

ENSIA
Rapportage zelfevaluatie
gemeente Almere

Colofon

ICTU 2017

Dit rapport bevat de antwoorden van de gemeente Almere op de onderwerpen uit de ENSIA Zelfevaluatie Informatiebeveiliging BIG 2017.

Inhoudsopgave

Inhoudsopgave	2
Suwinet	16
5.1 Informatiebeveiligingsbeleid	16
5.1.1 Beleidsdocumenten voor informatiebeveiliging	16
5.1.2 Beoordeling van het informatiebeveiligingsbeleid	16
6.1 Interne organisatie	16
6.1.1 Betrokkenheid van het College van B&W bij beveiliging	16
6.1.2 Coördineren van beveiliging	17
6.1.3 Verantwoordelijkheden	17
6.1.5 Geheimhoudingsovereenkomst	17
6.1.7 Contact met speciale belangengroepen	18
6.1.8 Beoordeling van het informatiebeveiligingsbeleid	18
6.2 Externe partijen	18
6.2.1 Identificatie van risico's die betrekking hebben op externe partijen	18
6.2.3: Beveiliging behandelen in overeenkomsten met een derde partij	19
8.1 Voorafgaand aan het dienstverband	19
8.1.1 Rollen en verantwoordelijkheden	19
8.1.2 Screening	20
.....	20
8.2: Tijdens het dienstverband	20
8.2.2 Bewustwording, opleiding en training ten aanzien van informatiebeveiliging	20
8.3: Beëindiging of wijziging van het dienstverband	21
8.3.1 Beëindiging van verantwoordelijkheden	21
10.1: Bedieningsprocedures en -verantwoordelijkheden	21
10.1.1 Gedocumenteerde bedieningsprocedures	21
10.1.2 Wijzigingsbeheer	21
10.1.3 Functiescheiding	21
10.1.4 Scheiding van faciliteiten voor ontwikkeling, testen en productie	22

10.3 Systeemplanning en -acceptatie.....	22
10.3.1 Capaciteitsbeheer	22
10.6: Beheer van netwerkbeveiliging	22
10.6.1 Maatregelen voor netwerken.....	22
10.6.2 Beveiliging van netwerkdiensten.....	23
10.8: Uitwisseling van informatie	23
10.8.1 Beleid en procedures voor informatie-uitwisseling.....	23
10.8.2 Uitwisselingsovereenkomsten.....	24
10.8.3 Fysieke media die worden getransporteerd	24
10.8.4. Elektronische berichtenuitwisseling	24
.....	24
10.10: Controle	24
10.10.1 Aanmaken audit-logbestanden	24
10.10.2 Controle systeemgebruik	25
10.10.3 Bescherming van informatie in logbestanden	25
10.10.6 Synchronisatie van systeemklokken	25
11.1 Toegangsbeleid	25
11.1.1 Toegangsbeveiliging	26
11.2 Beheer van toegangsrechten van gebruikers.....	26
11.2.1 Registratie van gebruikers	26
11.2.2. Beheer van speciale bevoegdheden.....	26
11.2.3. Beheer van gebruikerswachtwoorden.....	26
11.2.4 Beoordeling van toegangsrechten van gebruikers.....	26
11.3 Verantwoordelijkheden van gebruikers	26
11.3.1 Gebruik van wachtwoorden.....	27
11.4 Toegangsbeheersing voor netwerken	27
11.4.1 Beleid ten aanzien van het gebruik van netwerkdiensten.....	27
11.4.2 Authenticatie van gebruikers bij externe verbindingen	27
11.4.6 Beheersmaatregelen voor netwerkverbindingen	27
11.4.7 Beheersmaatregelen voor netwerkroutering	27

11.6: Toegangsbeheersing voor toepassingen en informatie	27
11.6.1. Beperking van toegang tot informatie	27
.....	28
11.7 Draagbare computers en telewerken	28
11.7.1 Draagbare computers en communicatievoorzieningen	28
11.7.2 Telewerken.....	28
12.1: Beveiligingseisen voor informatiesystemen.....	28
12.1.1 Analyse en specificatie van beveiligingseisen	28
12.2 Correcte verwerking in toepassingen	29
12.2.2 Beheersing van interne gegevensverwerking	29
12.2.3 Integriteit van berichten	29
12.2.4 Validatie van uitvoergegevens	29
.....	29
12.3 Cryptografische beheersmaatregelen	29
12.3.1 Beleid voor het gebruik van cryptografische beheersmaatregelen.....	29
.....	29
12.3.2 Sleutelbeheer	29
12.4 Beveiliging van systeembestanden	29
12.4.1 Beheersing van operationele software.....	30
.....	30
12.5 Beveiliging bij ontwikkelings- en ondersteuningsprocessen.....	30
12.5.1 Procedures voor wijzigingsbeheer	30
.....	30
12.5.2 Technische beoordeling van toepassingen na wijzigingen in het besturingssysteem.....	30
.....	30
12.5.4 Uitlekken van informatie	30
.....	30
12.5.5 Uitbestede ontwikkeling van programmatuur	30
12.6 Beheer van technische kwetsbaarheden.....	31
12.6.1 Beheersing van technische kwetsbaarheden	31

13.1 Rapportage van informatiebeveiligingsgebeurtenissen en zwakke plekken	31
13.1.1 Rapportage van informatiebeveiligingsgebeurtenissen	31
13.1.2 Rapportage van zwakke plekken in de beveiliging	31
13.2 Beheer van informatiebeveiligingsincidenten en verbeteringen	32
13.2.3 Verzamelen van bewijsmateriaal	32
15.1: Naleving van wettelijke voorschriften	32
15.1.3 Bescherming van bedrijfsdocumenten	32
15.1.4 Bescherming van gegevens en geheimhouding van persoonsgegevens	32
15.1.6 Voorschriften voor het gebruik van cryptografische beheersmaatregelen	32
15.2: Naleving van beveiligingsbeleid en -normen en technische naleving	33
15.2.1 Naleving van beveiligingsbeleid en -normen	33
15.2.2 Controle op technische naleving	33
BRP & PUN	34
5.1 Informatiebeveiligingsbeleid	34
5.1.1: Beleidsdocumenten voor informatiebeveiliging	34
6.1 Interne organisatie	34
6.1.1: Betrokkenheid van het College van B&W bij beveiliging	34
6.2 Externe partijen	35
6.2.1: Identificatie van risico's die betrekking hebben op externe partijen	35
7.1 Beheer van bedrijfsmiddelen	35
7.1.2 Eigendom van bedrijfsmiddelen	35
7.1.3 Aanvaardbaar gebruik van bedrijfsmiddelen	36
8.1 Voorafgaand aan het dienstverband	36
8.1.1. Rollen en verantwoordelijkheden	36
8.2 Tijdens het dienstverband	36
8.2.1 Directieverantwoordelijkheid	36
8.2.2 Bewustwording, opleiding en training ten aanzien van informatiebeveiliging	37
8.2.3 Disciplinaire maatregelen	37
9.1 Beveiligde ruimten	37
9.1.1. Fysieke beveiliging van de omgeving	37

9.1.2 Fysieke toegangsbeveiliging	38
9.1.3. Beveiliging van kantoren, ruimten en faciliteiten	38
9.1.5 Werken in beveiligde ruimten	38
9.1.6 Openbare toegang en gebieden voor laden en lossen	39
9.2 Beveiliging van apparatuur	39
9.2.5 Beveiliging van apparatuur buiten het terrein	39
10.1 Bedieningsprocedures en -verantwoordelijkheden.....	39
10.1.1 Gedocumenteerde bedieningsprocedures.....	39
10.1.3 Functiescheiding	39
10.2 Exploitatie door een derde partij	40
10.2.1 Dienstverlening.....	40
10.2.2 Controle en beoordeling van dienstverlening door een derde partij	41
10.5 Back-up	41
10.5.1 Reservekopieën maken (back-ups)	42
10.6 Beheer van netwerkbeveiliging	42
10.6.1 Maatregelen voor netwerken.....	42
10.7 Behandeling van media	42
10.7.1 Beheer van verwijderbare media	42
10.10 Controle	43
10.10.1 Aanmaken audit-logbestanden	43
10.10.2 Controle systeemgebruik	43
11.1 Toegangsbeleid	44
11.1.1 Toegangsbeveiliging	44
11.2 Beheer van toegangsrechten van gebruikers	44
11.2.1 Registratie van gebruikers	44
11.2.2 Beheer van speciale bevoegdheden.....	44
11.2.4 Beoordeling van toegangsrechten van gebruikers.....	44
11.3 Verantwoordelijkheden van gebruikers	44
11.3.1 Gebruik van wachtwoorden.....	45
11.3.3 'Clear desk'- en 'clear screen'-beleid	45

11.4 Toegangsbeheersing voor netwerken	45
11.4.1 Beleid ten aanzien van het gebruik van netwerkdiensten	45
11.4.4 Bescherming op afstand van poorten voor diagnose en configuratie	45
11.6 Toegangsbeheersing voor toepassingen en informatie	46
11.6.2 Isolatie van gevoelige systemen	46
11.7 Draagbare computers en telewerken	46
11.7.2 Telewerken	46
12.1 Beveiligingseisen voor informatiesystemen	46
12.1.1 Analyse en specificatie van beveiligingseisen	46
14.1 Informatiebeveiligingsaspecten van bedrijfscontinuïteitsbeheer	47
14.1.3 Continuïteitsplannen ontwikkelen en implementeren waaronder informatiebeveiliging ..	47
14.1.5 Testen, onderhoud en herbeoordelen van continuïteitsplannen	47
15.1 Naleving van wettelijke voorschriften	48
15.1.1 Identificatie van toepasselijke wetgeving	48
15.2 Naleving van beveiligingsbeleid en- normen en technische naleving	48
15.2.1 Naleving van beveiligingsbeleid en -normen	48
BAG & BGT	49
10.5 Back-up	49
14.1 Informatiebeveiligingsaspecten van bedrijfscontinuïteitsbeheer	49
BIG hoofdstuk 3: Implementatie van de Tactische Baseline	51
3.1 ISMS beleid (met basis IBP)	51
hoofdstuk 4 Samenwerkingsverbanden	52
4.1 Risicobeoordeling en risicoafweging	52
BIG hoofdstuk 5: Beveiligingsbeleid	53
5.1 Informatiebeveiligingsbeleid	53
5.1.1 Beleidsdocumenten voor informatiebeveiliging	53
5.1.2 Beoordeling van het informatiebeveiligingsbeleid	53
BIG hoofdstuk 6: Organisatie van de informatiebeveiliging	54
6.1 Interne organisatie	54
6.1.1: Betrokkenheid van het College van B&W bij beveiliging	54

6.1.2: Coördineren van beveiliging.....	54
6.1.3: Verantwoordelijkheden.....	54
6.1.4: Goedkeuringsproces voor ICT-voorzieningen	54
6.1.5: Geheimhoudingsovereenkomst	55
6.1.6: Contact met overheidsinstanties	55
6.1.7: Contact met speciale belangengroepen	55
6.1.8: Beoordeling van het informatiebeveiligingsbeleid	56
6.2 Externe Partijen	56
6.2.1: Identificatie van risico's die betrekking hebben op externe partijen.....	56
6.2.2: Beveiliging beoordelen in de omgang met klanten	58
6.2.3: Beveiliging behandelen in overeenkomsten met een derde partij	58
BIG hoofdstuk 7: Beheer van bedrijfsmiddelen	60
7.1 Beheer van bedrijfsmiddelen	60
7.1.1 Inventarisatie van bedrijfsmiddelen.....	60
7.1.2 Eigendom van bedrijfsmiddelen	60
7.1.3 Aanvaardbaar gebruik van bedrijfsmiddelen.....	60
7.2 Classificatie van informatie	60
7.2.1 Richtlijnen voor classificatie van informatie	60
7.2.2 Labeling en verwerking van informatie	61
BIG hoofdstuk 8: Personele beveiliging	62
8.1 Voorafgaand aan het dienstverband	62
8.1.1 Rollen en verantwoordelijkheden	62
8.1.2 Screening	62
8.1.3 Arbeidsvoorwaarden	62
8.2 Tijdens het dienstverband.....	63
8.2.1 Directieverantwoordelijkheid	63
8.2.2 Bewustwording, opleiding en training ten aanzien van informatiebeveiliging	63
8.2.3 Disciplinaire maatregelen.....	63
8.3 Beëindiging of wijziging van het dienstverband.....	64
8.3.1 Beëindiging van verantwoordelijkheden	64

BIG hoofdstuk 9: Fysieke beveiliging en beveiliging van de omgeving	65
9.1 Beveiligde ruimten	65
9.1.1 Fysieke beveiliging van de omgeving	65
9.1.2 Fysieke toegangsbeveiliging	65
9.1.3 Beveiliging van kantoren, ruimten en faciliteiten	65
9.1.4 Bescherming tegen bedreigingen van buitenaf	66
9.1.5 Werken in beveiligde ruimten	66
9.1.6 Openbare toegang en gebieden voor laden en lossen	66
9.2 Beveiliging van apparatuur	67
9.2.1 Plaatsing en bescherming van apparatuur	67
9.2.2 Plaatsing en bescherming van apparatuur	67
9.2.3 Beveiliging van kabels	67
9.2.4 Onderhoud van apparatuur	67
9.2.5 Beveiliging van apparatuur buiten het terrein	67
9.2.6 Veilig verwijderen of hergebruiken van apparatuur	68
9.2.7 Veilig verwijderen of hergebruiken van apparatuur	68
BIG hoofdstuk 10: Beheer van Communicatie en bedieningsprocessen	69
10.1 Bedieningsprocedures en verantwoordelijkheden	69
10.1.1 Gedocumenteerde bedieningsprocedures	69
10.1.2 Wijzigingsbeheer	69
10.1.3 Functiescheiding	69
10.1.4 Scheiding van faciliteiten voor ontwikkeling, testen en productie	70
10.2 Exploitaties door een derde partij	70
10.2.1 Dienstverlening	70
10.2.2 Controle en beoordeling van dienstverlening door een derde partij	71
10.2.3 Beheer van wijzigingen in dienstverlening door een derde partij	72
10.3 Systeemplanning en acceptatie	72
10.3.1 Capaciteitsbeheer	72
10.3.2. Systeem acceptatie	72
10.4 Bescherming van virussen en 'mobile code'	72

10.4.1 Maatregelen tegen virussen	72
10.4.2 Maatregelen tegen 'mobile code'	73
10.5 Back-up	73
10.5.1 Reservekopieën maken (back-ups)	73
10.6 Beheer van netwerkbeveiliging	73
10.6.1 Maatregelen voor netwerken	73
10.6.2 Beveiliging van netwerkdiensten	74
10.7 Behandeling van media	74
10.7.1 Beheer van verwijderbare media	74
10.7.2 Verwijdering van media	74
10.7.3 Procedures voor de behandeling van informatie	75
10.7.4 Beveiliging van systeemdokumentatie	75
10.8 Uitwisseling van informatie	75
10.8.1 Beleid en procedures voor informatie-uitwisseling	75
10.8.2 Uitwisselingsovereenkomsten	76
10.8.3 Fysieke media die worden getransporteerd	76
10.8.4. Elektronische berichtenuitwisseling	76
10.8.5 Systemen voor bedrijfsinformatie	77
10.9 Diensten voor e-commerce	77
10.9.1 E-commerce	77
10.9.3 Openbaar beschikbare informatie	77
10.10 Controle	77
10.10.1 Aanmaken audit-logbestanden	78
10.10.2 Controle systeemgebruik	78
10.10.3 Bescherming van informatie in logbestanden	78
10.10.6 Synchronisatie van systeemklokken	78
BIG hoofdstuk 11: Toegangsbeveiliging	80
11.1 Toegangsbeleid	80
11.1.1 Toegangsbeveiliging	80
.....	80

