Gemeente Deurne

Rapportage informatiebeveiliging 2022

op basis van de zelfevaluatie ENSIA

Leeswijzer en inhoud

Deze rapportage is opgesteld op basis van de zelfevaluatie ENSIA 2022

TERUGBLIK 2022
- Ontwikkelingen
- Resultaat bij belangrijkste doelen
- Beveiligingsincidenten en datalekken

STATUS INFORMATIEBEVEILIGING (BIO)
- Onze norm voor informatiebeveiliging samengevat (de BIO)
- Status Deurne ten opzichte van de BIO

VERANTWOORDING AAN HET RIJK
- Getoetste collegeverklaring ENSIA – DigiD
- Getoetste collegeverklaring ENSIA – Suwinet
- Status Basisregistratie Personen en Reisdocumenten
- Status GEO basisregistraties (BAG, BGT, BRO)
- Status Wet Onroerende Zaken (WOZ)

De BIO maatregelen zijn in deze rapportage beknopt opgenomen.

GEBRUIKTE SCHALEN:

groen: goed (90% - 100% van de punten)
geel: redelijk (75% - 90% van de punten)
rood: onvoldoende (0% - 75% van de punten)

groen: voldaan aan een norm
rood: niet voldaan aan een norm

TERUGBLIK 2022

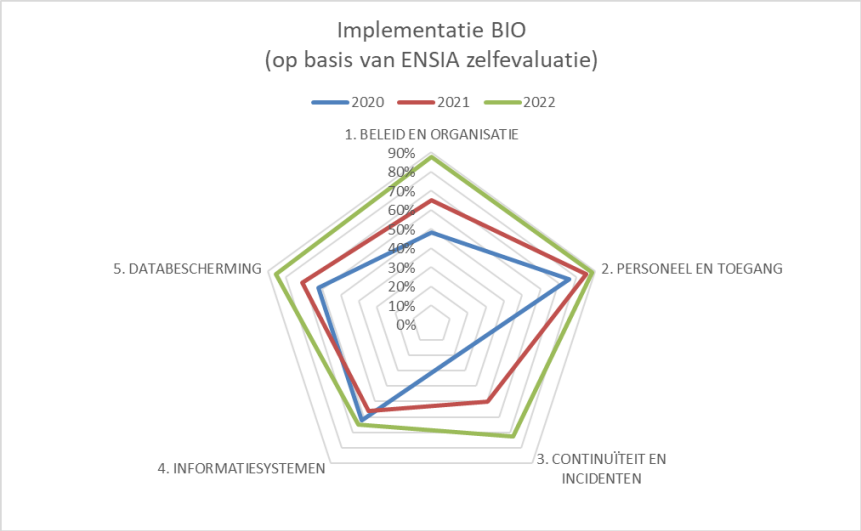
Belangrijke ontwikkelingen in 2022

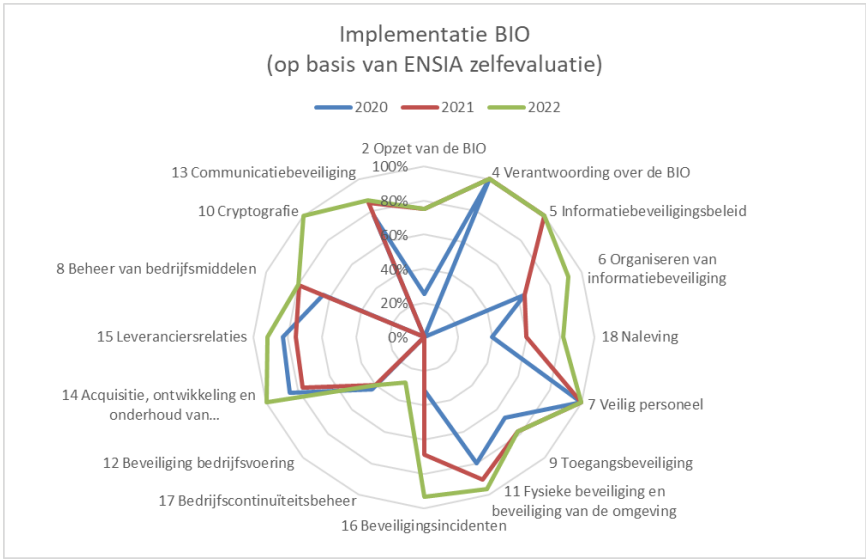
Deurne

- Systematiek om de informatiebeveiliging diepgaand te implementeren en “in control” te kunnen zijn van informatiebeveiliging verder ingevoerd.
- Nieuw protocol voor cybercrisis, wordt vanaf 2023 geoefend
- Bedrijfscontinuïteitplanning gestart.
- Aannemen personeel voor *IBP basis-op-orde* gestart Technisch netwerk/security specialist aangenomen
- Implementatie BIO naar 80% (was 68%)

Nederland en de wereld

- Misinformatie en phishing blijven belangrijk
- Meer *ransomware*, destructievere gevolgen
- Vaker diefstal van gegevens voor afpersing
- Meer en ernstiger kwetsbaarheden in software
- Gevaren in uitbestedings- en samenwerkingsketens
- Cyberaanvallen voor oorlog, terrorisme en activisme
- *Deepfake* technologie als wapen
- Europese regelgeving NIS2 verplicht informatiebeveiliging





Informatiebeveiligingsincidenten en Datalekken

	2018	2019	2020	2021	2022
Beveiligingsincidenten	onbekend	onbekend	23	27	24
