgangspunt. ENSIA behandelt ongeveer 70% van de BIO.

Belangrijkste ontwikkeling op het terrein van informatiebeveiliging in 2024 zijn:
- Voor de derde keer is van het Information Security Management System (ISMS) gebruik gemaakt. In dit systeem zijn in 2023 de ENSIA-normen en **alle** normen van de BIO opgenomen. In 2024 is dit beperkt tot de ‘kritische applicaties’. Dit zijn systemen/applicaties die kritiek zijn voor de gemeente Beverwijk en binnen 24 uur weer actief moeten zijn na een calamiteit.
  De normen worden als taak uitgezet naar deskundige medewerkers. Zij kunnen verklaren of ‘we’ aan de normen voldoen. Deze verklaring wordt vervolgens door de teammanager beoordeeld. Hiermee wordt duidelijk wat gedaan is en wat nog gedaan moet worden. In 2024 zijn ook de strategisch managers bij dit proces betrokken. Dit wordt elk jaar herhaald. Hierdoor wordt de verplichte plan, do, act en check (PDCA) cyclus nageleefd.
- Op het terrein van Gemeente brede bewustwording.
  - De Chief Information Security Officer (CISO) en de Privacy Officer (PO) zijn gestart met de workshop: digitale informatiebeveiliging en privacy - **nieuwe medewerkers**. Deze wordt maandelijks gegeven zowel aan nieuwe vaste medewerkers en inhuur.
  - Ontwikkelingen worden ook op strategisch niveau besproken (PFO twee maandelijks en SMT 2 keer per jaar en als dit nodig is). Er is een start gemaakt dit met behulp van Kritieke prestatie-indicatoren (KPI’s) uit te voeren.
  - Medewerkers worden op BINK geïnformeerd over IB gerelateerde onderwerpen.
  - E-learning methode voor elke medewerker zet zich voort; genaamd Sir Askalot.
  - Nep phishing actie is uitgevoerd.
  - Maria Genova heeft in een bijeenkomst een presentatie gegeven.
  - Deelname aan cyberoefening (derde keer).

Verder:
- Voortzetting van de baselinetoets. In deze toets wordt het beveiligingsniveau beoordeeld. Deze toets wordt gedaan bij de aanschaf van een nieuw systeem, een nieuw proces of andere ontwikkeling.
- Jaarlijkse controle van de Digitale Weerbaarheid.

- Verwerking verbeterpunten uit het ISMS. Deze zijn gerapporteerd naar de teammanagers die een rol hebben in de verbeterpunten.
- Implementatie van het Logische Toegang beleid, uitvoering van de Business Impact Analyse (BIA: is ter uitvoering van het bedrijfscontinuïteitsplan) en uit vraag naar ketenopbouw is per team uitgezet.

Kort overzicht en uitleg zelfevaluatie.
In 2023 is op 200 normen de BIO-controle uitgevoerd en 2024 zijn er 114 BIO-normen gecontroleerd. Het vergelijken van deze resultaten zou een vertekend beeld geven. We lis er naar aanleiding vanuit de controle van 2023 een aantal maatregelen doorgevoerd, te weten:

- De bewustwordingsactiviteiten zijn doorgevoerd in 2024;
- Het doorvoeren van de BIO normen in het ISMS en:
- De implementatie van diverse documenten die in 2024 zijn gemaakt.

Zoals uit de rapportage en scores blijkt voldoet Beverwijk **niet** aan alle 114 BIO-normen. De gemeente Beverwijk zal het komend jaar stappen moeten gaan maken met het in werking treden van de Network and Information Security directive (NIS2) en nationale wetgeving Cyberbeveiligingswet (Cbw).

We controleerden in 2024 de uit te voeren normen op **opzet, bestaan** en deels op **werking**. Dit laatste houdt in dat we ook moeten bewijzen hoe we de normen uit de BIO uitvoeren m.a.w. in hoeverre we kunnen aantonen dat de normen in de dagelijkse praktijk zijn geïmplementeerd. Het aantonen van in eerste instantie opzet en bestaan moet niet onderschat worden. Het brengt veel werk met zich mee en hierin loopt de organisatie flink achter. Voor de daadwerkelijke uitvoering zijn we afhankelijk van alle managers die verantwoordelijk zijn voor de uitvoering van deze normen. Uit de praktijk blijkt dat op dit moment nog onvoldoende uitvoering wordt gegeven aan de normen. Het opstellen van governance documenten gaat te traag. Hierover heeft de CISO het SMT geïnformeerd en zijn zorgen over uitgesproken. Om de benodigde stappen sneller te laten verlopen is een voorstel gedaan, maar er is besloten met de huidige werkwijze door te gaan. Hiermee lopen we het risico om niet op tijd klaar te zijn bij het ingaan van de NIS2/Cbw.