11.2 Beheer van toegangsrechten van gebruikers	80
11.2.1 Registratie van gebruikers	80
.....	80
11.2.2. Beheer van speciale bevoegdheden.....	80
11.2.3. Beheer van gebruikerswachtwoorden.....	80
.....	80
11.2.4 Beoordeling van toegangsrechten van gebruikers.....	80
11.3 Verantwoordelijkheden van gebruikers	81
11.3.1 Gebruik van wachtwoorden.....	81
11.3.2 Onbeheerde gebruikersapparatuur	81
.....	82
11.3.3 'Clear desk'- en 'clear screen'-beleid	82
11.4 Toegangsbeheersing voor netwerken	82
11.4.1 Beleid ten aanzien van het gebruik van netwerkdiensten.....	82
11.4.2 Authenticatie van gebruikers bij externe verbindingen	82
11.4.3 Identificatie van (netwerk)apparatuur.....	82
11.4.4 Bescherming op afstand van poorten voor diagnose en configuratie.....	82
11.4.5 Scheiding van netwerken	83
11.4.6 Beheersmaatregelen voor netwerkverbindingen	83
11.4.7 Beheersmaatregelen voor netwerkroutering.....	83
11.5 Toegangsbeveiliging voor besturingssystemen	83
11.5.1 Beveiligde inlogprocedures	83
11.5.2 Gebruikersidentificatie en -authenticatie	84
.....	84
11.5.3 Systemen voor wachtwoordbeheer.....	84
11.5.4 Gebruik van systeemhulpmiddelen	84
11.5.5 Time-out van sessies	84
11.5.6 Beperking van verbindingstijd	84
11.6 Toegangsbeheersing voor toepassingen en informatie	85
11.6.1. Beperking van toegang tot informatie	85

.....	85
11.6.2 Isolatie van gevoelige systemen	85
11.7 Draagbare computers en telenetwerken	85
11.7.1 Draagbare computers en communicatievoorzieningen	85
11.7.2 Telewerken.....	86
BIG hoofdstuk 12: Verwerving, ontwikkeling en onderhoud van informatiesystemen	87
12.1 Beveiligingseisen voor informatiesystemen.....	87
12.1.1 Analyse en specificatie van beveiligingseisen	87
12.2 Correcte verwerking in toepassingen	87
12.2.1 Validatie van invoergegevens (BRP)	87
12.2.2 Beheersing van interne gegevensverwerking	87
12.2.3 Integriteit van berichten	88
12.2.4 Validatie van uitvoergegevens	88
12.3 Cryptografische beheersmaatregelen	88
12.3.1 Beleid voor het gebruik van cryptografische beheersmaatregelen.....	89
12.3.2 Sleutelbeheer	89
12.4 Beveiliging van systeembestanden	89
12.4.1 Beheersing van operationele software.....	89
12.4.2 Bescherming van testdata.....	89
12.4.3 Toegangsbeheersing voor broncode van programmatuur.....	89
12.5 Beveiliging bij ontwikkeling en ondersteuningsprocessen.....	90
12.5.1 Procedures voor wijzigingsbeheer	90
12.5.2 Technische beoordeling van toepassingen na wijzigingen in het besturingssysteem.....	90
12.5.3 Restricties op wijzigingen in programmatuurpakketten	90
12.5.4 Uitlekken van informatie	91
12.5.5 Uitbestede ontwikkeling van programmatuur	91
12.6 Beheer van technische kwetsbaarheden.....	91
12.6.1 Beheersing van technische kwetsbaarheden	91
BIG hoofdstuk 13: Beheer van informatiebeveiligingsincidenten	93
13.1 Rapportage van informatiebeveiligingsgebeurtenissen en zwakke plekken	93

13.1.1 Rapportage van informatiebeveiligingsgebeurtenissen	93
13.1.2 Rapportage van zwakke plekken in de beveiliging	93
13.2 Beheer van informatiebeveiligingsincidenten en verbeteringen	93
13.2.1 Verantwoordelijkheden en procedures	93
13.2.2. Leren van informatiebeveiligingsincidenten	93
13.2.3 Verzamelen van bewijsmateriaal	94
BIG hoofdstuk 14: Bedrijfscontinuïteitsbeheer	95
14.1 Informatiebeveiligingsaspecten van bedrijfscontinuïteitsbeheer	95
14.1.1 Informatiebeveiliging opnemen in het proces van bedrijfscontinuïteitsbeheer	95
14.1.2 Bedrijfscontinuïteit en risicobeoordeling	95
14.1.3 Continuïteitsplannen ontwikkelen en implementeren waaronder informatiebeveiliging ..	95
14.1.4 Kader voor de bedrijfscontinuïteitsplanning	96
14.1.5 Testen, onderhoud en herbeoordelen van continuïteitsplannen.....	96
BIG hoofdstuk 15: Naleving.....	98
15.1 Naleving van wettelijke voorschriften	98
15.1.1 Identificatie van toepasselijke wetgeving	98
15.1.2 Intellectuele eigendomsrechten (Intellectual Property Rights (IPR))	98
15.1.3 Bescherming van bedrijfsdocumenten.....	98
15.1.4 Bescherming van gegevens en geheimhouding van persoonsgegevens	99
15.1.5 Voorkomen van misbruik van ICT-voorzieningen	99
15.1.6 Voorschriften voor het gebruik van cryptografische beheersmaatregelen	99
15.2 Naleving van beveiligingsbeleid en -normen en controle op technische naleving	100
15.2.1 Naleving van beveiligingsbeleid en -normen	100
15.2.2 Controle op technische naleving	100
15.3 Overwegingen bij audits van informatiesystemen	101
15.3.1 Beheersmaatregelen voor audits van informatiesystemen	101
15.3.2 Bescherming van hulpmiddelen voor audits van informatiesystemen	101

Leeswijzer

In dit rapport zijn de vragen en ingevulde antwoorden opgenomen uit de ENSIA BIG vragenlijst 2017. Het rapport ondersteunt gemeenten bij het opstellen van een verbeterplan. Het rapport is opgesteld in MS-Word formaat. U kunt de inhoud van de kolommen verder uitwerken om zo te komen tot een evaluatie en de bouwstenen voor een verbeterplan. Houdt hierbij telkens voor ogen welke detailniveau over informatieveiligheid u vrijgeeft aan uw doelgroep in verband met inzage in uw organisatiebeveiliging en de risico's die u daarbij loopt.

De rapportage bevat 4 kolommen: vraag, antwoord, advies en een kolom met evaluatie en impact. Wanneer de vraag bij een BIG-norm negatief beantwoord is (antwoord "nee"), wordt in de derde kolom een advies getoond. Dit inhoud van het advies geeft de reden en noodzaak om de betreffende BIG-norm te implementeren. In de vierde kolom is ruimte om te bepalen welk risico u loopt wanneer u op dit onderdeel niet voldoet aan de norm en om te bepalen met welke prioriteit de BIG-norm alsnog geïmplementeerd moet worden. Deze maatregelen moeten uiteindelijk worden opgenomen in het verbeterplan en volgens het principe van de PDCA-cyclus worden geïmplementeerd.

In de vierde kolom 'evaluatie en impact' is de mogelijkheid tot het maken van een risicoafweging. Er is een aantal vragen opgenomen om de risico's in kaart te brengen en een afweging te maken tot inzet (en in welke mate) van tegenmaatregelen. De risico's dienen geïdentificeerd, ingeschat, beoordeelt en beheerst te worden. Risicobeheersing zet u in om de impact van een manifest geworden risico te vermijden (opheffen van de oorzaak), te verminderen (terugbrengen netto verwachte omvang en/of terugbrengen waarschijnlijkheid) of het overdragen van het risico (bijvoorbeeld door te verzekeren of het aan anderen te geven).

De volgende ondersteunende vragen worden getoond in de vierde kolom:

1. **Betreft de vraag wetgeving? Indien ja, dan moet ik het implementeren.**

Indien een BIG-norm is afgeleid van wetgeving kunt u er niet voor kiezen om deze norm niet te implementeren en dient deze altijd te worden geïmplementeerd. Indien een antwoord negatief scoort bij vragen met betrekking op het SUWI- en DigiD normenkader, moet u sowieso een verbeterplan opstellen. In de collegeverklaring staat: 'De op de uitzonderingen gerichte beheersmaatregelen zijn in verbeterplannen opgenomen, zijn belegd en worden gemonitord.'

2. **Wat is het risico wanneer ik dit niet implementeer (kans x impact)?**

Om te bepalen met welke prioriteit een norm moet worden ingevoerd, maakt u een afweging welk risico uw organisatie loopt wanneer de norm niet wordt geïmplementeerd. Risico is de kans van optreden van een gebeurtenis maal de impact die de gebeurtenis heeft. Een grote kans hoeft nog geen groot risico te betekenen. En omgekeerd: wanneer de kans van een gebeurtenis groot is, maar het nadelige effect ervan heel klein, dan is het risico ook niet al te groot.

3. **Wat kost het ons als het risico manifest wordt?**

Naast de kans en de impact van een risico, dient vanuit bedrijfsvoering de vraag te worden beantwoord om de kosten van de schadelijke gevolgen van een manifest risico te normaliseren.

4. **Wat kost het om te implementeren?**

Risico's kunnen worden vermeden, verminderd of overgedragen. Om tegenmaatregelen in te implementeren is capaciteit nodig in termen van inzet van mensen en/of budget. De omvang en het beschikbaar krijgen/stellen van financiering dient in kaart te worden gebracht in de prioritering van implementatie van de maatregelen.

Slotvraag: Dient deze control geïmplementeerd te worden en met welke prioriteit?

Op basis van de uitwerking van bovenstaande antwoorden kunt u het antwoord op deze vraag geven en dit als advies voorleggen aan uw portefeuillehouder. Tenslotte, het bestuur besluit een tegenmaatregel te implementeren en met welke inzet van middelen dat mag gebeuren. Hierbij moet worden opgemerkt dat sommige maatregelen veel van de organisatie vragen en dat een verbeterplan daarom ook meerdere jaren kan beslaan of pas later in de tijd opgepakt zal worden.

Mocht het bestuur kiezen een bepaalde maatregel niet te implementeren dan dient daar verslag van te worden gemaakt, zodat in het kader van pas-toe-of-leg-uit aan dossiervorming gedaan wordt.

5.1 Informatiebeveiligingsbeleid

5.1.1 Beleidsdocumenten voor informatiebeveiliging

Vraag	Antwoord	Suwinorm 2017
5.1.1.a Is er een actueel informatiebeveiligingsbeleid (gebaseerd op de BIG)?	Ja	B.01
Is het informatiebeveiligingsbeleid vastgesteld door het College?	Ja	Niet van toepassing
Is het informatiebeveiligingsbeleid jonger dan drie jaar?	Ja	Niet van toepassing
Is het informatiebeveiligingsbeleid gepubliceerd en kenbaar gemaakt aan alle medewerkers en externe partijen?	Ja	Niet van toepassing
5.1.1.b Is er in het gemeentelijk informatiebeveiligingsbeleid expliciet aandacht voor speciale gemeentelijke voorzieningen en wetgeving?	Ja	B.01
Kunt u aangeven voor welke voorzieningen en wetgeving er expliciet aandacht is in het informatiebeveiligingsbeleid?	<ul style="list-style-type: none"> • Voor de BRP • Voor de PUN • Voor Suwinet 	
5.1.1.c Heeft u het gemeentelijke informatiebeveiligingsbeleid vertaald naar te nemen maatregelen of te implementeren maatregelen naar de door u opgerichte samenwerkingsverbanden of die waarin uw gemeente een deelname heeft?	N.v.t	B.01

5.1.2 Beoordeling van het informatiebeveiligingsbeleid

Vraag	Antwoord	Suwinorm 2017
5.1.2.a Wordt het informatiebeveiligingsbeleid minimaal één keer per drie jaar of bij grote wijzigingen binnen de organisatie opnieuw beoordeeld en indien nodig aangepast?	Ja	C.01

6.1 Interne organisatie

6.1.1 Betrokkenheid van het College van B&W bij beveiliging

Vraag	Antwoord	Suwinorm 2017
-------	----------	---------------

6.1.1.a Worden de informatiebeveiligingsdoelstellingen vastgesteld door het College?	Ja	B.01, C.01
Wordt de voortgang jaarlijks besproken tussen bestuur en management?	Ja	Niet van toepassing
Wordt er over de voortgang gerapporteerd?	Ja	Niet van toepassing

6.1.2 Coördineren van beveiliging

Vraag	Antwoord	Suwinorm 2017
6.1.2. a Zijn de informatiebeveiligingsactiviteiten vastgesteld en belegd? Door welke vertegenwoordigers / rollen worden de informatiebeveiligingsactiviteiten (op alle niveaus) uitgevoerd binnen de organisatie?	Ja <ul style="list-style-type: none"> • CISO • Er zijn op afdelingsniveau en binnen samenwerkingsverbanden IB-contactpersonen 	B.04 Niet van toepassing
Kunt u aangeven op welke wijze er intern verantwoording wordt afgelegd over de informatiebeveiligingsactiviteiten?	Er vindt niet iedere drie jaar verantwoording plaats en/of er is geen onafhankelijke toets	B.04

6.1.3 Verantwoordelijkheden

Vraag	Antwoord	Suwinorm 2017
6.1.3 a Zijn de beveiligingsrollen voor wat betreft informatiebeveiliging van de (lijn, proces, systeem) manager belegd?	<ul style="list-style-type: none"> • Ja, in de functiebeschrijvingen • Ja, in de taakopdrachten • Ja, voor de basisregistraties 	B.05

6.1.5 Geheimhoudingsovereenkomst

Vraag	Antwoord	Suwinorm 2017
6.1.5.a Is er een beleid om de geheimhoudingsverklaring te laten tekenen bij een aanstelling? Kunt u aangeven op welke wijze dit gebeurt?	Ja <ul style="list-style-type: none"> • Iedere ambtelijk medewerker ondertekent een individuele verklaring integriteit / tot geheimhouding of legt de ambtseed of ambtsbelofte af • Externe en tijdelijke medewerkers ondertekenen een geheimhoudingsverklaring 	Niet van toepassing Niet van toepassing

	<ul style="list-style-type: none"> Bij de aanstelling wordt een VOG gevraagd 	
--	---	--

6.1.7 Contact met speciale belangengroepen

Vraag	Antwoord	Suwinorm 2017
6.1.7.a Onderhoud de gemeente contacten met relevante expertise groepen en leveranciers om in geval van incidenten snel/juist te kunnen handelen?	Ja	B.04
Kunt u aangeven met welke expertisegroepen uw gemeenten contacten onderhoudt?	<ul style="list-style-type: none"> IBD BKWI 	Niet van toepassing

6.1.8 Beoordeling van het informatiebeveiligingsbeleid

Vraag	Antwoord	Suwinorm 2017
6.1.8.a Wordt het informatiebeveiligingsbeleid onafhankelijk beoordeeld en wordt hierover intern verantwoording afgelegd?	Ja	C.01, C.08
6.1.8.b Wordt over het functioneren van informatiebeveiliging verantwoording afgelegd aan de gemeenteraad?	Ja, minimaal 1 keer per jaar	C.01, C.08
6.1.8.c Heeft u een sluitende IB-verantwoording ingericht binnen uw gemeente?	Ja	C.01, C.08

6.2 Externe partijen

6.2.1 Identificatie van risico's die betrekking hebben op externe partijen

Vraag	Antwoord	Suwinorm 2017
6.2.1.a Worden externe partijen (inclusief samenwerkingsverbanden) gebruikt om ICT-voorzieningen in stand te houden dan wel te beheren of worden externe partijen gebruikt voor de invulling van bedrijfsprocessen?	Externe partijen worden zowel voor het in standhouden/beheren van ICT-voorzieningen als voor de invulling van bedrijfsprocessen gebruikt	B.03
6.2.1.b Is er voor uitbesteding van een proces of systeem een risicoafweging gemaakt en zijn de relevante beveiligingsrisico's in kaart gebracht?	Ja	B.03
6.2.1.c Als er uitbesteed is, zijn er dan beveiligingsmaatregelen vastgelegd in de (inkoop) contracten?	Ja	B.03
6.2.1.d Als er uitbesteed is en er zijn persoonsgegevens betrokken, is er dan met de leverancier een bewerkersovereenkomst conform het model van de BIG-OP		B.03

afgesloten? Kunt u aangeven op welke wijze de afspraken zijn gemaakt?	Niet van toepassing • Op basis van de BIG en in overleg met de leverancier	B.03
6.2.1.e Als er persoonsgegevens verwerkt worden, is er dan een wettelijke grondslag en is doelbinding en proportionaliteit gewaarborgd?	Niet van toepassing	B.03
6.2.1.f Is in deze contracten opgenomen dat een leverancier verplicht is om binnen 24 uur alle beveiligingsinbreuken te melden? (WBP-eis).	Niet van toepassing	Niet van toepassing
6.2.1.g Worden de aan de leverancier opgelegde informatiebeveiligingsmaatregelen jaarlijks gecontroleerd?	Ja, en we ontvangen een TPM/SAE/SAS	Niet van toepassing
6.2.1.h Worden de rapportages over leveranciers verwerkt in de Collegeverklaring?	Ja	Niet van toepassing