waarbij persoonsgegevens betrokken (datalek)	8	10	14	13	12
gemeld aan autoriteit persoonsgegevens	3	5	4	4	4
gemeld aan of door betrokkenen	0	0	4	6	0

STATUS INFORMATIEBEVEILIGING

op basis van de Baseline
Informatiebeveiliging Overheid (BIO)

DE BASELINE INFORMATIEBEVEILIGING OVERHEID (BIO)

Alle gemeentes volgen de BIO. Dit zijn verplichte maatregelen voor informatiebeveiliging.
Ze kunnen in 5 groepen worden samengevat.

BIO Hoofdstuk		Normen	Consolidatie	Totaal	
2	Opzet van de BIO	4	1. BELEID EN ORGANISATIE	32	215
4	Verantwoording over de BIO	3			
5	Informatiebeveiligingsbeleid	2			
6	Organiseren van informatiebeveiliging	12			
18	Naleving	11			
7	Veilig personeel	8	2. PERSONEEL EN TOEGANG	60	
9	Toegangsbeveiliging	27			
11	Fysieke beveiliging en beveiliging van de omgeving	25			
16	Beveiligingsincidenten (Beheer van informatie..)	15	3. CONTINUÏTEIT EN INCIDENTEN	22	
17	Bedrijfscontinuïteitsbeheer (Informatiebeveiligingsaspecten van ..)	7			
12	Beveiliging bedrijfsvoering	33	4. INFORMATIESYSTEMEN	60	
14	Acquisitie, ontwikkeling en onderhoud van informatiesystemen	15			
15	Leveranciersrelaties	12			
8	Beheer van bedrijfsmiddelen	15	5. DATABESCHERMING	41	
10	Cryptografie	4			
13	Communicatiebeveiliging	22			

SAMENGEVAT: WAT SCHRIJFT DE BIO VOOR

Bestuurlijke principes en beleid, organisatie van de beveiliging en naleving

Het bestuur van Deurne:

- Volgt het beleid van de informatiebeveiligingsdienst gemeenten (IBD)
- Zorgt ervoor dat de juiste activiteiten voor informatiebeveiliging door de organisatie worden uitgevoerd
- Controleert de juiste werking van de informatiebeveiliging

1. BELEID EN ORGANISATIE
H2 / H4 / H5 / H6 / H18

Actueel beleid en organisatie van informatiebeveiliging en controle op naleving

- Bestuur, directie en management laten zien dat informatiebeveiliging belangrijk is
- Informatiebeveiliging is georganiseerd
- Wij houden ons aan onze afspraken en leven de wet- en regelgeving na
- We zijn transparant en leggen verantwoording af.

