Zaaknr. : 722926
Kenmerk : 722927

Onderwerp: Managementsamenvatting externe audit informatiebeveiliging 2023

Mededeling voor het algemeen bestuur.

Portefeuillehouder:	K. van den Berg
Programmadirecteur:	Arthur Meuleman

Eind 2023 is door Verdonck Klooster & Associates (VKA) een externe audit uitgevoerd naar de huidige status van informatieveiligheid en het managementsysteem (PDCA). Doel is de noodzakelijke verbeteracties te bepalen om het beveiligingsniveau op het gewenste niveau te brengen. De externe audit maakt onderdeel uit van de sectorbrede audit die om de 2 jaar wordt uitgevoerd.

De gezamenlijke waterschappen hebben zich tot doel gesteld te streven naar een volwassenheidsniveau van 4. Bij de audits zijn de volwassenheidsniveaus gehanteerd afkomstig van het Centrum Informatiebeveiliging en Privacybescherming (CIP) Baseline Informatiebeveiliging Overheden (BIO).

Algemene voorbeelden volwassenheidsniveaus CIP/BIO		
Niveau 2	**Niveau 3**	**niveau 4**
Informatiebeveiliging is een project	Informatiebeveiliging is een proces	Informatiebeveiliging is onderdeel van de bedrijfsprocessen
Zaken worden opgestart maar meestal verder niet gevolgd	Zaken worden gepland, opgestart en soms gevolgd	PDCA is gestructureerd aanwezig, bijvoorbeeld in jaarplannen
De CISO probeert management aandacht te krijgen	Informatiebeveiliging is in relevante procedures voldoende gedefinieerd	Informatiebeveiliging is in relevante procedures voldoende gedefinieerd
Elke medewerker verdiept zich naar eigen inzicht en behoefte	Jaarlijkse opleidingen en awareness	Actieve intervisie op best practices
Meest verplichte overheidsmaatregelen zijn toegepast	Verplichte overheidsmaatregelen worden toegepast	Aantoonbare sturing op de BIO en informatiebeveiligingsbeleid
Classificatie van informatie is deels op orde	De 10 basisvereisten worden in belangrijke gevallen gebruikt	Leidinggevenden geven voorbeeldgedrag
De 10 basisvereisten worden af en toe gebruikt		Verplichte overheidsmaatregelen en risico-assessment indien dat nodig is wegens het belang van informatie

Management Samenvatting VKA
Het gehele Information Security Management Systeem bekijkende zien we op maatregelniveau een belangrijke mate van volwassenheid van meer dan een 3,4. Hierbij kent Kantoorautomatisering (KA) het hoogste volwassenheidsniveau (3,6) gevolgd door de het managementsysteem (PDCA) en Procesautomatisering (PA). De aanpak is goed op koers. De mate van volwassenheid wordt voor een belangrijk deel veroorzaakt door de fase waarin het programma zich bevindt. Brabantse Delta is goed op weg, maar er moet nog een en ander worden afgemaakt.

Voor de Kantoorautomatisering geldt: goed op weg. Dit blijkt o.a. uit het gebruik van de X-matrix en de rapportages voor de besturing van Kantoorautomatisering. Ook is er op het vlak van veilig personeel voortgang geboekt. De juridische ontwikkelingen worden gevolgd met de juiste aandacht.

Procesautomatisering ijlt wat na. Maar met de adoptie van de CyberSecurity ImplementatieRichtlijn(CSIR) worden de goede stappen gezet en komend jaar zal het de voordelen gaan krijgen van de ingezette aanpak.

PDCA is ook goed op weg en zal ook komend jaar verdere voortgang kunnen boeken door de PDCA-cyclus langer dan 1 jaar uit te voeren Er worden wel activiteiten uit 'The Three Lines of Defense' uitgevoerd maar daar ligt nog de ruimte voor verbetering.

In bovenstaande punten liggen dan ook de belangrijkste mogelijkheden om naar volwassenheid niveau 3,5 en hoger te komen. Daarnaast zijn er op de verschillende normen nog punten van verbetering. Deze worden verder toegelicht.