6.2.3: Beveiliging behandelen in overeenkomsten met een derde partij

Vraag	Antwoord	Suwinorm 2017
6.2.3.a Zijn alle ontdekte beveiligingsmaatregelen uit de risicoafweging vastgelegd en geïmplementeerd voordat het product of de dienst in werking gezet wordt?	Nee	Niet van toepassing
Welke van de volgende onderwerpen zijn vastgelegd en geregeld in formele contracten bij de uitbesteding dan wel ontwikkeling van software?	Niet van toepassing	Niet van toepassing
6.2.3.b Is in contracten vastgelegd hoe wordt omgegaan met wijzigingsbeheer?	Ja	Niet van toepassing
6.2.3.c Is in contracten met externe leveranciers de aansprakelijkheid uitgewerkt?	Ja	Niet van toepassing
6.2.3.d Worden leveranciereisen doorvertaald naar onderaannemers?	Ja	B.03, U.01
6.2.3.e Is in contracten vastgelegd hoe er wordt omgegaan met geheimhouding?	Ja	Niet van toepassing

8.1 Voorafgaand aan het dienstverband

8.1.1 Rollen en verantwoordelijkheden

Vraag	Antwoord	Suwinorm 2017
-------	----------	---------------

8.1.1.a Zijn de rollen en verantwoordelijkheden van werknemers, ingehuurd personeel en externe gebruikers met betrekking tot informatiebeveiliging vastgelegd?	Ja	Niet van toepassing
Kunt u aangeven met betrekking tot welke van de hiernaast genoemde opties dit wordt vastgelegd en gecommuniceerd?	<ul style="list-style-type: none"> • m.b.t. het beveiligingsbeleid • m.b.t. de bescherming van bedrijfsmiddelen • m.b.t. speciale verantwoordelijkheden (ingeval van een BRP, BUN, SUWI rol/functie) • m.b.t. de rapportage van beveiligingsincidenten 	Niet van toepassing

8.1.2 Screening

Vraag	Antwoord	Suwinorm 2017
8.1.2.a Wordt de achtergrond van kandidaten voor een dienstverband, ingehuurd personeel en externe gebruikers evenredig gecontroleerd aan de eisen volgend uit de classificatie van informatie waar men toegang toe krijgt?	Ja	Niet van toepassing
Worden deze controles periodiek herhaald?	Nee	Niet van toepassing
Worden de gegevens die de medewerker opgeeft geverifieerd?	Ja	Niet van toepassing
Is voor alle medewerkers minimaal een VOG vereist?	Ja	Niet van toepassing

8.2: Tijdens het dienstverband

8.2.2 Bewustwording, opleiding en training ten aanzien van informatiebeveiliging

Vraag	Antwoord	Suwinorm 2017
8.2.2.a Zorgt het management ervoor dat de medewerkers voldoende kennis en bewustzijn hebben op het gebied van informatiebeveiliging?	Ja	B.01
Hoe zorgt het management hier voor?	<ul style="list-style-type: none"> • met bewustwordingscampagnes 	Niet van toepassing
Zijn hier verslagen van?	Ja	Niet van toepassing
Zijn er voldoende middelen gealloceerd voor het bevorderen	Ja	Niet van toepassing

van kennis en bewustwording van de medewerkers ten aanzien van informatieveiligheid?		
--	--	--

8.3: Beëindiging of wijziging van het dienstverband

8.3.1 Beëindiging van verantwoordelijkheden

Vraag	Antwoord	Suwinorm 2017
8.3.1.a Heeft het lijnmanagement een procedure vastgesteld bij wijziging of beëindiging van het dienstverband, contract of overeenkomst op het gebied van informatiebeveiliging?	Ja	U.02
8.3.1.b Worden toegangsrechten volgens de procedure ingetrokken als het dienstverband wijzigt dan wel eindigt?	Ja	Niet van toepassing

10.1: Bedieningsprocedures en -verantwoordelijkheden

10.1.1 Gedocumenteerde bedieningsprocedures

Vraag	Antwoord	Suwinorm 2017
10.1.1.a Zijn er actuele schriftelijke procedures voor het operationeel beheer (en gebruik) van de IT voorzieningen (software, hardware, netwerk, databases)?	Ja	Niet van toepassing
10.1.1.b Wordt de Suwinetinfrastructuur, servers en netwerkcomponenten, gehardend volgens de vastgestelde configuratie baseline?	Ja	U.10

10.1.2 Wijzigingsbeheer

Vraag	Antwoord	Suwinorm 2017
10.1.2.a Is er een vastgestelde procedure voor het beheerst uitvoeren van wijzigingen op de IT voorzieningen (een wijzigingsbeheerproces)?	Ja	C.03
Zijn hier ook verslagen van?	Ja	Niet van toepassing

10.1.3 Functiescheiding

Vraag	Antwoord	Suwinorm 2017
10.1.3.a Zijn de taken en verantwoordelijkheden voor het	Ja	B.05

gebruik en het beheer van IT voorzieningen naar rato van de organisatiegrootte gescheiden?		
Kunt u aangeven hoe de taken en verantwoordelijkheden voor het gebruik en het beheer van IT voorzieningen zijn gescheiden?	<ul style="list-style-type: none"> • Dit hebben we gedaan voor de functies van BRP, PUN en SUWI • De rol van CISO of controller informatiebeveiliging is apart, onafhankelijk belegd 	Niet van toepassing
10.1.3.b Welke rollen en functiebenamingen zijn er belegd, dan wel aangewezen door het college?	<ul style="list-style-type: none"> • Systeembeheerder • Applicatiebeheerder BRP • Gegevensbeheerder BRP • Privacybeheerder BRP • Security Officer SUWI • Toezichthouder BRP 	B.05
10.1.3.c Is er sprake van een scheiding in verantwoordelijkheden tussen: uitvoerder en de beveiligingsfunctionaris en tussen opdrachtgever en de beveiligingsfunctionaris?	<ul style="list-style-type: none"> • Ja, tussen de uitvoerder en de beveiligingsfunctionaris • Ja, tussen de opdrachtgever en de beveiligingsfunctionaris 	Niet van toepassing

10.1.4 Scheiding van faciliteiten voor ontwikkeling, testen en productie

Vraag	Antwoord	Suwinorm 2017
10.1.4.a Wordt er in huis software ontwikkeld of getest?	Er wordt alleen software getest	U.09
Maakt u daarbij gebruik van een OTAP-omgeving?	Ja	Niet van toepassing

10.3 Systeemplanning en -acceptatie

10.3.1 Capaciteitsbeheer

Vraag	Antwoord	Suwinorm 2017
10.3.1.a Zijn er maatregelen getroffen waarmee de afgesproken actuele en toekomstig systeembelasting inzichtelijk en op voldoende niveau is?	Ja Nee	Niet van toepassing
10.3.2.a Is er een formele testprocedure voor accepteren van nieuwe en gewijzigde systemen (zowel door de gebruikersorganisatie als het beheer)?	Ja	C.03

10.6: Beheer van netwerkbeveiliging

10.6.1 Maatregelen voor netwerken

Vraag	Antwoord	Suwinorm 2017
10.6.1.a Welke maatregelen heeft u genomen om de aanwezige netwerken adequaat te monitoren en beveiligen?	<ul style="list-style-type: none"> • Wij hebben dit uitbesteed bij een andere gemeente/leverancier • Wij hebben op alle vertrouwde koppelvlakken een beheerde firewall • Wij maken generiek gebruik van een IDS • Wij doen aan content scanning • De gegevensuitwisseling tussen vertrouwde en onvertrouwde zones worden inhoudelijk geautomatiseerd en gecontroleerd op de aanwezigheid van malware • Er zijn procedures voor beheer van apparatuur op afstand 	Niet van toepassing
10.6.1.b Heeft u al deze maatregelen ook expliciet ingezet in het kader van telewerken in relatie tot BRP en Suwi?	Ja	Niet van toepassing

10.6.2 Beveiliging van netwerkdiensten

Vraag	Antwoord	Suwinorm 2017
10.6.2.a Worden de beveiligingskenmerken, de niveaus van dienstverlening en de beheereisen vanuit systemen en processen doorvertaald naar de overeenkomsten voor netwerkdiensten?	Ja	Niet van toepassing

10.8: Uitwisseling van informatie

10.8.1 Beleid en procedures voor informatie-uitwisseling

Vraag	Antwoord	Suwinorm 2017
10.8.1.a Is er beleid en zijn er procedures voor een beheerste en beveiligde wijze van informatie-uitwisseling, zowel binnen als buiten de gemeente?	Ja	U.07, U.08, B.01
Kunt u aangeven waarvoor deze procedures en beleid gelden?	<ul style="list-style-type: none"> • Voor transport van geclassificeerde informatie • Voor faxen en e-mail 	Niet van toepassing

	<ul style="list-style-type: none"> • Voor mobiele apparaten 	
Zijn de medewerkers geïnstrueerd over het beleid en procedures voor een beheerste en beveiligde wijze van informatie-uitwisseling?	Ja	Niet van toepassing

10.8.2 Uitwisselingsovereenkomsten

Vraag	Antwoord	Suwinorm 2017
10.8.2.a Zijn er overeenkomsten afgesloten voor de beheerste en beveiligde wijze van informatie-uitwisseling met andere partijen?	Ja	Niet van toepassing
Kunt u aangeven welke van de hiernaast genoemde aspecten zijn meegenomen in de overeenkomst?	<ul style="list-style-type: none"> • Betrouwbaarheid 	Niet van toepassing
Is de overeenkomst bij alle medewerkers bekend?	Nee	Niet van toepassing

10.8.3 Fysieke media die worden getransporteerd

Vraag	Antwoord	Suwinorm 2017
10.8.3.a Is er een procedure of zijn er middelen waarmee bij transport van (verwijderbare / mobiele) elektronische gegevensdragers zoals cd-roms, usb-sticks, externe disks en backup tapes maar ook lap-tops) vertrouwelijke informatie op een veilige wijze is opgeslagen?	Ja	Niet van toepassing

10.8.4. Elektronische berichtenuitwisseling

Vraag	Antwoord	Suwinorm 2017
10.8.4.a Zijn er middelen waarmee vertrouwelijke informatie op adequate wijze is beveiligd bij uitwisseling via berichtenverkeer (bijvoorbeeld XML of e-mail)?	Ja	U.07, U.08, B.01, B.06
Kunt u aangeven welke middelen hiervoor worden ingezet?	<ul style="list-style-type: none"> • Encryptie • PKI-Overheid 	Niet van toepassing

10.10: Controle

10.10.1 Aanmaken audit-logbestanden

Vraag	Antwoord	Suwinorm 2017
-------	----------	---------------

10.10.1.a Worden systeemhandelingen gelogd, zodanig dat handelingen van gebruikers en beheerders kunnen worden geanalyseerd onder meer t.b.v. een audittrail?	Ja	C.05
Kunt u aangeven voor welke systemen er wordt gelogd?	<ul style="list-style-type: none"> • Ja, voor wat betreft Suwinet-inlezen en DKD-inlezen • Ja, voor wat betreft BRP • Ja, voor overige systemen 	Niet van toepassing
Worden storingen gelogd?	Ja	Niet van toepassing
Worden administratieve handelingen gelogd?	Ja	Niet van toepassing
Worden de login-gegevens minimaal 3 maanden bewaard?	Ja	Niet van toepassing

10.10.2 Controle systeemgebruik

Vraag	Antwoord	Suwinorm 2017
10.10.2.a Is er een procedure voor het structureel controleren van de logbestanden op het netwerk-systeemgebruik?	Ja	C.06
Kunt u aangeven of er een procedure is om de handelingen van gebruikers te controleren?	Voor wat betreft SUWI Voor wat betreft BRP Voor wat betreft DigiD	Niet van toepassing

10.10.3 Bescherming van informatie in logbestanden

Vraag	Antwoord	Suwinorm 2017
10.10.3.a Krijgen logbestanden adequate bescherming tegen verminking, verlies en verandering?	Ja	C.05

10.10.6 Synchronisatie van systeemklokken

Vraag	Antwoord	Suwinorm 2017
10.10.6.a Wordt er kloksynchronisatie toegepast op alle actieve infrastructuur en informatiesystemen?	Ja	Niet van toepassing

11.1 Toegangsbeleid

11.1.1 Toegangsbeveiliging

Vraag	Antwoord	Suwinorm 2017
11.1.1.a Is er beleid vastgesteld dat richting geeft aan de beheerste logische toegang tot gegevens en informatie?	Ja	Niet van toepassing

11.2 Beheer van toegangsrechten van gebruikers

11.2.1 Registratie van gebruikers

Vraag	Antwoord	Suwinorm 2017
11.2.1.a Is er een vastgestelde autorisatieprocedure voor het administreren van gebruikers en het toekennen / intrekken van toegangsrechten voor alle informatie en –systemen en de controle daarop?	Ja	U.02, U.03, U.04
Is deze procedure belegd bij de betrokken systeem/proces eigenaar?	Ja	Niet van toepassing

11.2.2. Beheer van speciale bevoegdheden

Vraag	Antwoord	Suwinorm 2017
11.2.2.a Wordt de toewijzing en het gebruik van speciale bevoegdheden beperkt en beheerst?	Ja	U.02, U.03, U.04
Is dit herleidbaar aan een (beheer) principe of doelstelling?	Ja	Niet van toepassing

11.2.3. Beheer van gebruikerswachtwoorden

Vraag	Antwoord	Suwinorm 2017
11.2.3.a Is er een vastgestelde procedure voor de vormgeving en het (veilig) uitgeven en opslaan van wachtwoorden en andere authenticatie middelen?	Ja	U.03

11.2.4 Beoordeling van toegangsrechten van gebruikers

Vraag	Antwoord	Suwinorm 2017
11.2.4.a Worden de toegangsrechten van gebruikers regelmatig beoordeeld in een formeel proces?	Ja	C.04
Zijn er verslagen van de beoordeling van de toegangsrechten?	Ja	Niet van toepassing

11.3 Verantwoordelijkheden van gebruikers

11.3.1 Gebruik van wachtwoorden

Vraag	Antwoord	Suwinorm 2017
11.3.1.a Worden alle medewerkers regelmatig geïnformeerd over de regels voor het juist en veilig gebruik van wachtwoorden?	Ja	U.05, B.01

11.4 Toegangsbeheersing voor netwerken

11.4.1 Beleid ten aanzien van het gebruik van netwerkdiensten

Vraag	Antwoord	Suwinorm 2017
11.4.1.a Is er een formele procedure voor het toekennen van toegangsrechten voor het netwerk en netwerkdiensten?	Ja	Niet van toepassing

11.4.2 Authenticatie van gebruikers bij externe verbindingen

Vraag	Antwoord	Suwinorm 2017
11.4.2.a Is er een vastgestelde procedure voor het authenticeren van (externe) gebruikers voor toegang tot het netwerk van buiten?	Ja	Niet van toepassing
Wordt er hierbij gebruik gemaakt van een twee factor authenticatie?	Ja	Niet van toepassing

11.4.6 Beheersmaatregelen voor netwerkverbindingen

Vraag	Antwoord	Suwinorm 2017
11.4.6.a Is de toegang van gebruikers in een gemeenschappelijk netwerk (met andere organisaties) ingericht volgens het geldende toegangsbeleid van de organisatie?	Ja	U.11

11.4.7 Beheersmaatregelen voor netwerkroutering

Vraag	Antwoord	Suwinorm 2017
11.4.7.a Zijn netwerken voorzien van beheersmaatregelen voor netwerkroutering, om te bewerkstelligen dat computerverbindingen en informatiestromen niet in strijd zijn met het toegangsbeleid voor de bedrijfstoeepassingen?	Ja	U.07, B.06