Het bestuur en medewerkers zijn actief betrokken bij informatiebeveiliging. Er is een organisatiebreed beleid dat richting en sturing geeft. De organisatie is effectief ingericht, waarbij rollen, taken en bevoegdheden zijn ondergebracht. Verantwoording is structureel ingericht, zodat naleving is geborgd.

2. PERSONEEL EN TOEGANG
H7 / H9 / H11

Juiste toegang voor medewerkers tot gebouwen, systemen en gegevens

- Voor, tijdens en na het dienstverband is alles goed geregeld
- Medewerkers gaan bewust om met informatie
- Medewerkers hebben juiste toegangsrechten (fysiek en digitaal)

Alleen de juiste personen hebben toegang tot de gebouwen, systemen en gegevens van de gemeente. Er zijn passende maatregelen, zowel in organisatie als in techniek. Dit gaat om waarborgen rondom in- en externe medewerkers, toegang tot gebouwen en omgeving en toegang tot de (digitale) informatievoorziening.

SAMENGEVAT: WAT SCHRIJFT DE BIO VOOR

3. CONTINUÏTEIT EN INCIDENTEN
H16 / H17

Zorgen voor de continuïteit van onze dienstverlening en opvolging van incidenten

- Wij komen afspraken met inwoners na
- Bij calamiteiten en incidenten weten we wat we moeten doen
- Continuïteitsplannen zijn actueel en worden getest
- Incidenten worden altijd gemeld

De diensten van de gemeente worden geleverd volgens de afspraken die de gemeente daarover maakt met inwoners en bedrijven. Ook bij incidenten worden de diensten geleverd volgens deze afspraken.

4. INFORMATIESYSTEMEN
H12 / H14 / H15

Veilige omgang met informatiesystemen en afspraken hierover met leveranciers

- Wijzigingen in systemen worden op een gecontroleerde manier doorgevoerd
- We zijn beschermd tegen malware
- Back-ups worden volgens beleid uitgevoerd en getest
- De afspraken met leveranciers zijn vastgelegd

Informatiesystemen zijn een keten van mensen, processen en middelen. Hierin zijn procedures en maatregelen beschikbaar ter bescherming van de omgeving. Het gaat hierbij om zowel de interne als de externe informatiesystemen (uitbesteding, leveranciers en Cloud- toepassingen).

5. DATABESCHERMING
H8 / H10 / H13

Veilige omgang met data in applicaties

- Data wordt op de juiste manier beschermd
- De gegevens van de burgers worden veilig opgeslagen en gecommuniceerd. Binnen en buiten de gemeente

STATUS DEURNE TEN OPZICHTE VAN DE BIO

Goede vooruitgang in werken volgens de BIO.
Op belangrijke punten wordt nog niet aan de norm voldaan. Hierdoor lopen we risico's.
De focus moet uitgaan naar:

- verder invoeren en borgen toegangsbeveiliging
- testen van wijzigingen in informatiesystemen
- monitoring en detectie van incidenten (SIEM/SOC)
- back-up en herstel in ketens van applicaties
- voorbereiden op grote incidenten (cybercrisis, continuïteitsplan)

redelijk
80% 2021: 68%

0% - 75% | 75% - 90% | 90% - 100%

1. BELEID EN ORGANISATIE Actueel beleid en organisatie van informatiebeveiliging en controle op naleving	88% 2021: 65%
2. PERSONEEL EN TOEGANG Juiste toegang voor medewerkers tot gebouwen, systemen en gegevens	88% 2021: 85%
3. CONTINUÏTEIT EN INCIDENTEN Zorgen voor de continuïteit van onze dienstverlening en opvolging van incidenten	73% 2021: 50%
4. INFORMATIESYSTEMEN Veilige omgang met informatiesystemen en afspraken hierover met onze leveranciers	65% 2021: 56%
5. DATABESCHERMING Veilige omgang met data in onze software	85% 2021: 71%