Doel informatiebeveiliging voor 2025
Het doel ten aanzien van informatiebeveiliging voor 2025 is te voldoen aan de NIS2, de Cbw en de BIO2.0. De NIS2 is vastgesteld door de Europese Unie en bedoeld om de cyberbeveiliging en de weerbaarheid van essentiële diensten in EU-lidstaten te verbeteren. Deze richtlijn stelt strengere beveiligingsnormen en meldingsvereisten voor incidenten. De richtlijn wordt vertaald naar nationale wetgeving zijnde de Cbw. Deze normen worden geïmplementeerd in BIO2.0. De gemeenten zijn onder de NIS2-richtlijn als essentiële organisatie aangewezen. Hiermee vervalt de vrijblijvendheid volledig om aan de BIO te voldoen en wordt dit een verplichting. Belangrijke onderdelen van de NIS2 zijn:

Zorgplicht – dit houdt voor de gemeente Beverwijk in dat we moeten voldoen aan de BIO, risicogericht gaan werken en we aan de governance voldoen.
Registratieplicht – we zijn verplicht ons te registreren. Deze registratie moet zorgen voor een Europees breed beeld van het aantal organisaties die onder de NIS2 vallen.
Meldplicht – we moeten incidenten binnen 24 uur melden bij de toezichthouder.
Toezichthouder – als toezichthouder is de Rijksinspectie Digitale Infrastructuur (RDI) aangeweze. De toezichthouder kijkt naar de naleving van de verplichtingen uit de richtlijn, zoals de zorg- en meldplicht. Uiteraard blijven we met ENSIA verantwoording afleggen aan de gemeenteraad.
Verantwoording – alle verantwoordelijken (Burgemeester, Gemeentebestuur en de Gemeentesecretaris) moeten kunnen aantonen dat zij hun verantwoordelijkheid goed nakomen. Indien de verantwoording niet op een juiste manier in acht wordt genomen zijn hieraan consequenties verbonden.

De NIS2 heeft niet alleen betrekking op de kantoorautomatisering, het betreft ook de **operationele technologie (OT)** zoals, besturing en bediening van bruggen, sluizen, gemalen, afvalwaterinstallaties en rioolpompgemalen, beheer van parkeergarages en zwembaden, bediening van toegangsbeveiliging (slagbomen, elektronische hekwerken, camera systemen), gebouwbeheersystemen (verwarming, koeling, ventilatie, noodstroomvoorzieningen), (IoT-) sensoren in publieke ruimten (camerasystemen, verkeertellers en detectielussen), enz..
Dit is in een memo in het SMT gebracht en is op 20 februari 2024 bekrachtigd. Dit houdt in dat er maatregelen zijn genomen die dit jaar uitgevoerd gaan worden.

Risicomanagement
Als gevolg van de NIS2, Cbw en de BIO2.0 zal de uitvoering van informatiebeveiliging verschuiven naar het risicomanagement. Risicomanagement vraagt een organisatie brede uitvoering. Om dit te bereiken is het nodig het risicobeleid, -protocollen en -analyses op te zetten, zodat er grip ontstaat op bedreigingen. Op basis hiervan zullen de risico's bij de eigenaren worden belegd. Als we dit risicomanagement in de huidige situatie uitvoeren is er een risico dat we niet op tijd klaar zijn bij ingang van de wet en informatiebeveiligingsrisico's gaan lopen. Om te voldoen aan de benodigde eisen is het ons advies aan te sluiten bij de door de VNG geadviseerde aanpak genoemd in hun brief van 19 september 2024 kenmerk U202400439. Dit advies is niet gevolgd.