11.6: Toegangsbeheersing voor toepassingen en informatie

11.6.1. Beperking van toegang tot informatie

Vraag	Antwoord	Suwinorm 2017
11.6.1.a Wordt de toegang tot informatie en functies van toepassingssystemen door gebruikers en ondersteunend personeel beperkt?	Ja	U.02, U.03, U.04

11.7 Draagbare computers en telewerken

11.7.1 Draagbare computers en communicatievoorzieningen

Vraag	Antwoord	Suwinorm 2017
11.7.1.a Is er formeel beleid en zijn geschikte beveiligingsmaatregelen getroffen voor de inrichting en gebruik van laptops, tablets en andere mobiele communicatie apparaten?	Ja	Niet van toepassing
Kunt u aangeven welke beveiligingsmaatregelen u heeft getroffen?	<ul style="list-style-type: none"> • Door middel van MDM/WTR • Harddisk encryptie voor laptops 	Niet van toepassing
Gelden deze maatregelen voor de hele gemeente?	Ja	Niet van toepassing
Heeft uw gemeente uitgewerkt welke systemen wel en niet geraadpleegd mogen worden?	Ja	Niet van toepassing

11.7.2 Telewerken

Vraag	Antwoord	Suwinorm 2017
11.7.2.a Is er beleid en zijn er procedures voor het werken met informatiesystemen buiten de reguliere kantooromgeving?	<ul style="list-style-type: none"> • Ja, er is beleid en er zijn procedures 	Niet van toepassing
Heeft de gemeente een telewerkbeleid?	Ja	Niet van toepassing
Heeft de gemeente uitgewerkt welke systemen wel en niet mogen worden geraadpleegd?	Ja	Niet van toepassing
Zijn de telewerkvoorzieningen op basis van zero-footprint ingericht?	Nee	Niet van toepassing

12.1: Beveiligingseisen voor informatiesystemen

12.1.1 Analyse en specificatie van beveiligingseisen

Vraag	Antwoord	Suwinorm 2017
-------	----------	---------------

12.1.1.a Wordt bij het analyseren en specificeren van de eisen voor nieuwe systemen of systeemwijzingen expliciet aandacht besteed aan de eisen voor informatiebeveiliging?	Ja	Niet van toepassing
---	----	---------------------

12.2 Correcte verwerking in toepassingen

12.2.2 Beheersing van interne gegevensverwerking

Vraag	Antwoord	Suwinorm 2017
12.2.2.a Is er beleid of zijn er richtlijnen voor verwerking-, en uitvoervalidaties bij de ontwikkeling van (web-) applicaties?	Nee	Niet van toepassing

12.2.3 Integriteit van berichten

Vraag	Antwoord	Suwinorm 2017
12.2.3.a Zijn er maatregelen geïmplementeerd om verandering van berichten in toepassingen te voorkomen?	Nee	Niet van toepassing

12.2.4 Validatie van uitvoergegevens

Vraag	Antwoord	Suwinorm 2017
12.2.4.a Is er beleid of zijn er richtlijnen voor invoer- en verwerkingvalidaties bij de ontwikkeling van (web-) applicaties?	Nee	Niet van toepassing

12.3 Cryptografische beheersmaatregelen

12.3.1 Beleid voor het gebruik van cryptografische beheersmaatregelen

Vraag	Antwoord	Suwinorm 2017
12.3.1.a Is er een vastgesteld beleid voor het toepassen en beheren van cryptografische middelen?	Ja	U.11

12.3.2 Sleutelbeheer

Vraag	Antwoord	Suwinorm 2017
12.3.2.a Zijn er maatregelen getroffen specifiek voor het beheren van cryptografische sleutels?	Ja	Niet van toepassing

12.4 Beveiliging van systeembestanden

12.4.1 Beheersing van operationele software

Vraag	Antwoord	Suwinorm 2017
12.4.1.a Zijn er maatregelen getroffen voor het beheren en het beheerst wijzigen van (applicatie-) programmatuur?	Ja	Niet van toepassing
12.4.1.b Is er een hardeningsproces voor ICT-componenten?	Ja	Niet van toepassing

12.5 Beveiliging bij ontwikkelings- en ondersteuningsprocessen

12.5.1 Procedures voor wijzigingsbeheer

Vraag	Antwoord	Suwinorm 2017
12.5.1.a Is binnen de gemeente een formeel proces ingericht voor het uitvoeren van wijzigingen?	Ja	Niet van toepassing

12.5.2 Technische beoordeling van toepassingen na wijzigingen in het besturingssysteem

Vraag	Antwoord	Suwinorm 2017
12.5.2.a Voert u zelf testen uit op kritische toepassingen, na wijzigingen in de besturingssystemen?	Ja	Niet van toepassing
Kunt u aangeven waarom er geen testen worden uitgevoerd op de kritische toepassingen, na wijzigingen in de besturingssystemen?	Niet van toepassing	Niet van toepassing
Kunt u aangeven op welk niveau(s) de testen plaatsvinden?	<ul style="list-style-type: none">• <u>Op applicatieniveau (informatiesysteem)</u>• <u>Op gegevensniveau (databasesysteem)</u>	Niet van toepassing

12.5.4 Uitlekken van informatie

Vraag	Antwoord	Suwinorm 2017
12.5.4.a Heeft de gemeente maatregelen getroffen voor het 'scannen' van in en uitgaand netwerkverkeer (content scanning, IDS, IPS)?	Ja	Niet van toepassing
Kunt u aangeven waarom er geen maatregelen zijn getroffen?	Niet van toepassing	Niet van toepassing

12.5.5 Uitbestede ontwikkeling van programmatuur

Vraag	Antwoord	Suwinorm 2017
12.5.5.a Zijn er contracten afgesloten met de IT Leveranciers voor systeemontwikkeling met expliciet aandacht voor informatiebeveiligingseisen, ontwikkelstandaarden en intellectueel eigendom?(zie ook vragen 6.2 en 10.2)	Nee	Niet van toepassing

12.6 Beheer van technische kwetsbaarheden

12.6.1 Beheersing van technische kwetsbaarheden

Vraag	Antwoord	Suwinorm 2017
12.6.1.a Zijn er maatregelen getroffen voor het regelmatig controleren op technische kwetsbaarheden in IT Services en Servers?	Ja	Niet van toepassing
Kunt u aangeven welke maatregelen er zijn getroffen voor het regelmatig controleren op technische kwetsbaarheden in IT Services en Servers?	<ul style="list-style-type: none"> • Vulnerability scans • Pentesten • Patchmanagement 	Niet van toepassing
12.6.1.b Krijgt de gemeente kwetsbaarheidswaarschuwingen van de IBD	Ja	Niet van toepassing
12.6.1.c Zijn de laatste (beveiligings)patches geïnstalleerd en worden deze volgens een patchmanagement proces doorgevoerd?	Ja	Niet van toepassing
12.6.1.d Worden de penetratietests periodiek uitgevoerd?	Ja	Niet van toepassing
12.6.1.e Worden de vulnerability assessments (security scans) periodiek uitgevoerd?	Ja	Niet van toepassing

13.1 Rapportage van informatiebeveiligingsgebeurtenissen en zwakke plekken

13.1.1 Rapportage van informatiebeveiligingsgebeurtenissen

Vraag	Antwoord	Suwinorm 2017
13.1.1.a Is er een incident management procedure?	Ja	Niet van toepassing
Zijn een reactie- en escalatieprocedure en een registratiesysteem onderdeel van de incident management procedure?	ja	Niet van toepassing

13.1.2 Rapportage van zwakke plekken in de beveiliging

Vraag	Antwoord	Suwinorm 2017
13.1.2.a Kent iedereen zijn/haar verantwoordelijkheden met betrekking tot het melden van verdachte zwakke plekken met betrekking tot informatiebeveiliging?	Ja	B.01, B.04
Is er een integriteitsprotocol?	Ja	Niet van toepassing
Is de procedure met betrekking tot het melden van verdachte en zwakke plekken met betrekking tot informatiebeveiliging bij iedereen bekend?	Ja	Niet van toepassing

13.2 Beheer van informatiebeveiligingsincidenten en verbeteringen

13.2.3 Verzamelen van bewijsmateriaal

Vraag	Antwoord	Suwinorm 2017
13.2.3.a Wordt er rekening gehouden met het verzamelen van bewijsmateriaal als er een incident opgetreden is?	Ja	Niet van toepassing

15.1: Naleving van wettelijke voorschriften

15.1.3 Bescherming van bedrijfsdocumenten

Vraag	Antwoord	Suwinorm 2017
15.1.3.a Wordt opslag en archivering van registraties / dossiers volgens vastgesteld beleid uitgevoerd?	Nee	Niet van toepassing

15.1.4 Bescherming van gegevens en geheimhouding van persoonsgegevens

Vraag	Antwoord	Suwinorm 2017
15.1.4.a Wordt de bescherming van gegevens en privacy bewerkstelligd overeenkomstig relevante wetgeving, regelgeving en voorschriften en indien van toepassing contractuele bepalingen?	Ja, middels Privacy functionaris	Niet van toepassing

15.1.6 Voorschriften voor het gebruik van cryptografische beheersmaatregelen

Vraag	Antwoord	Suwinorm 2017
15.1.6.a Worden cryptografische beheersmaatregelen toegepast in overeenstemming met relevante	Ja	Niet van toepassing

wetten en voorschriften? Kunt u aangeven volgens welke wetten en voorschriften de cryptografische beheersmaatregelen worden toegepast?	<ul style="list-style-type: none"> • Volgens de ICT-beveiligingsrichtlijnen voor webapplicaties van het NCSC • Volgens SUWI • Volgens BRP • Conform de pas-toe-of-leg-uit lijst van het forum standaardisatie 	Niet van toepassing
---	---	---------------------

15.2: Naleving van beveiligingsbeleid en -normen en technische naleving

15.2.1 Naleving van beveiligingsbeleid en -normen

Vraag	Antwoord	Suwinorm 2017
15.2.1.a Hoe ziet het verantwoordelijke (lijn) management er op toe dat de IB maatregelen afgeleid van het IB beleid worden uitgevoerd? Dit is Suwi en een BRP en PUN eis.	<ul style="list-style-type: none"> • Door middel van P&C rapportages • Door middel van interne controle • Door middel van self assessments • Door middel van audits 	B.02

15.2.2 Controle op technische naleving

Vraag	Antwoord	Suwinorm 2017
15.2.2.a Zorgen lijnmanagers en proceseigenaren dat de voor hun relevante informatiesystemen jaarlijks onderzocht worden op zwakheden door het laten uitvoeren van penetratietesten en kwetsbaarheidsanalyses?	Nee	Niet van toepassing
Kunt u aangeven voor welke systemen dit wordt gedaan?	Niet van toepassing	Niet van toepassing
15.2.2.b Zijn de relevante afgegeven TPM-verklaringen niet ouder dan 1 jaar?	Ja	Niet van toepassing

BRP & PUN

5.1 Informatiebeveiligingsbeleid

5.1.1: Beleidsdocumenten voor informatiebeveiliging

Vraag	Antwoord	BRP	PUN
5.1.1.a Is er een actueel informatiebeveiligingsbeleid (gebaseerd op de BIG)?	Ja	Wet BRP 1.11, lid 1/Besluit BRP 6	Niet van toepassing
Is het informatiebeveiligingsbeleid vastgesteld door het College?	Ja		
Is het informatiebeveiligingsbeleid jonger dan drie jaar?	Ja		
Is het informatiebeveiligingsbeleid gepubliceerd en kenbaar gemaakt aan alle medewerkers en externe partijen?	Ja		
5.1.1.b Is er in het gemeentelijk informatiebeveiligingsbeleid expliciet aandacht voor speciale gemeentelijke voorzieningen en wetgeving?	Ja	Wet BRP 1.11, lid 1/Besluit BRP 6	Niet van toepassing
Kunt u aangeven voor welke voorzieningen en wetgeving er expliciet aandacht is in het informatiebeveiligingsbeleid?	<ul style="list-style-type: none"> • Voor de BRP • Voor de PUN • Voor Suwinet 		
5.1.1.c Heeft u het gemeentelijke informatiebeveiligingsbeleid vertaald naar te nemen maatregelen of te implementeren maatregelen naar de door u opgerichte samenwerkingsverbanden of die waarin uw gemeente een deelname heeft?	N.v.t.	Wet BRP 1.11, lid 1/Besluit BRP 6	Niet van toepassing

6.1 Interne organisatie

6.1.1: Betrokkenheid van het College van B&W bij beveiliging

Vraag	Antwoord	BRP	PUN
6.1.1.a Worden de informatiebeveiligingsdoelstellingen vastgesteld door het College?	Ja	Besluit BRP 6, LO 7.2, 7.4.7, 4.2.4, 3.1	Niet van toepassing
Wordt de voortgang jaarlijks besproken tussen bestuur en management?	Ja		
Wordt er over de voortgang gerapporteerd?	Ja		

6.1.5.a Is er een beleid om de geheimhoudingsverklaring te laten tekenen bij een aanstelling?	Ja	WBP 12, lid 2	WBP 12, lid 2
Kunt u aangeven op welke wijze dit gebeurt?	<ul style="list-style-type: none"> • Iedere ambtelijk medewerker ondertekent een individuele verklaring integriteit / tot geheimhouding of legt de ambtseed of ambtsbelofte af • Externe en tijdelijke medewerkers ondertekenen een geheimhoudingsverklaring • Bij de aanstelling wordt een VOG gevraagd 		
6.1.8.a Wordt het informatiebeveiligingsbeleid onafhankelijk beoordeeld en wordt hierover intern verantwoording afgelegd?	Ja	Wet BRP 4.3, lid 1	Niet van toepassing

6.2 Externe partijen

6.2.1: Identificatie van risico's die betrekking hebben op externe partijen

Vraag	Antwoord	BRP	PUN
6.2.1.a Worden externe partijen (inclusief samenwerkingsverbanden) gebruikt om ICT-voorzieningen in stand te houden dan wel te beheren of worden externe partijen gebruikt voor de invulling van bedrijfsprocessen?	Externe partijen worden zowel voor het in standhouden/beheren van ICT-voorzieningen als voor de invulling van bedrijfsprocessen gebruikt	Wet BRP 1.10, lid 2	Niet van toepassing
6.2.1.g Worden de aan de leverancier opgelegde informatiebeveiligingsmaatregelen jaarlijks gecontroleerd?	Ja, en we ontvangen een TPM/SAE/SAS	Besluit BRP 8, 9	Niet van toepassing

7.1 Beheer van bedrijfsmiddelen

7.1.2 Eigendom van bedrijfsmiddelen

Vraag	Antwoord	BRP	PUN
7.1.2.a Is er voor elk bedrijfsproces, applicatie, gegevensverzameling en	Ja	WBP 8	Niet van toepassing

ICT-faciliteit een verantwoordelijke lijnmanager?			
Is de verantwoordelijke lijnmanager formeel vastgesteld?	Ja		

7.1.3 Aanvaardbaar gebruik van bedrijfsmiddelen

Vraag	Antwoord	BRP	PUN
7.1.3.a Zijn er regels opgesteld voor het juist gebruiken van (ICT-)bedrijfsmiddelen?	Ja	Niet van toepassing	PUN 93

8.1 Voorafgaand aan het dienstverband

8.1.1. Rollen en verantwoordelijkheden

Vraag	Antwoord	BRP	PUN
8.1.1.a Zijn de rollen en verantwoordelijkheden van werknemers, ingehuurd personeel en externe gebruikers met betrekking tot informatiebeveiliging vastgelegd?	Ja	Besluit BRP 6	Niet van toepassing
Kunt u aangeven met betrekking tot welke van de hiernaast genoemde opties dit wordt vastgelegd en gecommuniceerd?	<ul style="list-style-type: none"> • m.b.t. het beveiligingsbeleid ▪ m.b.t. de bescherming van bedrijfsmiddelen ▪ m.b.t. speciale verantwoordelijkheden (in geval van een BRP, BUN, SUWI rol/functie) ▪ m.b.t. de rapportage van beveiligingsincidenten 		