1. BELEID EN ORGANISATIE

redelijk

Actueel beleid en organisatie van informatiebeveiliging en controle op naleving

- Bestuur, directie en management laten zien dat informatiebeveiliging belangrijk is
- Informatiebeveiliging is georganiseerd
- Wij houden ons aan onze afspraken en leven de wet- en regelgeving na

88%
2021: 65%

Onderdelen:

0% - 75% | 75% - 90% | 90% - 100%

H2 / Opzet van de BIO	75% 2021: 750%
H4 / Verantwoording over de BIO	100% 2021: 100%
H5 / Informatiebeveiligingsbeleid	100% 2021: 100%
H6 / Organiseren van informatiebeveiliging	92% 2021: 64%
H18 / Naleving	82% 2021: 60%

Geadviseerde verbeteracties

1. *Laat eisen aan beveiligingsniveau (BBN) expliciet vaststellen door verantwoordelijke voor een proces (eigenaarschap).*
2. *Maak het sturen op informatiebeveiliging en privacy expliciet onderdeel van "integraal management".* prio
3. *Voer op basis van een vastgesteld intern auditplan regelmatig controles uit op informatiebeveiliging en het naleven van privacyregels (dit omvat ook een verbetering voor de BRP en Reisdocumenten).* prio
4. *Verbeter de beveiliging van informatie op smartphones en laptops (mobiele apparaten).*

Risico's

- *Management neemt geen verantwoordelijkheid maar laat informatiebeveiliging en privacy over aan de werkvloer.*
- *Te rooskleurig beeld door uitsluitend zelfevaluatie van betrokkenen. Geen bijsturing op risico's.*
- *In- en externe wet- en regelgeving privacy & informatiebeveiliging worden niet nagekomen.*
- *Onrechtmatige raadpleging en misbruik van toegang tot persoonsgegevens door personeel.*
- *Gegevens op zakelijke en privé smartphones zijn niet goed genoeg beschermd tegen kopiëren buiten de veilige omgeving.*

2. PERSONEEL EN TOEGANG

redelijk

Juiste toegang voor medewerkers tot gebouwen, systemen en gegevens

- Voor, tijdens en na het dienstverband is alles goed geregeld
- Medewerkers gaan bewust om met informatie
- Medewerkers hebben juiste toegangsrechten (fysiek en digitaal)

88%
2021: 85%

Onderdelen:

0% - 75% | 75% - 90% | 90% - 100%

H7 / Veilig personeel	100% 2021: 100%
H9 / Toegangsbeveiliging	78% 2102: 78%
H11 / Fysieke beveiliging en beveiliging van de omgeving	96% 2021: 90%

Geadviseerde verbeteracties

prio
1. *Borg toegang tot informatiesystemen met (half)jaarlijkse beoordeling door systeemeigenaar.*
2. *Maak een wachtwoordkluis breder beschikbaar en ondersteun bij het kiezen van sterke wachtwoorden.*

Risico's

- *Vertrouwelijke informatie en persoonsgegevens zijn in te zien door medewerkers die dit niet nodig hebben.*
- *Wachtwoorden zijn zwak en/of worden hergebruikt in meerdere systemen.*

3. CONTINUÏTEIT EN INCIDENTEN

onvoldoende

Zorgen voor de continuïteit van onze dienstverlening en opvolging van incidenten

- Wij komen afspraken met inwoners na
- Bij calamiteiten en incidenten weten we wat we moeten doen
- Continuïteitsplannen zijn actueel en worden getest
- Incidenten worden altijd gemeld

73%
2021: 50%

Onderdelen:

0% - 75% 75% - 90% 90% - 100%

H16 / Beheer van beveiligingsincidenten	93% 2021: 69%
H17 / Bedrijfscontinuïteitsbeheer & informatiebeveiliging	29% 2021: 0%

Geadviseerde verbeteracties

prio • *Sluit een contract af voor directe bijstand bij cyberincidenten.*

prio • *Bepaal de kritische bedrijfsprocessen en stel hiervoor continuïteitsplannen op om de dienstverlening te verzekeren tijdens een calamiteit.*

Risico's

- *De dienstverlening aan inwoners komt na een ernstig incident of gerichte cyber-aanval langdurig stil te liggen.*

4. INFORMATIESYSTEMEN

onvoldoende

Veilige omgang met informatiesystemen en afspraken hierover met leveranciers

- Wijzigingen in systemen worden op een gecontroleerde manier doorgevoerd
- We zijn beschermd tegen malware
- Back-ups worden volgens beleid uitgevoerd en getest
- De afspraken met leveranciers zijn vastgelegd

65%
2021: 56%

Onderdelen: 0% - 75% | 75% - 90% | 90% - 100%

H12 / Beveiliging van de bedrijfsvoering (*) Percentage lager dan in 2021 omdat aan de verantwoording (zelf bepaalde) maatregelen zijn toegevoegd. Hier wordt nog niet altijd aan voldaan.	(*)39% 2021: 40%
H14 / Acquisitie, ontwikkeling en onderhoud van informatie systemen	100% 2021: 77%
H15 / Leveranciersrelaties	92% 2021: 75%

Geadviseerde verbeteracties

- prio *Stem de strategie voor back-up en herstel van gegevens af op de behoeften van bedrijfsprocessen.*
- prio *Verbeter het contractbeheer en de controle op naleven van afspraken door leveranciers en partners. Maak het sturen hierop expliciet onderdeel van "integraal management".*
- prio *Breng logbestanden op orde en controleer met steekproeven of geautomatiseerd om dreigingen, aanvallen of misbruik te kunnen opmerken.*

Risico's

- *Back-ups van gegevens en systemen voldoen niet aan behoeften van proceseigenaren.*
- *Verhoogde risico's voor informatiebeveiliging en privacy bij uitbesteden en samenwerken omdat 3de partijen in gebreke blijven.*
- *Een cyberaanval ontwricht de bedrijfsvoering of veroorzaakt een groot datalek. (zie gemeente Hof van Twente, gemeente Buren).*

5. DATABESCHERMING

redelijk

Veilige omgang met data in onze applicaties
- Data wordt op de juiste manier beschermd
- De gegevens van de burgers worden veilig opgeslagen en gecommuniceerd.
- Binnen en buiten de gemeente

85%
2021: 71%

Onderdelen:

0% - 75% | 75% - 90% | 90% - 100%

H8 / Beheer van bedrijfsmiddelen	80% 2021: 79%
H10 / Cryptografie	100%: 2021: 0%
H13 / Communicatiebeveiliging	86% 2021: 85%

Geadviseerde verbeteracties

prio
- *Beter beschermen van de meest gevoelige (gemeentelijke) gegevens tegen weg kopiëren uit de veilige omgeving.*
- *Richt het computernetwerk in met afgescheiden "kamers" (segmenten).*
- *Let op signalen die kunnen duiden op grootschalige gegevensdiefstal (data-exfiltratie) na een inbraak.*

Risico's
- *Informatie wordt onveilig en/of onrechtmatig verwerkt op apparaten die ook privé eigendom kunnen zijn.*
- *Een aanvaller (cyber-crimineel) die in ons netwerk binnen is kan ongehinderd alle "kamers" doorzoeken.*
- *Grootschalige gegevensdiefstal na een inbraak (zie: gemeente Buren).*

ENSIA VERANTWOORDING AAN HET RIJK

Getoetste collegeverklaring ENSIA - DIGID

voldaan

Van onze ENSIA-zelfevaluatie worden jaarlijks twee onderdelen geaudit door een IT-auditor: DigiD en Suwinet. De basis voor de audit vormt de collegeverklaring. Hierin zijn de uitkomsten van de ENSIA-zelfevaluatie opgenomen. Er wordt getoetst op opzet en bestaan (niet op werking). Voor DigiD worden de collegeverklaring en bijlagen als verantwoording verzonden naar toezichthouder Logius/BZK.