Rapportage Verhogen digitale veiligheid (Bijlage 3, D-139448 geheim)
Wetende dat de BIO maatregelen door veel gemeenten, waaronder ook de gemeente Beverwijk, niet gehaald worden is door de Informatiebeveiligingsdienst (IBD) een selectie gemaakt van de meest essentiële beveiligingsmaatregelen uit de BIO. Deze zijn opgenomen in de rapportage Verhogen digitale veiligheid (D-139448). Op basis van deze rapportage kan gesteld worden dat nog niet volledig voldaan wordt aan de meest essentiële beveiligingsmaatregelen. Voor de genoemde maatregelen is in 2024 een aantal stappen gemaakt en belangrijk is om dit in 2025 door te zetten. Elk jaar wordt een meting voor de digitale veiligheid uitgevoerd en gerapporteerd aan Burgemeester en Gemeentesecretaris.

Proces meldingen HIGH/HIGH en register beveiligingsmeldingen en -incidenten 2024
We krijgen regelmatig meldingen binnen van de Informatiebeveiligingsdienst (IBD). Hiervoor is in 2022 een proces opgenomen in de Servicedesk (SSP) en in 2024 als formeel proces opgetekend. Het proces loopt van de melding tot beoordeling van de melding tot afronding. Alle belanghebbenden zijn hierbij betrokken. Dit proces wordt ook gebruikt voor andere meldingen dan die van de IBD. Hiermee wordt ook de digitale weerbaarheid gewaarborgd.

Ad 2: Verticaal proces: verantwoording aan de rijksoverheid

De verantwoording aan de rijksoverheid betreft een aantal rapportages. De verantwoording aan de rijksoverheid betreft de volgende rapportages:

A. Collegeverklaring over DigiD en Suwinet (Bijlage 4, D-139455 geheim)
B. Rapportage BAG, BGT en BRO (Bijlage 5, D-139475)

A. Collegeverklaring over DigiD en Suwinet (Bijlage 4, D-139455 geheim)
Met de voorliggende ENSIA-collegeverklaring geeft het college aan in hoeverre de beheersingsmaatregelen voldoen aan de normen die gelden voor **DigiD en Suwinet** en op welke onderdelen de gemeente niet voldoet aan deze normen. De collegeverklaring is opgesteld aan de hand van de uitkomsten van de ingevulde zelfevaluaties die door de lijnverantwoordelijken zijn beoordeeld, onder coördinatie van de ENSIA-coördinator. Aan de verklaring zijn vier bijlagen met meer informatie toegevoegd. En te vinden onder documentnummer, Bijlage 4.1 **D-139462**, Bijlage 4.2 **D-139467,** Bijlage 4.3 **D-139471 en** Bijlage 4.4 **D-139472.**

Een gecertificeerde IT-auditor heeft de collegeverklaring met bijlagen gecontroleerd. Na vaststelling van de collegeverklaring zal de auditor zijn Assurance rapport afgeven. De IT-auditor verklaart hierin dat de collegeverklaring een getrouw beeld geeft.

Verbeterplan Suwinet.
In 2022 en 2023 hebben we niet voldaan aan de auditeisen. Het gevolg hiervan is dat de gemeente is aangesproken door de Directie Stelsel & Volksverzekeringen van het Ministerie van Sociale Zaken en Integratie en is de gemeente Beverwijk op trede 2 van het interventieprotocol terecht gekomen. Er is in 2024 een brief ontvangen van het ministerie en de aankondiging van een ambtelijk overleg met het ministerie, dat in januari 2025 heeft plaatsgevonden. We hebben goede stappen gezet, echter hebben wij over 2024 nog niet voldaan aan twee normen (9.2.5 en 12.4.1). Daarom is een verbeterplan gemaakt, waarmee we verwachten in 2025 te voldoen (bijlage 04.4 A).

De vacature ISO/ENSIA coördinator is sinds 1 juni 2024 ingevuld. Met deze functie leggen we de werkzaamheden op de juiste plek. Met dit proces hebben we inmiddels meer grip gekregen op de Suwinet audit. Ook is het Suwinet proces formeel opgesteld.

Verbeterplan DigiD
Er is geen verbeterplan.

B. Rapportage BAG, BGT en BRO (Bijlage 5, D-139475)
Binnen het ENSIA-stelsel zijn voor het Geo-domein BAG, BGT en BRO-domein specifieke zelfevaluaties opgenomen over het gebruik van deze drie basisregistraties. De zelfevaluaties binnen het Geo-domein zijn gekoppeld aan en percentage waarvan 100% het maximum is. In de bijlage (D-139475) is per stelsel een rapportage opgenomen met de bevindingen.

Beverwijk, 30 april 2025

Ruud van der Heide
ISO / ENSIA Coördinator