8.2 Tijdens het dienstverband

8.2.1 Directieverantwoordelijkheid

Vraag	Antwoord	BRP	PUN
8.2.1.a Bevordert en controleert het lijnmanagement dat gemeenteambtenaren, ingehuurd personeel en externe gebruikers	Ja	Besluit BRP 6	Niet van toepassing

zich houden aan de beveiligingsregels overeenkomstig het beleid en de procedures van de organisatie?			
Waaruit blijkt dat?	<ul style="list-style-type: none"> • uit verslagen van (werk)besprekingen 		

8.2.2 Bewustwording, opleiding en training ten aanzien van informatiebeveiliging

Vraag	Antwoord	BRP	PUN
8.2.2.a Zorgt het management ervoor dat de medewerkers voldoende kennis en bewustzijn hebben op het gebied van informatiebeveiliging?	Ja	Besluit BRP 6	Niet van toepassing
Hoe zorgt het management hier voor?	<ul style="list-style-type: none"> • met bewustwordingscampagnes 		
Zijn hier verslagen van?	Ja		
Zijn er voldoende middelen gealloceerd voor het bevorderen van kennis en bewustwording van de medewerkers ten aanzien van informatieveiligheid?	Ja		

8.2.3 Disciplinaire maatregelen

Vraag	Antwoord	BRP	PUN
8.2.3.a Is er een disciplinair proces vastgelegd, conform CAR/UWO, voor werknemers die inbreuk maken op het informatiebeveiligingsbeleid?	Ja	Besluit BRP 6	Niet van toepassing

9.1 Beveiligde ruimten

9.1.1. Fysieke beveiliging van de omgeving

Vraag	Antwoord	BRP	PUN
9.1.1.a Zijn er gepaste toegangsbeveiligingsmaatregelen genomen voor ruimtes waar zich informatie en ICT-voorzieningen bevinden?	Ja	Besluit BRP 6	PUN 91
Kunt u aangeven voor welke ruimtes er			

gepaste toegangsbeveiligingsmaatregelen zijn genomen?	<ul style="list-style-type: none"> • Voor wat betreft de werkruimten ▪ Voor de server- en SER-ruimten ▪ Voor wat betreft de reisdocumenten • Voor wat betreft de ruimten waar persoonsgegevens verwerkt worden 		
Wordt hier mee voldaan aan artikel 91 van de PUN?	Ja		

9.1.2 Fysieke toegangsbeveiliging

Vraag	Antwoord	BRP	PUN
9.1.2. a Is de toegang tot de gebouwen en de beveiligde zones uitsluitend mogelijk voor geautoriseerde personen?	Ja	Besluit BRP 6	Niet van toepassing

9.1.3. Beveiliging van kantoren, ruimten en faciliteiten

Vraag	Antwoord	BRP	PUN
9.1.3.a Zijn er (binnen de kantoren / ruimtes) maatregelen getroffen voor de bescherming van mobiele gegevens- en andere informatie (dragers). Denk hierbij ook aan lockers en kluizen.	Ja	Besluit BRP 6	PUN 91
Kunt u aangeven welke (beschermings) maatregelen er zijn getroffen?	<ul style="list-style-type: none"> • Voor de opslag van gegevensdragers ▪ Er is een actief sleutelplan voor kluizen en sloten ▪ Het is bekend waar incidenten gemeld kunnen worden 		

9.1.5 Werken in beveiligde ruimten

Vraag	Antwoord	BRP	PUN
9.1.5.a Zijn er maatregelen en procedures geïmplementeerd voor het werken in en toezien op beveiligde ruimtes?	Ja	Besluit BRP 6	PUN 91
Kunt u aangeven waarvoor de maatregelen en procedures zijn	<ul style="list-style-type: none"> • Voor bezoekers 		

geïmplementeerd?	<ul style="list-style-type: none"> • Voor ongeautoriseerd personeel • Voor geautoriseerd personeel • Voor het maken van foto's en video's 		
------------------	--	--	--

9.1.6 Openbare toegang en gebieden voor laden en lossen

Vraag	Antwoord	BRP	PUN
9.1.6.a Zijn publiek toegankelijke ruimtes afgeschermd zodat onbevoegden zich geen toegang kunnen verschaffen tot bedrijfsmiddelen?	Ja	Besluit BRP 6	PUN 91

9.2 Beveiliging van apparatuur

9.2.5 Beveiliging van apparatuur buiten het terrein

Vraag	Antwoord	BRP	PUN
9.2.5.a Zijn er maatregelen en procedures geïmplementeerd voor apparatuur als er buiten de vertrouwde omgeving gewerkt wordt?	Ja, met maatregelen en procedures	Niet van toepassing	PUN 80, 80a, 90, 91

10.1 Bedieningsprocedures en -verantwoordelijkheden

10.1.1 Gedocumenteerde bedieningsprocedures

Vraag	Antwoord	BRP	PUN
10.1.1.a Zijn er actuele schriftelijke procedures voor het operationeel beheer (en gebruik) van de IT voorzieningen (software, hardware, netwerk, databases)?	Ja	Besluit BRP 6, LO 7.4.1	Niet van toepassing

10.1.3 Functiescheiding

Vraag	Antwoord	BRP	PUN
10.1.3.a Zijn de taken en verantwoordelijkheden voor het gebruik en het beheer van IT	Ja	Besluit BRP 6, LO 7.4.1	Niet van toepassing

voorzieningen naar rato van de organisatiegrootte gescheiden? Kunt u aangeven hoe de taken en verantwoordelijkheden voor het gebruik en het beheer van IT voorzieningen zijn gescheiden?	<ul style="list-style-type: none"> • Dit hebben we gedaan voor de functies van BRP, PUN en SUWI • De rol van CISO of controller informatiebeveiliging is apart, onafhankelijk belegd 		
10.1.3.b Welke rollen en functiebenamingen zijn er belegd, dan wel aangewezen door het college?	<ul style="list-style-type: none"> • Systeembeheerder • Applicatiebeheerder BRP • Gegevensbeheerder BRP • Privacybeheerder BRP • Security Officer SUWI • Toezichthouder BRP 	Besluit BRP 6, LO 7.4.1	Niet van toepassing
10.1.3.c Is er sprake van een scheiding in verantwoordelijkheden tussen: uitvoerder en de beveiligingsfunctionaris en tussen opdrachtgever en de beveiligingsfunctionaris?	<ul style="list-style-type: none"> • Ja, tussen de uitvoerder en de beveiligingsfunctionaris • Ja, tussen de opdrachtgever en de beveiligingsfunctionaris 	Besluit BRP 6, LO 7.4.1	PUN 93

10.2 Exploitatie door een derde partij

10.2.1 Dienstverlening

Vraag	Antwoord	BRP	PUN
10.2.1.a Zijn voor de uitbestede IT diensten, naast de afgesproken dienstenniveaus, ook alle relevante beveiligingseisen opgenomen in de contracten met de IT leveranciers en/of bewerkers? Kunt u aangeven waar deze beveiligingseisen op zijn gericht?	Ja <ul style="list-style-type: none"> • Maatregelen gericht op medewerkers • Maatregelen gericht op de toegang tot gebouwen en ruimten • Maatregelen gericht op een deugdelijke werking van de apparatuur en programmatuur 	Besluit BRP 8,9	Niet van toepassing

	<ul style="list-style-type: none"> • Maatregelen gericht op de beveiliging van de apparatuur en programmatuur ▪ Maatregelen gericht op het gegevensbeheer ▪ Maatregelen ingeval van schending van de geheimhouding ▪ Maatregelen ingeval van calamiteiten ▪ Gebruik van gegevens uitsluitend voor de afgesproken werkzaamheden ▪ De bewerker houdt zich aan de wettelijke voorschriften ▪ De bewerker staat toe dat de gemeente controles uitvoert ▪ Werkzaamheden worden opgeschort op vordering van de gemeente ▪ Werkzaamheden worden zonder toestemming van de gemeente door de bewerker niet uitbesteed 		
--	---	--	--

10.2.2 Controle en beoordeling van dienstverlening door een derde partij

Vraag	Antwoord	BRP	PUN
10.2.2.a Hoe is in het afgelopen jaar getoetst dat de IT-leveranciers en/of bewerkers zich houden aan de afgesproken diensten niveaus en informatiebeveiligingseisen?	<ul style="list-style-type: none"> • Er is intern door de gemeente zelf een controle uitgevoerd ▪ De IT-leverancier heeft een toets uit laten voeren 	Besluit BRP 8,9	Niet van toepassing

10.5 Back-up

10.5.1 Reservekopieën maken (back-ups)

Vraag	Antwoord	BRP	PUN
10.5.1.a Heeft u een actueel back-up beleid en worden back-ups dienovereenkomstig gemaakt, getest en opgeslagen?	Ja	Besluit BRP 6	PUN 92
Kunt u aangeven waarvoor u een actueel back-beleid heeft en waarvoor de back-ups worden gemaakt, getest en opgeslagen?	<ul style="list-style-type: none"> Deze is generiek ingericht voor alle data en informatie 		

10.6 Beheer van netwerkbeveiliging

10.6.1 Maatregelen voor netwerken

Vraag	Antwoord	BRP	PUN
10.6.1.a Welke maatregelen heeft u genomen om de aanwezige netwerken adequaat te monitoren en beveiligen?	<ul style="list-style-type: none"> Wij hebben dit uitbesteed bij een andere gemeente/leverancier Wij hebben op alle vertrouwde koppelvlakken een beheerde firewall Wij maken generiek gebruik van een IDS Wij doen aan content scanning De gegevensuitwisseling tussen vertrouwde en onvertrouwde zones worden inhoudelijk geautomatiseerd en gecontroleerd op de aanwezigheid van malware Er zijn procedures voor beheer van apparatuur op afstand 	Niet van toepassing	Circulaire BPR/U59776

10.7 Behandeling van media

10.7.1 Beheer van verwijderbare media

Vraag	Antwoord	BRP	PUN
-------	----------	-----	-----

10.7.1.a Zijn er procedures en maatregelen voor het beheer en de beveiliging van informatie op papier en op (verwijderbare) elektronische gegevensdragers zoals laptops, usb-sticks, externe disks en backup tapes?	Ja	Niet van toepassing	PUN 91
Voldoet u hiermee aan artikel 91 van de PUN?	Ja		

10.10 Controle

10.10.1 Aanmaken audit-logbestanden

Vraag	Antwoord	BRP	PUN
10.10.1.a Worden systeemhandelingen gelogd, zodanig dat handelingen van gebruikers en beheerders kunnen worden geanalyseerd onder meer t.b.v. een audittrail?	Ja	Besluit BRP 6, LO 4.2	Niet van toepassing
Kunt u aangeven voor welke systemen er wordt gelogd?	<ul style="list-style-type: none"> Ja, voor wat betreft Suwinet, inlezen en DKD-inlezen Ja, voor wat betreft BRP Ja, voor overige systemen 		
Worden administratieve handelingen gelogd?	Ja		
Worden de login-gegevens minimaal 3 maanden bewaard?	Ja		

10.10.2 Controle systeemgebruik

Vraag	Antwoord	BRP	PUN
10.10.2.a Is er een procedure voor het structureel controleren van de logbestanden op het netwerk- systeemgebruik?	Ja	Besluit BRP 6, LO 4.2	Niet van toepassing
Kunt u aangeven of er een procedure is om de handelingen van gebruikers te controleren?	<ul style="list-style-type: none"> Voor wat betreft SUWI Voor wat betreft BRP Voor wat betreft DigiD 		

11.1 Toegangsbeleid

11.1.1 Toegangsbeveiliging

Vraag	Antwoord	BRP	PUN
11.1.1.a Is er beleid vastgesteld dat richting geeft aan de beheerste logische toegang tot gegevens en informatie?	Ja	Besluit BRP 6	PUN 90

11.2 Beheer van toegangsrechten van gebruikers

11.2.1 Registratie van gebruikers

Vraag	Antwoord	BRP	PUN
11.2.1.a Is er een vastgestelde autorisatieprocedure voor het administreren van gebruikers en het toekennen / intrekken van toegangsrechten voor alle informatie en –systemen en de controle daarop?	Ja	Besluit BRP 6	PUN 90
Is deze procedure belegd bij de betrokken systeem/proces eigenaar?	Ja		

11.2.2 Beheer van speciale bevoegdheden

Vraag	Antwoord	BRP	PUN
11.2.2.a Wordt de toewijzing en het gebruik van speciale bevoegdheden beperkt en beheerst?	Ja	Besluit BRP 6	Niet van toepassing
Is dit herleidbaar aan een (beheer) principe of doelstelling?	Ja		

11.2.4 Beoordeling van toegangsrechten van gebruikers

Vraag	Antwoord	BRP	PUN
11.2.4.a Worden de toegangsrechten van gebruikers regelmatig beoordeeld in een formeel proces?	Ja	Besluit BRP 6	Niet van toepassing
Zijn er verslagen van de beoordeling van de toegangsrechten?	Ja		

11.3 Verantwoordelijkheden van gebruikers

11.3.1 Gebruik van wachtwoorden

Vraag	Antwoord	BRP	PUN
11.3.1.a Worden alle medewerkers regelmatig geïnformeerd over de regels voor het juist en veilig gebruik van wachtwoorden?	Ja	Besluit BRP 6	Niet van toepassing
11.3.1.b Welke voorwaarden zijn aan de wachtwoorden gesteld? Geef aan wat voor uw organisatie van toepassing is.	<ul style="list-style-type: none"> • Wachtwoorden bestaan uit minimaal 8 karakters, waarvan tenminste 1 hoofdletter, 1 cijfer en 1 vreemd teken • Wachtwoorden zijn maximaal 60 dagen geldig en mogen niet binnen 6 keer herhaald worden • Tijdelijke of standaard wachtwoorden worden bij het eerste gebruik vervangen • Het wachtwoord is alleen bij de gebruiker bekend 	Besluit BRP 6	Niet van toepassing

11.3.3 'Clear desk'- en 'clear screen'-beleid

Vraag	Antwoord	BRP	PUN
11.3.3.a Is er een clear desk-beleid voor papier, usb-sticks, externe schijven en mobiele devices en een clear screen-beleid voor ICT-voorzieningen?	Ja	Besluit BRP 6	Niet van toepassing

11.4 Toegangsbeheersing voor netwerken

11.4.1 Beleid ten aanzien van het gebruik van netwerkdiensten

Vraag	Antwoord	BRP	PUN
11.4.1.a Is er een formele procedure voor het toekennen van toegangsrechten voor het netwerk en netwerkdiensten?	Ja	Besluit BRP 6	PUN 91

11.4.4 Bescherming op afstand van poorten voor diagnose en configuratie

Vraag	Antwoord	BRP	PUN
11.4.4.a Is er een procedure voor de	Ja	Besluit BRP 6	Niet van toepassing

beheerste toegang tot netwerkpoorten (bv firewalls) en netwerkcomponenten (bv switches) voor beheeractiviteiten (bv diagnose, configureren)?			
--	--	--	--

11.6 Toegangsbeheersing voor toepassingen en informatie

11.6.2 Isolatie van gevoelige systemen

Vraag	Antwoord	BRP	PUN
11.6.2.a Zijn systemen met risicovolle informatie in een eigen omgeving (netwerksegment) ondergebracht dat 'logisch of fysiek gescheiden' is van de rest van het netwerk? Kunt u aangeven voor welke systemen?	Ja <ul style="list-style-type: none"> Voor verkeer uit de DMZ Voor beheer (actieve) netwerkcomponenten 	Niet van toepassing	Circulaire BPR/U59776

11.7 Draagbare computers en telewerken

11.7.2 Telewerken

Vraag	Antwoord	BRP	PUN
11.7.2.a Is er beleid en zijn er procedures voor het werken met informatiesystemen buiten de reguliere kantooromgeving?	<ul style="list-style-type: none"> Ja, er is beleid en er zijn procedures 	Besluit BRP 6	Niet van toepassing
Heeft de gemeente een telewerkbeleid?	Ja		
Heeft de gemeente uitgewerkt welke systemen wel en niet mogen worden geraadpleegd?	Ja		

12.1 Beveiligingseisen voor informatiesystemen

12.1.1 Analyse en specificatie van beveiligingseisen

Vraag	Antwoord	BRP	PUN
12.1.1.a Wordt bij het analyseren en specificeren van de eisen voor	Ja	Besluit BRP 6	Niet van toepassing

nieuwe systemen of systeemwijzingen expliciet aandacht besteed aan de eisen voor informatiebeveiliging?			
---	--	--	--