DigiD:
DigiD is een authenticatiemiddel dat wordt ingezet voor onze digitale dienstverlening.

Niet voldaan voldaan

Website deurne.nl	Aanvragen van diensten van de gemeente	Geen risico's	
iBurgerzaken	Aanvragen van diensten van Burgerzaken (BRP en reisdocumenten)	Geen risico's	

Voor DigiD aansluitingen voldoet Deurne op alle punten aan de norm. Daarom zijn geen verbetermaatregelen gepland.

Getoetste collegeverklaring ENSIA - Suwinet

voldaan

Van onze ENSIA-zelfevaluatie worden jaarlijks twee onderdelen geaudit door een IT-auditor: DigiD en Suwinet. De basis voor de audit vormt de collegeverklaring. Hierin zijn de uitkomsten van de ENSIA-zelfevaluatie opgenomen. Er wordt getoetst op opzet en bestaan (niet op werking). Voor Suwinet worden de collegeverklaring en bijlagen als verantwoording verzonden naar toezichthouder BKWI/SZW.

SUWI (Wet Structuur Uitvoeringsorganisatie Werk en Inkomen):
Suwinet is een digitale infrastructuur die is ontwikkeld door de Suwipartijen (UWV, SVB en gemeenten) om ervoor te zorgen dat zij gegevens met elkaar kunnen uitwisselen voor de uitoefening van hun wettelijke taak. Er worden alleen gegevens uitgewisseld waar een wettelijke grondslag voor is. Wij gebruiken Suwinet voor de uitvoering van de Participatiewet, de uitvoering van de IOAZ en IOAW, raadplegen van adresgegevens bij Burgerzaken en het raadplegen van gegevens door gemeentelijk gerechtsdeurwaarders wanneer er een getekend dwangbevel is.

Niet voldaan voldaan

Participatiewet/IOAZ/IOAW - Suwinet Inkijk - DKD Inlezen	Gebruik Suwinet door Senzer	Geen risico's	

Voor het gebruik van Suwinet voldoet Deurne op alle punten aan de norm. Daarom zijn geen verbetermaatregelen gepland.

Status Basisregistratie Personen en Reisdocumenten

redelijk

Van onze zelfevaluatie ENSIA wordt de verantwoording over de Basisregistratie Personen (BRP) en de wet- en regelgeving voor de Reisdocumenten (paspoorten en ID-kaarten) afgeleid. De uitkomsten worden verzonden aan de Rijksdienst voor de Identiteitsgegevens (RvIG). De zelfevaluatie voor informatiebeveiliging vindt via de ENSIA systematiek plaats. De verantwoording over de kwaliteit van de registraties komt voort uit de zelfevaluatie in de Kwaliteitsmonitor.

De zelfevaluaties over informatiebeveiliging en de kwaliteit leiden tot scores. Gemeenten worden geacht de volgende score te behalen, zowel voor de BRP als voor Reisdocumenten:

- Informatiebeveiliging (BIO): 1200 punten (norm = 100%)
- Kwaliteit (wettelijk): 700 punten (norm = 100%)
- Kwaliteit (aanbeveling): 100 punten (norm = 0%)

De gemeente heeft zich in VNG-verband verplicht te voldoen aan de BIO. Daarom stellen wij de norm voor Informatiebeveiliging op 1200 punten (100%).