Toelichting PA
De waterschappen Aa en Maas, Brabantse Delta (BD) en De Dommel werken samen op het gebied van informatieveiligheid en hebben een gedeeld beleid en governance structuur. Op algemene onderwerpen is het antwoord van BD: PA volgt KA, maar wel met de kanttekening dat BD de CSIR als basis heeft vastgesteld en verwerkt in beleid en procedures. Het interview gaf de nodige extra informatie bij de aangeleverde stukken voor een goede beoordeling van de huidige volwassenheid en verbetermogelijkheden.

Op basis van de aangeleverde informatie zijn de drie belangrijkste verbeterpunten:

1. Fysieke beveiliging: De eerste stap, het definiëren van fysieke zones met bijbehorende classificatie is uitgevoerd. Het is nu een zaak van doorpakken naar realisatie: vertalen naar een sleutelplan, keuze voor het soort sleutel, waaronder de programmeerbare sleutel met passend sleutelbeheer.

1. Netwerk en informatietransport: Netwerkbeleid en opzet zijn vastgesteld. De volledige realisatie wordt afgerond in 2024. Zet de implementatie voort en houd hierbij rekening met het toepassen van hardening (is het aanpassen van veiligheidsconfiguraties om de risico's te verkleinen) beleid en voldoende scheiding tussen KA en PA.

2. Contracteisen en audits: De PA contracteisen voor security zijn nog niet doorgevoerd in de bestaande interne en externe afspraken, waaronder de wijze van beoordeling en de toepassing ervan.

Toelichting KA
De meerderheid van de verbeterpunten is bereikt. De X-matrix is geïntroduceerd als besturingstool voor het jaarplan en het beleid is vernieuwd. De voortgang van het beleid wordt consequent aan het managementteam gerapporteerd. De rol van de Chief Information Security Officer en de rapportagelijnen zijn vastgesteld, waarbij belangrijke juridische ontwikkelingen zoals BIO 2.0 worden gevolgd. Nieuw personeel wordt tijdens onboarding geïnformeerd over digitale werkwijzen en de noodzaak van een Verklaring Omtrent Gedrag bij aanstelling, alsook de geheimhoudingsplicht bij het verlaten van het waterschap.

Op basis van de aangeleverde informatie zijn de drie belangrijkste verbeterpunten:

1. Zet de implementatie van het Identity and Access Management-project voort en voer het systeem volledig in om een robuuste identiteits- en toegangsbeheerstructuur te garanderen.

2. Rond het zoneringsproject af om een verhoogde beveiliging en risicobeheersing gebaseerd op locatie-specifieke criteria te waarborgen.

3. Ontwikkel en implementeer een volledig auditplan om de controlewerkzaamheden te versterken en compliance te waarborgen met daarin ook aandacht voor privacy.

Toelichting PDCA
In 2023 is een aanzienlijk deel van de verbeterpunten behaald. Het jaarplan wordt bestuurd met de X-matrix en het beleid is vernieuwd. Belangrijk hierbij is de rapportage aan het MT over de realisatie van het beleid. Verder is de PDCA-cyclus voor security in het tweede kwartaal gestart, met rapportages over KPI's vanaf datzelfde kwartaal. De verantwoordelijkheden binnen het beleid zijn vastgesteld en er is een fundament gelegd voor risicobereidheid door een document met visie op risicomanagement. Er is een meerjarenplan voor security opgesteld en er zijn stappen gezet in de samenwerking met Arda om de aanpak voor verschillende doelgroepen te verfijnen.

Drie belangrijkste verbeterpunten:

1. Continueer de strategische aanpak om de organisatorische volwassenheid te verhogen. Zorg hierdoor voor een implementatietermijn die langer is dan één jaar om niveau 4 van volwassenheid te bereiken.

2. Ontwikkel een heldere risicobereidheidsverklaring binnen de organisatie. Deze verklaring moet aansluiten bij de strategische doelstellingen en zorgen voor een gedragen basis voor alle risicomanagementactiviteiten.

3. Zorg voor een gelijkwaardige integratie van privacy in de PDCA-cyclus, net zoals security. Dit verzekert een uniforme benadering van beide domeinen binnen de organisatie en bevordert een integrale aanpak van risicobeheersing.

Datum: 8 januari 2024
Naam schrijver: A. van der Meer

.