14.1 Informatiebeveiligingsaspecten van bedrijfscontinuïteitsbeheer

14.1.3 Continuïteitsplannen ontwikkelen en implementeren waaronder informatiebeveiliging

Vraag	Antwoord	BRP	PUN
14.1.3.a Is er een vastgesteld Continuïteitsplan (voor het handhaven van de beschikbaarheid van systemen, dan wel het binnen de afgesproken tijd weer opbrengen van IT systemen in het geval van ernstige verstoringen)? Kunt u aangeven voor welke systemen en processen u een vastgesteld Continuïteitsplan heeft?	Ja <ul style="list-style-type: none">Voor wat betreft BRPVoor wat betreft de dienstverlening van de BRPVoor wat betreft BAG	LO 7.4	Niet van toepassing
14.1.3.b Wordt er voor BRP rekening gehouden met de tijd tussen de laatste back-up en een mogelijk herstel?	Ja	LO 7.4	Niet van toepassing
14.1.3.c Is het voor de BRP specifiek mogelijk dat er een volledige reconstructie mogelijk is binnen 24 uur?	Ja	LO 7.4	Niet van toepassing

14.1.5 Testen, onderhoud en herbeoordelen van continuïteitsplannen

Vraag	Antwoord	BRP	PUN
14.1.5.a Worden continuïteitsplannen jaarlijks getest of ze actueel en doeltreffend blijven?	Ja	LO 7.4	Niet van toepassing
Kunt u aangeven voor welke systemen de continuïteitsplannen worden getest?	<ul style="list-style-type: none">Alleen voor BRP		

15.1 Naleving van wettelijke voorschriften

15.1.1 Identificatie van toepasselijke wetgeving

Vraag	Antwoord	BRP	PUN
15.1.1.a Heeft de gemeente voor de inrichting en uitvoering van processen / informatiesystemen geregeld dat wordt voldaan aan alle voor IB relevante wet- en regelgeving en contractuele afspraken?	Ja	Besluit BRP 6	PUN 91
Kunt u aangeven aan welke IB relevante wet- en regelgeving wordt voldaan en waarvoor er contractuele afspraken zijn gemaakt?	<ul style="list-style-type: none"> • WBP • PUN • SUWI • BRP • BAG • BGT • DigiD • Beveiligingsrichtlijnen voor web applicaties • WABB • BIG 		

15.2 Naleving van beveiligingsbeleid en- normen en technische naleving

15.2.1 Naleving van beveiligingsbeleid en -normen

Vraag	Antwoord	BRP	PUN
15.2.1.a Hoe ziet het verantwoordelijke (lijn) management er op toe dat de IB maatregelen afgeleid van het IB beleid worden uitgevoerd? Dit is Suwi en een BRP en PUN eis.	<ul style="list-style-type: none"> • Door middel van P&C rapportages • Door middel van interne controle • Door middel van self assessments • Door middel van audits 	Besluit BRP 6	PUN 91

BAG & BGT

10.5 Back-up

Vraag	Antwoord	BRP	PUN
10.5.1.a Heeft u een actueel back-up beleid en worden back-ups dienovereenkomstig gemaakt, getest en opgeslagen?	Ja	5.4.2	Niet van toepassing
Kunt u aangeven waarvoor u een actueel back-beleid heeft en waarvoor de back-ups worden gemaakt, getest en opgeslagen?	<ul style="list-style-type: none"> Deze is generiek ingericht voor alle data en informatie 		

14.1 Informatiebeveiligingsaspecten van bedrijfscontinuïteitsbeheer

Vraag	Antwoord	BAG	BGT
14.1.3.a Is er een vastgesteld Continuïteitsplan (voor het handhaven van de beschikbaarheid van systemen, dan wel het binnen de afgesproken tijd weer opbrengen van IT systemen in het geval van ernstige verstoringen)?	Ja	5.4.2	Niet van toepassing
Kunt u aangeven voor welke systemen en processen u een vastgesteld Continuïteitsplan heeft?	<ul style="list-style-type: none"> Voor wat betreft BRP Voor wat betreft de dienstverlening van de BRP Voor wat betreft BAG 		

BIG hoofdstuk 3: Implementatie van de Tactische Baseline

3.1 ISMS beleid (met basis IBP)

Vraag	Antwoord	Advies	Evaluatie en impact
3.1.a Is er een integraal implementatieplan?	Ja		
Wordt er periodiek gerapporteerd over de voortgang?	Ja		
3.1.b Is er een Information Security Management System – (ISMS) waar het plan een onderdeel van is?	Ja		

hoofdstuk 4 Samenwerkingsverbanden

4.1 Risicobeoordeling en risicoafweging

Vraag	Antwoord	Advies	Evaluatie en impact
4.1.a Is er met alle samenwerkingsverbanden gemeenschappelijke norm afgesproken zoals de BIG die op gemeenten van toepassing is?	Geen samenwerkingsverbanden		
4.1.b Zijn er met deze samenwerkingsverbanden afspraken gemaakt over de jaarlijkse verantwoording over informatieveiligheid?	Niet van toepassing		
4.1.c Heeft u de ter zake relevante normen die binnen de samenwerking gelden gecontroleerd en daar waar nodig deze gebruikt om vragen te beantwoorden binnen ENSIA?	Niet van toepassing		
4.1.d Is er ook een vorm van rapportage afgesproken met de samenwerkingsverbanden over de mate waarin zij in control zijn op informatieveiligheid?	Niet van toepassing		

BIG hoofdstuk 5: Beveiligingsbeleid

5.1 Informatiebeveiligingsbeleid

5.1.1 Beleidsdocumenten voor informatiebeveiliging

Vraag	Antwoord	Advies	Evaluatie en impact
5.1.1.a Is er een actueel informatiebeveiligingsbeleid (gebaseerd op de BIG)?	Ja		
Is het informatiebeveiligingsbeleid vastgesteld door het College?	Ja		
Is het informatiebeveiligingsbeleid jonger dan drie jaar?	Ja		
Is het informatiebeveiligingsbeleid gepubliceerd en kenbaar gemaakt aan alle medewerkers en externe partijen?	Ja		
5.1.1.b Is er in het gemeentelijk informatiebeveiligingsbeleid expliciet aandacht voor speciale gemeentelijke voorzieningen en wetgeving?	Ja		
Kunt u aangeven voor welke voorzieningen en wetgeving er expliciet aandacht is in het informatiebeveiligingsbeleid?	<ul style="list-style-type: none">• Voor de BRP• Voor de PUN• Voor Suwinet		
5.1.1.c Heeft u het gemeentelijke informatiebeveiligingsbeleid vertaald naar te nemen maatregelen of te implementeren maatregelen naar de door u opgerichte samenwerkingsverbanden of die waarin uw gemeente een deelname heeft?	N.v.t.		

5.1.2 Beoordeling van het informatiebeveiligingsbeleid

Vraag	Antwoord	Advies	Evaluatie en impact
5.1.2.a Wordt het informatiebeveiligingsbeleid minimaal één keer per drie jaar of bij grote wijzigingen binnen de organisatie opnieuw beoordeeld en indien nodig aangepast?	Ja		

BIG hoofdstuk 6: Organisatie van de informatiebeveiliging

6.1 Interne organisatie

6.1.1: Betrokkenheid van het College van B&W bij beveiliging

Vraag	Antwoord	Advies	Evaluatie en impact
6.1.1.a Worden de informatiebeveiligingsdoelstellingen vastgesteld door het College?	Ja		
Wordt de voortgang jaarlijks besproken tussen bestuur en management?	Ja		
Wordt er over de voortgang gerapporteerd?	Ja		

6.1.2: Coördineren van beveiliging

Vraag	Antwoord	Advies	Evaluatie en impact
6.1.2. a Zijn de informatiebeveiligingsactiviteiten vastgesteld en belegd?	Ja		
Door welke vertegenwoordigers / rollen worden de informatiebeveiligingsactiviteiten (op alle niveaus) uitgevoerd binnen de organisatie?	<ul style="list-style-type: none">• CISO• Er zijn op afdelingsniveau en binnen samenwerkingsverbanden IB-contactpersonen		
Kunt u aangeven op welke wijze er intern verantwoording wordt afgelegd over de informatiebeveiligingsactiviteiten?	Er vindt niet iedere drie jaar verantwoording plaats en/of er is geen onafhankelijke toets		

6.1.3: Verantwoordelijkheden

Vraag	Antwoord	Advies	Evaluatie en impact
6.1.3 a Zijn de beveiligingsrollen voor wat betreft informatiebeveiliging van de (lijn, proces, systeem) manager belegd?	<ul style="list-style-type: none">• Ja, in de functiebeschrijvingen• Ja, in de taakopdrachten• Ja, voor de basisregistraties		

6.1.4: Goedkeuringsproces voor ICT-voorzieningen

Vraag	Antwoord	Advies	Evaluatie en impact
-------	----------	--------	---------------------

impact			
6.1.4.a Is er geïmplementeerd beleid voor het goedkeuren van nieuwe ICT-voorzieningen?	Ja		
Is er aandacht voor beveiliging binnen dit proces?	Ja		

6.1.5: Geheimhoudingsovereenkomst

Vraag	Antwoord	Advies	Evaluatie en impact
6.1.5.a Is er een beleid om de geheimhoudingsverklaring te laten tekenen bij een aanstelling?	Ja		
Kunt u aangeven op welke wijze dit gebeurt?	<ul style="list-style-type: none"> • Iedere ambtelijk medewerker ondertekent een individuele verklaring integriteit / tot geheimhouding of legt de ambtseed of ambtsbelofte af • Externe en tijdelijke medewerkers ondertekenen een geheimhoudingsverklaring • Bij de aanstelling wordt een VOG gevraagd 		

6.1.6: Contact met overheidsinstanties

Vraag	Antwoord	Advies	Evaluatie en impact
6.1.6 a Worden er contacten onderhouden in relatie tot informatiebeveiliging met relevante (overheids) organisaties en is dit vastgelegd?	Ja		
Kunt u aangeven met welke instanties er contacten worden onderhouden?	<ul style="list-style-type: none"> • Met de politie • Met de Suwidesk • Met de RVIG desk 		

6.1.7: Contact met speciale belangengroepen

Vraag	Antwoord	Advies	Evaluatie en
-------	----------	--------	--------------

impact			
6.1.7.a Onderhoud de gemeente contacten met relevante expertise groepen en leveranciers om in geval van incidenten snel/juist te kunnen handelen?	Ja		
Kunt u aangeven met welke expertisegroepen uw gemeenten contacten onderhoudt?	<ul style="list-style-type: none"> • IBD • BKWI 		

6.1.8: Beoordeling van het informatiebeveiligingsbeleid

Vraag	Antwoord	Advies	Evaluatie en impact
6.1.8.a Wordt het informatiebeveiligingsbeleid onafhankelijk beoordeeld en wordt hierover intern verantwoording afgelegd?	Ja		
6.1.8.b Wordt over het functioneren van informatiebeveiliging verantwoording afgelegd aan de gemeenteraad?	Ja, minimaal 1 keer per jaar		
6.1.8.c Heeft u een sluitende IB-verantwoording ingericht binnen uw gemeente?	Ja		
Vraagt u jaarlijks van uw directeuren / afdelingshoofden / samenwerkingsverbanden om een in control verklaring over de op hun van toepassing zijnde maatregelen?	Nee		<p>1. Betreft de vraag wetgeving? Indien ja, dan moet ik het implementeren.</p> <p>2. Wat is het risico wanneer ik dit niet implementeer (kans x impact)?</p> <p>3. Wat kost het ons als het risico manifest wordt?</p> <p>4. Wat kost het om te implementeren?</p> <p>Dient deze control geïmplementeerd te worden en met welke prioriteit?</p>

6.2 Externe Partijen

6.2.1: Identificatie van risico's die betrekking hebben op externe partijen

Vraag	Antwoord	Advies	Evaluatie en impact
6.2.1.a Worden externe partijen	Externe partijen		

(inclusief samenwerkingsverbanden) gebruikt om ICT-voorzieningen in stand te houden dan wel te beheren of worden externe partijen gebruikt voor de invulling van bedrijfsprocessen?	worden zowel voor het in standhouden/beheren van ICT-voorzieningen als voor de invulling van bedrijfsprocessen gebruikt		
6.2.1.b Is er voor uitbesteding van een proces of systeem een risicoafweging gemaakt en zijn de relevante beveiligingsrisico's in kaart gebracht?	Ja		
6.2.1.c Als er uitbesteed is, zijn er dan beveiligingsmaatregelen vastgelegd in de (inkoop) contracten?	Ja		
6.2.1.d Als er uitbesteed is en er zijn persoonsgegevens betrokken, is er dan met de leverancier een bewerkersovereenkomst conform het model van de BIG-OP afgesloten?	Nee	Als er persoonsgegevens uitbesteed worden dan is een bewerkersovereenkomst een must. U kunt het voorbeeld van de IBD te gebruiken als basis voor de onderhandeling met de leverancier.	1. Betreft de vraag wetgeving? Indien ja, dan moet ik het implementeren.2. Wat is het risico wanneer ik dit niet implementeer (kans x impact)?3. Wat kost het ons als het risico manifest wordt?4. Wat kost het om te implementeren?Dient deze control geïmplementeerd te worden en met welke prioriteit?
Kunt u aangeven op welke wijze de afspraken zijn gemaakt?	<ul style="list-style-type: none"> Op basis van de BIG en in overleg met de leverancier 		
6.2.1.e Als er persoonsgegevens verwerkt worden, is er dan een wettelijke grondslag en is doelbinding en proportionaliteit gewaarborgd?	Niet van toepassing		
6.2.1.f Is in deze contracten opgenomen dat een leverancier verplicht is om binnen 24 uur alle beveiligingsinbreuken te melden? (WBP-eis).	Niet van toepassing		
6.2.1.g Worden de aan de leverancier opgelegde informatiebeveiligingsmaatregelen	Ja, en we ontvangen een TPM/SAE/SAS		

n jaarlijks gecontroleerd?			
6.2.1.h Worden de rapportages over leveranciers verwerkt in de Collegeverklaring?	Ja		

6.2.2: Beveiliging beoordelen in de omgang met klanten

Vraag	Antwoord	Advies	Evaluatie en impact
6.2.2.a Wordt aan externe medewerkers pas toegang verleend tot informatie en of bedrijfsmiddelen nadat alle beveiligingseisen geïmplementeerd zijn?	Ja		
6.2.2.b Is dat ook vastgesteld en vastgelegd en uitgewerkt in de contracten?	Nee	In contracten met externe partijen dient te worden vastgelegd welke beveiligingsmaatregelen vereist zijn.	<p>1. Betreft de vraag wetgeving? Indien ja, dan moet ik het implementeren.</p> <p>2. Wat is het risico wanneer ik dit niet implementeer (kans x impact)?</p> <p>3. Wat kost het ons als het risico manifest wordt?</p> <p>4. Wat kost het om te implementeren?</p> <p>Dient deze control geïmplementeerd te worden en met welke prioriteit?</p>

6.2.3: Beveiliging behandelen in overeenkomsten met een derde partij

Vraag	Antwoord	Advies	Evaluatie en impact
6.2.3.a Zijn alle ontdekte beveiligingsmaatregelen uit de risicoafweging vastgelegd en geïmplementeerd voordat het product of de dienst in werking gezet wordt?	Nee	Bij afspraken met externe partijen moeten een aantal onderwerpen uitgewerkt worden; als u beveiligingseisen, aansprakelijkheid en dergelijke niet van tevoren uitwerkt, loopt u een bestuurlijk risico.	<p>1. Betreft de vraag wetgeving? Indien ja, dan moet ik het implementeren.</p> <p>2. Wat is het risico wanneer ik dit niet implementeer (kans x impact)?</p> <p>3. Wat kost het ons als het risico manifest wordt?</p> <p>4. Wat kost het om te implementeren?</p> <p>Dient deze control geïmplementeerd te worden en met welke prioriteit?</p>

Welke van de volgende onderwerpen zijn vastgelegd en geregeld in formele contracten bij de uitbesteding dan wel ontwikkeling van software?	Niet van toepassing		
6.2.3.b Is in contracten vastgelegd hoe wordt omgegaan met wijzigingsbeheer?	Ja		
6.2.3.c Is in contracten met externe leveranciers de aansprakelijkheid uitgewerkt?	Ja		
6.2.3.d Worden leverancierseisen doorvertaald naar onderaannemers?	Ja		
6.2.3.e Is in contracten vastgelegd hoe er wordt omgegaan met geheimhouding?	Ja		

BIG hoofdstuk 7: Beheer van bedrijfsmiddelen

7.1 Beheer van bedrijfsmiddelen

7.1.1 Inventarisatie van bedrijfsmiddelen

Vraag	Antwoord	Advies	Evaluatie en impact
7.1.1.a Is er een actuele registratie van bedrijfsmiddelen? Kunt u aangeven voor welke bedrijfsmiddelen er een actuele registratie is?	Ja <ul style="list-style-type: none">• Hard- en software• Applicaties		

7.1.2 Eigendom van bedrijfsmiddelen

Vraag	Antwoord	Advies	Evaluatie en impact
7.1.2.a Is er voor elk bedrijfsproces, applicatie, gegevensverzameling en ICT-faciliteit een verantwoordelijke lijnmanager?	Ja		
Is de verantwoordelijke lijnmanager formeel vastgesteld?	Ja		

7.1.3 Aanvaardbaar gebruik van bedrijfsmiddelen

Vraag	Antwoord	Advies	Evaluatie en impact
7.1.3.a Zijn er regels opgesteld voor het juist gebruiken van (ICT-)bedrijfsmiddelen?	Ja		

7.2 Classificatie van informatie

7.2.1 Richtlijnen voor classificatie van informatie

Vraag	Antwoord	Advies	Evaluatie en impact
7.2.1.a Zijn er rubricerings- of classificatierichtlijnen opgesteld binnen de gemeente?	Nee	Het beschermingsniveau kan worden beoordeeld door het analyseren van de vertrouwelijkheid, integriteit en beschikbaarheid en andere eisen voor de informatie. Na verloop van tijd is informatie vaak niet langer gevoelig of kritiek, bijvoorbeeld wanneer de	1. Betreft de vraag wetgeving? Indien ja, dan moet ik het implementeren. 2. Wat is het risico wanneer ik dit niet implementeer (kans x impact)? 3. Wat kost het ons als het risico manifest wordt? 4. Wat kost het om te implementeren?