0% - 75% 75% - 95% 95% - 100%

Basisregistratie Personen (BRP)

De zelfevaluatie BRP over het jaar 2022 is afgerond met

- Informatiebeveiliging: 1110 punten (93%)
- Kwaliteit (wettelijk): 700 punten (100%)
- Kwaliteit (aanbeveling): 83 punten (83%)

94%

Wet- en regelgeving voor Reisdocumenten

De zelfevaluatie Reisdocumenten over het jaar 2022 is afgerond met

- Informatiebeveiliging: 1100 punten (92%)
- Kwaliteit (wettelijk): 700 punten (100%)
- Kwaliteit (aanbeveling): 80 punten (80%)

94%

prio

De verbetermaatregel die de gemeente zich voorneemt is betere controle op naleven van privacy-regelgeving (de AVG) bij de BRP en Reisdocumenten. Dit was ook in 2021 het geval. Hieraan is nog geen invulling gegeven.

Status GEO-basisregistraties

voldaan

Wij verantwoorden ons aan het ministerie van BZK/Directoraat Generaal Bestuur, Ruimte en Wonen (DGBRW) over drie basisregistraties in het geografische domein. De rapportages zijn tot stand gekomen op basis van door ons uitgevoerde zelfevaluaties. De zelfevaluaties betreffen de kwaliteit van de registraties (geen informatiebeveiliging).

De zelfevaluaties over informatiebeveiliging en de kwaliteit leiden tot scores. Gemeenten worden geacht de volgende score te behalen:

- Basisregistratie Adressen en Gebouwen (BAG): norm is 75%
- Basisregistratie Grootschalige Topografie (BGT): norm, is 75%
- Basisregistratie Ondergrond (BRO): norm is 60%

0% - 74% 75% - 100%

Basisregistratie Adressen en Gebouwen (BAG)
De zelfevaluatie BAG over het jaar 2022 is afgerond met een score van 124 van maximaal 140 punten.

89%

Basisregistratie Grootschalige Topografie (BGT)
De zelfevaluatie BGT over het jaar 2022 is afgerond met een score van 90 van maximaal 120 punten.

75%

0% - 59% 60% - 100%

Basisregistratie Ondergrond (BRO)
De zelfevaluatie BRO over het jaar 2022 is afgerond met een score van 80 van maximaal 90 punten.

89%

Deurne voldoet aan de gestelde norm.
Om dit vast te houden en verder te stroomlijnen zijn diverse procesverbeteringen gepland.

Status Basisregistratie WOZ

Wij verantwoorden ons aan de toezichthouder Waarderingskamer over de uitvoering van de Wet waardering onroerende zaken (WOZ). De Belastingsamenwerking Oost-Brabant (BSOB) voert deze voor de gemeente Deurne uit. Deze rapportage is gebaseerd op een door de BSOB uitgevoerde zelfevaluatie over informatiebeveiliging en informatie-architectuur. Zelfevaluaties over andere aspecten van de WOZ-uitvoering rapporteert de BSOB direct aan de Waarderingskamer.

Belastingsamenwerking Oost-Brabant

Niet voldaan voldaan

Informatiebeveiliging	niet voldaan
Informatie-architectuur	niet voldaan

Bevindingen:

- *BSOB voldoet nog niet volledig aan de BIO.*
  Informatie-architectuur is goed in beeld. Enkele koppelvlakken waarop informatie wordt uitgewisseld voldoen niet aan huidige eisen.

Verbeteracties 2022:

- *Informatiebeveiligingsrollen zijn belegd in de organisatie.*
- *Team van CISO, Privacy Officer en FG is uitgebreid met een ISO voor de operationele informatiebeveiligingstaken.*
- *Start van projectmatige implementatie van informatiebeveiliging volgens de BIO.*

Aanbevelingen aan het college/bestuur:

- *Houd informatieveiligheid en informatiemanagement op de organisatie- en bestuurlijke agenda van BSOB.*
- *Geef de verdere implementatie van de BIO een hoge prioriteit binnen het BSOB management.*
- *Maak een plan voor vervangen van verouderde koppelvlakken.*