		<p>informatie openbaar is gemaakt. Ook daarmee behoort rekening te worden gehouden, omdat overclassificatie kan leiden tot de implementatie van overbodige beheersmaatregelen die leiden tot onnodige extra uitgaven.</p> <p>Het tegelijk bestuderen van documenten met soortgelijke beveiligingseisen bij het toewijzen van classificatieniveaus kan helpen bij het vereenvoudigen van de classificatietaak.</p>	Dient deze control geïmplementeerd te worden en met welke prioriteit?
Zijn de richtlijnen opgesteld op basis van het BIG-OP product dataclassificatie?	Niet van toepassing		
Zijn de essentiële gegevensverzamelingen binnen de gemeenten allen geclassificeerd volgens deze richtlijnen?	Niet van toepassing		

7.2.2 Labeling en verwerking van informatie

Vraag	Antwoord	Advies	Evaluatie en impact
7.2.2.a Worden er procedures ontwikkeld op basis van uitgevoerde dataclassificaties, zodat informatie het juiste niveau van bescherming krijgt?	Ja		
7.2.2.b Worden de ontwikkelde procedures ook gevolgd?	Ja		
Geldt dat ook voor de primaire processen/systemen?	Ja		

BIG hoofdstuk 8: Personele beveiliging

8.1 Voorafgaand aan het dienstverband

8.1.1 Rollen en verantwoordelijkheden

Vraag	Antwoord	Advies	Evaluatie en impact
8.1.1.a Zijn de rollen en verantwoordelijkheden van werknemers, ingehuurd personeel en externe gebruikers met betrekking tot informatiebeveiliging vastgelegd?	Ja		
Kunt u aangeven met betrekking tot welke van de hiernaast genoemde opties dit wordt vastgelegd en gecommuniceerd?	<ul style="list-style-type: none"> • m.b.t. het beveiligingsbeleid • m.b.t. de bescherming van bedrijfsmiddelen • m.b.t. speciale verantwoordelijkheden (ingeval van een BRP, BUN, SUWI rol/functie) • m.b.t. de rapportage van beveiligingsincidenten 		

8.1.2 Screening

Vraag	Antwoord	Advies	Evaluatie en impact
8.1.2.a Wordt de achtergrond van kandidaten voor een dienstverband, ingehuurd personeel en externe gebruikers evenredig gecontroleerd aan de eisen volgend uit de classificatie van informatie waar men toegang toe krijgt?	Ja		
Worden deze controles periodiek herhaald?	Nee		
Worden de gegevens die de medewerker opgeeft geverifieerd?	Ja		
Is voor alle medewerkers minimaal een VOG vereist?	Ja		

8.1.3 Arbeidsvoorwaarden

Vraag	Antwoord	Advies	Evaluatie en
-------	----------	--------	--------------

impact			
8.1.3.a Hebben de werknemers, ingehuurd personeel en externe gebruikers de voorwaarden met betrekking tot hun verantwoordelijkheden ten aanzien van informatiebeveiliging en privacy eisen, specifiek ter kennisname gekregen en aanvaard?	Ja		

8.2 Tijdens het dienstverband

8.2.1 Directieverantwoordelijkheid

Vraag	Antwoord	Advies	Evaluatie en impact
8.2.1.a Bevordert en controleert het lijnmanagement dat gemeentebambtenaren, ingehuurd personeel en externe gebruikers zich houden aan de beveiligingsregels overeenkomstig het beleid en de procedures van de organisatie?	Ja		
Waaruit blijkt dat?	<ul style="list-style-type: none"> uit verslagen van (werk)besprekingen 		

8.2.2 Bewustwording, opleiding en training ten aanzien van informatiebeveiliging

Vraag	Antwoord	Advies	Evaluatie en impact
8.2.2.a Zorgt het management ervoor dat de medewerkers voldoende kennis en bewustzijn hebben op het gebied van informatiebeveiliging?	Ja		
Hoe zorgt het management hier voor?	<ul style="list-style-type: none"> met bewustwordingscampagnes 		
Zijn hier verslagen van?	Ja		
Zijn er voldoende middelen gealloceerd voor het bevorderen van kennis en bewustwording van de medewerkers ten aanzien van informatieveiligheid?	Ja		

8.2.3 Disciplinaire maatregelen

Vraag	Antwoord	Advies	Evaluatie en
-------	----------	--------	--------------

impact			
8.2.3.a Is er een disciplinair proces vastgelegd, conform CAR/UWO, voor werknemers die inbreuk maken op het informatiebeveiligingsbeleid?	Ja		

8.3 Beëindiging of wijziging van het dienstverband

8.3.1 Beëindiging van verantwoordelijkheden

Vraag	Antwoord	Advies	Evaluatie en impact
8.3.1.a Heeft het lijnmanagement een procedure vastgesteld bij wijziging of beëindiging van het dienstverband, contract of overeenkomst op het gebied van informatiebeveiliging?	Ja		
8.3.1.b Worden toegangsrechten volgens de procedure ingetrokken als het dienstverband wijzigt dan wel eindigt?	Ja		

BIG hoofdstuk 9: Fysieke beveiliging en beveiliging van de omgeving

9.1 Beveiligde ruimten

9.1.1 Fysieke beveiliging van de omgeving

Vraag	Antwoord	Advies	Evaluatie en impact
9.1.1.a Zijn er gepaste toegangsbeveiligingsmaatregelen genomen voor ruimtes waar zich informatie en ICT-voorzieningen bevinden? Kunt u aangeven voor welke ruimtes er gepaste toegangsbeveiligingsmaatregelen zijn genomen?	Ja <ul style="list-style-type: none">Voor wat betreft de werkruimtenVoor de server- en SER-ruimtenVoor wat betreft de reisdocumentenVoor wat betreft de ruimten waar persoonsgegevens verwerkt worden		
Wordt hier mee voldaan aan artikel 91 van de PUN?	Ja		

9.1.2 Fysieke toegangsbeveiliging

Vraag	Antwoord	Advies	Evaluatie en impact
9.1.2. a Is de toegang tot de gebouwen en de beveiligde zones uitsluitend mogelijk voor geautoriseerde personen?	Ja		

9.1.3 Beveiliging van kantoren, ruimten en faciliteiten

Vraag	Antwoord	Advies	Evaluatie en impact
9.1.3.a Zijn er (binnen de kantoren / ruimtes) maatregelen getroffen voor de bescherming van mobiele gegevens- en andere informatie (dragers). Denk hierbij ook aan lockers en kluizen. Kunt u aangeven welke (beschermings) maatregelen er zijn getroffen?	Ja <ul style="list-style-type: none">Voor de opslag van gegevensdragers		

	<ul style="list-style-type: none"> • Er is een actief sleutelplan voor kluisen en sloten • Het is bekend waar incidenten gemeld kunnen worden 		
--	---	--	--

9.1.4 Bescherming tegen bedreigingen van buitenaf

Vraag	Antwoord	Advies	Evaluatie en impact
9.1.4.a Zijn er verzekeringsmaatregelen genomen die bescherming bieden tegen schade door geweld van buiten?	Ja		
Kunt u aangeven waartegen u bent verzekerd?	<ul style="list-style-type: none"> • Legen brand • Legen bliksem • Legen explosies 		

9.1.5 Werken in beveiligde ruimten

Vraag	Antwoord	Advies	Evaluatie en impact
9.1.5.a Zijn er maatregelen en procedures geïmplementeerd voor het werken in en toezien op beveiligde ruimtes?	Ja		
Kunt u aangeven waarvoor de maatregelen en procedures zijn geïmplementeerd?	<ul style="list-style-type: none"> • Voor bezoekers • Voor ongeautoriseerd personeel • Voor geautoriseerd personeel • Voor het maken van foto's en video's 		

9.1.6 Openbare toegang en gebieden voor laden en lossen

Vraag	Antwoord	Advies	Evaluatie en impact
9.1.6.a Zijn publiek toegankelijke ruimtes afgeschermd zodat onbevoegden zich geen toegang kunnen verschaffen tot bedrijfsmiddelen?	Ja		

9.2 Beveiliging van apparatuur

9.2.1 Plaatsing en bescherming van apparatuur

Vraag	Antwoord	Advies	Evaluatie en impact
9.2.1.a Wordt apparatuur overeenkomstig de voorschriften geplaatst en gebruikt zodat het risico van schade, storing en onbevoegde toegang verminderd worden?	Ja		
Kunt u aangeven waartegen de apparatuur wordt beschermd?	<ul style="list-style-type: none">• <u>Iegen blikseminslag en spanningsschommeling</u> <u>en</u>• <u>Iegen brand en waterschade</u>• <u>Iegen onbevoegde toegang</u>		

9.2.2 Plaatsing en bescherming van apparatuur

Vraag	Antwoord	Advies	Evaluatie en impact
9.2.2.a Zijn er maatregelen en procedures geïmplementeerd om uitval van apparatuur te voorkomen door stroomuitval of onderbreking van de nutsvoorzieningen?	Ja, maatregelen		

9.2.3 Beveiliging van kabels

Vraag	Antwoord	Advies	Evaluatie en impact
9.2.3.a Zijn de voedings- en telecommunicatiekabels aangelegd conform de NEN 1010?	Ja		

9.2.4 Onderhoud van apparatuur

Vraag	Antwoord	Advies	Evaluatie en impact
9.2.4.a Zijn er procedures voor het beheerst en door bevoegde personen uit te laten voeren van technisch onderhoud aan IT apparatuur?	Ja, middels <u>procedures en onderhoudscontracten</u>		

9.2.5 Beveiliging van apparatuur buiten het terrein

Vraag	Antwoord	Advies	Evaluatie en impact
9.2.5.a Zijn er maatregelen en procedures geïmplementeerd voor apparatuur als er buiten de vertrouwde omgeving gewerkt wordt?	Ja, met maatregelen en procedures		

9.2.6 Veilig verwijderen of hergebruiken van apparatuur

Vraag	Antwoord	Advies	Evaluatie en impact
9.2.6.a Is er een procedure voor het veilig verwijderen van alle gevoelige (bedrijfsvertrouwelijke) informatie op IT middelen die worden gerepareerd of niet meer worden gebruikt?	Ja		

9.2.7 Veilig verwijderen of hergebruiken van apparatuur

Vraag	Antwoord	Advies	Evaluatie en impact
9.2.7.a Is er voor gezorgd dat apparatuur, informatie en programmatuur niet zonder toestemming van de gebruikelijke (werk) locatie kan worden meegenomen?	Ja		

BIG hoofdstuk 10: Beheer van Communicatie en bedieningsprocessen

10.1 Bedieningsprocedures en verantwoordelijkheden

10.1.1 Gedocumenteerde bedieningsprocedures

Vraag	Antwoord	Advies	Evaluatie en impact
10.1.1.a Zijn er actuele schriftelijke procedures voor het operationeel beheer (en gebruik) van de IT voorzieningen (software, hardware, netwerk, databases)?	Ja		
10.1.1.b Wordt de Suwinetinfrastructuur, servers en netwerkcomponenten, gehardend volgens de vastgestelde configuratie baseline?	Ja		

10.1.2 Wijzigingsbeheer

Vraag	Antwoord	Advies	Evaluatie en impact
10.1.2.a Is er een vastgestelde procedure voor het beheerst uitvoeren van wijzigingen op de IT voorzieningen (een wijzigingsbeheerproces)?	Ja		
Zijn hier ook verslagen van?	Ja		

10.1.3 Functiescheiding

Vraag	Antwoord	Advies	Evaluatie en impact
10.1.3.a Zijn de taken en verantwoordelijkheden voor het gebruik en het beheer van IT voorzieningen naar rato van de organisatiegrootte gescheiden?	Ja		
Kunt u aangeven hoe de taken en verantwoordelijkheden voor het gebruik en het beheer van IT voorzieningen zijn gescheiden?	<ul style="list-style-type: none">Dit hebben we gedaan voor de functies van BRP, PUN en SUWIDe rol van CISO of controller informatiebeveiliging is apart, onafhankelijk belegd		

10.1.3.b Welke rollen en functiebenamingen zijn er belegd, dan wel aangewezen door het college?	<ul style="list-style-type: none"> • Systeembeheerder • Applicatiebeheerder BRP • Gegevensbeheerder BRP • Privacybeheerder BRP • Security Officer SUWI • Toezichthouder BRP 	Taken en verantwoordelijkheidsgebieden behoren te worden gescheiden om gelegenheid voor onbevoegde of onbedoelde wijziging of misbruik van de bedrijfsmiddelen van de organisatie te verminderen.	
10.1.3.c Is er sprake van een scheiding in verantwoordelijkheden tussen: uitvoerder en de beveiligingsfunctionaris en tussen opdrachtgever en de beveiligingsfunctionaris?	<ul style="list-style-type: none"> • Ja, tussen de uitvoerder en de beveiligingsfunctionaris • Ja, tussen de opdrachtgever en de beveiligingsfunctionaris 	Zonder een beveiligingsfunctionaris reisdocumenten kunt u niet voldoen aan de wet PUN	

10.1.4 Scheiding van faciliteiten voor ontwikkeling, testen en productie

Vraag	Antwoord	Advies	Evaluatie en impact
10.1.4.a Wordt er in huis software ontwikkeld of getest?	Er wordt alleen software getest		
Maakt u daarbij gebruik van een OTAP-omgeving?	Ja		

10.2 Exploitaties door een derde partij

10.2.1 Dienstverlening

Vraag	Antwoord	Advies	Evaluatie en impact
10.2.1.a Zijn voor de uitbestede IT diensten, naast de afgesproken dienstenniveaus, ook alle relevante beveiligingseisen opgenomen in de contracten met de IT leveranciers en/of bewerkers?	Ja		
Kunt u aangeven waar deze beveiligingseisen op zijn gericht?	<ul style="list-style-type: none"> • Maatregelen gericht op medewerkers • Maatregelen gericht op de toegang tot gebouwen en ruimten • Maatregelen gericht op een deugdelijke werking van de apparatuur en 		

	<ul style="list-style-type: none"> programmatuur Maatregelen gericht op de beveiliging van de apparatuur en programmatuur Maatregelen gericht op het gegevensbeheer Maatregelen ingeval van schending van de geheimhouding Maatregelen ingeval van calamiteiten Gebruik van gegevens uitsluitend voor de afgesproken werkzaamheden De bewerker houdt zich aan de wettelijke voorschriften De bewerker staat toe dat de gemeente controles uitvoert Werkzaamheden worden opgeschort op vordering van de gemeente Werkzaamheden worden zonder toestemming van de gemeente door de bewerker niet uitbesteed 		
--	--	--	--

10.2.2 Controle en beoordeling van dienstverlening door een derde partij

Vraag	Antwoord	Advies	Evaluatie en impact
10.2.2.a Hoe is in het afgelopen jaar getoetst dat de IT-leveranciers en/of bewerkers zich houden aan de afgesproken diensten niveaus en informatiebeveiligingseisen?	<ul style="list-style-type: none"> Er is intern door de gemeente zelf een controle uitgevoerd De IT-leverancier heeft een toets uit laten voeren 	<p>De diensten, rapporten en registraties die door de derde partij worden geleverd, behoren regelmatig te worden gecontroleerd en beoordeeld en er behoren regelmatig audits te worden uitgevoerd.</p>	
Is er door de externe IT leverancier			

een TPM opgeleverd?			
---------------------	--	--	--

10.2.3 Beheer van wijzigingen in dienstverlening door een derde partij

Vraag	Antwoord	Advies	Evaluatie en impact
10.2.3.a Wordt er met partijen waaraan IT diensten zijn uitbesteed periodiek overleg gevoerd over bestaan en actualiteit van IB-maatregelen rondom beschikbaarheid, bescherming en continuïteit van de IT voorziening/ -diensten ?	Ja		

10.3 Systeemplanning en acceptatie

10.3.1 Capaciteitsbeheer

Vraag	Antwoord	Advies	Evaluatie en impact
10.3.1.a Zijn er maatregelen getroffen waarmee de afgesproken actuele en toekomstig systeembelasting inzichtelijk en op voldoende niveau is?	Ja		

10.3.2. Systeem acceptatie

Vraag	Antwoord	Advies	Evaluatie en impact
10.3.2.a Is er een formele testprocedure voor accepteren van nieuwe en gewijzigde systemen (zowel door de gebruikersorganisatie als het beheer)?	Ja		

10.4 Bescherming van virussen en 'mobile code'

10.4.1 Maatregelen tegen virussen

Vraag	Antwoord	Advies
10.4.1.a Welke antivirus maatregelen heeft u ingevoerd?	<ul style="list-style-type: none"> • Detectieve maatregelen (scanners) • Preventieve maatregelen (patching en hardening) • Recovery maatregelen (back-up) • Bewustwording van gebruikers 	Er behoren maatregelen te worden getroffen voor detectie, preventie en herstellen om te beschermen tegen virussen en er behoren geschikte procedures te worden ingevoerd om het bewustzijn van de gebruikers te vergroten.

10.4.2 Maatregelen tegen 'mobile code'

Vraag	Antwoord	Advies	Evaluatie en impact
10.4.2.a Welke maatregelen heeft u genomen tegen het onbedoeld of onbewust uitvoeren van ongewenste mobiele codes, zoals Java en Flash?	Java/Flash wordt door ons met minimale rechten beschikbaar gesteld		

10.5 Back-up

10.5.1 Reservekopieën maken (back-ups)

Vraag	Antwoord	Advies	Evaluatie en impact
10.5.1.a Heeft u een actueel back-up beleid en worden back-ups dienovereenkomstig gemaakt, getest en opgeslagen?	Ja		
Kunt u aangeven waarvoor u een actueel back-beleid heeft en waarvoor de back-ups worden gemaakt, getest en opgeslagen?	<ul style="list-style-type: none"> Deze is generiek ingericht voor alle data en informatie 		

10.6 Beheer van netwerkbeveiliging

10.6.1 Maatregelen voor netwerken

Vraag	Antwoord	Advies	Evaluatie en impact
10.6.1.a Welke maatregelen heeft u genomen om de aanwezige netwerken adequaat te monitoren en beveiligen?	<ul style="list-style-type: none"> Wij hebben dit uitbesteed bij een andere gemeente/leverancier Wij hebben op alle vertrouwde koppelvlakken een beheerde firewall Wij maken generiek gebruik van een IDS Wij doen aan content scanning De gegevensuitwisseling tussen vertrouwde en onvertrouwde zones worden inhoudelijk 		

	<p>geautomatiseerd en gecontroleerd op de aanwezigheid van malware</p> <p>• Er zijn procedures voor beheer van apparatuur op afstand</p>		
10.6.1.b Heeft u al deze maatregelen ook expliciet ingezet in het kader van telewerken in relatie tot BRP en Suwi?	Ja		

10.6.2 Beveiliging van netwerkdiensten

Vraag	Antwoord	Advies	Evaluatie en impact
10.6.2.a Worden de beveiligingskenmerken, de niveaus van dienstverlening en de beheereisen vanuit systemen en processen doorvertaald naar de overeenkomsten voor netwerkdiensten?	Ja		

10.7 Behandeling van media

10.7.1 Beheer van verwijderbare media

Vraag	Antwoord	Advies	Evaluatie en impact
10.7.1.a Zijn er procedures en maatregelen voor het beheer en de beveiliging van informatie op papier en op (verwijderbare) elektronische gegevensdragers zoals laptops, usb-sticks, externe disks en backup tapes?	Ja		
Voldoet u hiermee aan artikel 91 van de PUN?	Ja		

10.7.2 Verwijdering van media

Vraag	Antwoord	Advies	Evaluatie en impact
10.7.2.a Heeft u procedures opgesteld voor verwijderen/vernietigen van informatie?	Ja		
Geldt dit ook voor verwijderbare media en het verwijderen van vertrouwelijke data (van harddisks)?	Ja		

10.7.3 Procedures voor de behandeling van informatie

Vraag	Antwoord	Advies	Evaluatie en impact
10.7.3.a Zijn er procedures voor de behandeling en opslag van informatie? Kunt u aangeven welke procedures en regels er zijn?	Ja <ul style="list-style-type: none"> Gevoelige en vertrouwelijke informatie mag niet buiten het gemeentelijke netwerk (DMZ) opgeslagen worden Er is clean desk policy 		

10.7.4 Beveiliging van systeemdokumentatie

Vraag	Antwoord	Advies	Evaluatie en impact
10.7.4.a Wordt systeem documentatie voldoende beschermd tegen onbevoegde toegang?	Ja		
Staat uw systeemdokumentatie op een logisch afgeschermd omgeving?	Ja		
Is uw systeemdokumentatie geclassificeerd en beveiligd met een wachtwoord?	Nee		

10.8 Uitwisseling van informatie

10.8.1 Beleid en procedures voor informatie-uitwisseling

Vraag	Antwoord	Advies	Evaluatie en impact
10.8.1.a Is er beleid en zijn er procedures voor een beheerste en beveiligde wijze van informatie-uitwisseling, zowel binnen als buiten de gemeente? Kunt u aangeven waarvoor deze procedures en beleid gelden?	Ja <ul style="list-style-type: none"> Voor transport van geclassificeerde informatie Voor faxen en e-mail 		

Zijn de medewerkers geïnstrueerd over het beleid en procedures voor een beheerste en beveiligde wijze van informatie-uitwisseling?	Ja	<ul style="list-style-type: none"> Voor mobiele apparaten 		
--	----	--	--	--

10.8.2 Uitwisselingsovereenkomsten

Vraag	Antwoord	Advies	Evaluatie en impact
10.8.2.a Zijn er overeenkomsten afgesloten voor de beheerste en beveiligde wijze van informatie-uitwisseling met andere partijen?	Ja		
Kunt u aangeven welke van de hiernaast genoemde aspecten zijn meegenomen in de overeenkomst?	<ul style="list-style-type: none"> Betrouwbaarheid 		
Is de overeenkomst bij alle medewerkers bekend?	Nee		

10.8.3 Fysieke media die worden getransporteerd

Vraag	Antwoord	Advies	Evaluatie en impact
10.8.3.a Is er een procedure of zijn er middelen waarmee bij transport van (verwijderbare / mobiele) elektronische gegevensdragers zoals cd-roms, usb-sticks, externe disks en backup tapes maar ook lap-tops) vertrouwelijke informatie op een veilige wijze is opgeslagen?	Ja		

10.8.4. Elektronische berichtenuitwisseling

Vraag	Antwoord	Advies	Evaluatie en impact
10.8.4.a Zijn er middelen waarmee vertrouwelijke informatie op adequate wijze is beveiligd bij uitwisseling via berichtenverkeer (bijvoorbeeld XML of e-mail)?	Ja		
Kunt u aangeven welke middelen hiervoor worden ingezet?	<ul style="list-style-type: none"> Encryptie PKI-Overheid 		

10.8.5 Systemen voor bedrijfsinformatie

Vraag	Antwoord	Advies	Evaluatie en impact
10.8.5.a Zijn er vastgestelde procedures of richtlijnen waarmee vertrouwelijke informatie op de KA (kantoor automatisering) omgeving op adequate en afdoende wijze wordt beveiligd?	Ja		
Zijn de risico's in kaart gebracht?	Ja		
Zijn de onderlinge verbanden inzichtelijk gemaakt?	Nee		

10.9 Diensten voor e-commerce

10.9.1 E-commerce

Vraag	Antwoord	Advies	Evaluatie en impact
10.9.1.a Heeft u maatregelen geïmplementeerd voor het beschermen van online transacties of voor het gebruik maken van beveiligde authenticatie mechanismen?	Nee	informatie die een rol speelt bij e-commerce en die via openbare netwerken wordt uitgewisseld, behoort te worden beschermd tegen frauduleuze activiteiten, geschillen over contracten en onbevoegde openbaarmaking en modificatie.	1. Betreft de vraag wetgeving? Indien ja, dan moet ik het implementeren. 2. Wat is het risico wanneer ik dit niet implementeer (kans x impact)? 3. Wat kost het ons als het risico manifest wordt? 4. Wat kost het om te implementeren? Dient deze control geïmplementeerd te worden en met welke prioriteit?
Kunt u aangeven voor welk soort producten en diensten er maatregelen zijn geïmplementeerd?	Niet van toepassing		

10.9.3 Openbaar beschikbare informatie

Vraag	Antwoord	Advies	Evaluatie en impact
10.9.3.a Heeft u maatregelen geïmplementeerd die er voor zorgen dat openbare informatie beschermd is tegen modificatie?	Ja		

10.10 Controle

10.10.1 Aanmaken audit-logbestanden

Vraag	Antwoord	Advies	Evaluatie en impact
10.10.1.a Worden systeemhandelingen gelogd, zodanig dat handelingen van gebruikers en beheerders kunnen worden geanalyseerd onder meer t.b.v. een audittrail?	Ja		
Kunt u aangeven voor welke systemen er wordt gelogd?	<ul style="list-style-type: none"> • Ja, voor wat betreft Suwinet-inlezen en DKD-inlezen • Ja, voor wat betreft BRP • Ja, voor overige systemen 		
Worden storingen gelogd?	Ja		
Worden administratieve handelingen gelogd?	Ja		
Worden de login-gegevens minimaal 3 maanden bewaard?	Ja		

10.10.2 Controle systeemgebruik

Vraag	Antwoord	Advies	Evaluatie en impact
10.10.2.a Is er een procedure voor het structureel controleren van de logbestanden op het netwerk-systeemgebruik?	Ja		
Kunt u aangeven of er een procedure is om de handelingen van gebruikers te controleren?	Voor wat betreft SUWI Voor wat betreft BRP Voor wat betreft DigiD		

10.10.3 Bescherming van informatie in logbestanden

Vraag	Antwoord	Advies	Evaluatie en impact
10.10.3.a Krijgen logbestanden adequate bescherming tegen verminking, verlies en verandering?	Ja		

10.10.6 Synchronisatie van systeemklokken

Vraag	Antwoord	Advies	Evaluatie en impact
-------	----------	--------	---------------------

10.10.6.a Wordt er kloksynchronisatie toegepast op alle actieve infrastructuur en informatiesystemen?	Ja		
---	----	--	--

BIG hoofdstuk 11: Toegangsbeveiliging

11.1 Toegangsbeleid

11.1.1 Toegangsbeveiliging

Vraag	Antwoord	Advies	Evaluatie en impact
11.1.1.a Is er beleid vastgesteld dat richting geeft aan de beheerste logische toegang tot gegevens en informatie?	Ja		

11.2 Beheer van toegangsrechten van gebruikers

11.2.1 Registratie van gebruikers

Vraag	Antwoord	Advies	Evaluatie en impact
11.2.1.a Is er een vastgestelde autorisatieprocedure voor het administreren van gebruikers en het toekennen / intrekken van toegangsrechten voor alle informatie en –systemen en de controle daarop?	Ja		
Is deze procedure belegd bij de betrokken systeem/proces eigenaar?	Ja		

11.2.2. Beheer van speciale bevoegdheden

Vraag	Antwoord	Advies	Evaluatie en impact
11.2.2.a Wordt de toewijzing en het gebruik van speciale bevoegdheden beperkt en beheerst?	Ja		
Is dit herleidbaar aan een (beheer) principe of doelstelling?	Ja		

11.2.3. Beheer van gebruikerswachtwoorden

Vraag	Antwoord	Advies	Evaluatie en impact
11.2.3.a Is er een vastgestelde procedure voor de vormgeving en het (veilig) uitgeven en opslaan van wachtwoorden en andere authenticatie middelen?	Ja		

11.2.4 Beoordeling van toegangsrechten van gebruikers

Vraag	Antwoord	Advies	Evaluatie en impact
11.2.4.a Worden de toegangsrechten van gebruikers regelmatig beoordeeld in een formeel proces?	Ja		
Zijn er verslagen van de beoordeling van de toegangsrechten?	Ja		

11.3 Verantwoordelijkheden van gebruikers

11.3.1 Gebruik van wachtwoorden

Vraag	Antwoord	Advies	Evaluatie en impact
11.3.1.a Worden alle medewerkers regelmatig geïnformeerd over de regels voor het juist en veilig gebruik van wachtwoorden?	Ja		
11.3.1.b Welke voorwaarden zijn aan de wachtwoorden gesteld? Geef aan wat voor uw organisatie van toepassing is.	<ul style="list-style-type: none"> Wachtwoorden bestaan uit minimaal 8 karakters, waarvan tenminste 1 hoofdletter, 1 cijfer en 1 vreemd teken Wachtwoorden zijn maximaal 60 dagen geldig en mogen niet binnen 6 keer herhaald worden Ijdelijke of standaard wachtwoorden worden bij het eerste gebruik vervangen Het wachtwoord is alleen bij de gebruiker bekend 		

11.3.2 Onbeheerde gebruikersapparatuur

Vraag	Antwoord	Advies	Evaluatie en impact
11.3.2.a Worden alle medewerkers regelmatig geïnformeerd over de regels voor het juist en veilig gebruik van hun mobiele apparatuur, zoals laptops, smartphones en tablets?	Ja		
11.3.2.b Worden deze regels	Ja		

(waar mogelijk) door een policy afgedwongen?			
--	--	--	--

11.3.3 'Clear desk'- en 'clear screen'-beleid

Vraag	Antwoord	Advies	Evaluatie en impact
11.3.3.a Is er een clear desk-beleid voor papier, usb-sticks, externe schijven en mobiele devices en een clear screen-beleid voor ICT-voorzieningen?	Ja		
11.3.3.b Is er een clear screen-beleid voor ICT-voorzieningen?	Ja		

11.4 Toegangsbeheersing voor netwerken

11.4.1 Beleid ten aanzien van het gebruik van netwerkdiensten

Vraag	Antwoord	Advies	Evaluatie en impact
11.4.1.a Is er een formele procedure voor het toekennen van toegangsrechten voor het netwerk en netwerkdiensten?	Ja		

11.4.2 Authenticatie van gebruikers bij externe verbindingen

Vraag	Antwoord	Advies	Evaluatie en impact
11.4.2.a Is er een vastgestelde procedure voor het authenticeren van (externe) gebruikers voor toegang tot het netwerk van buiten?	Ja		
Wordt er hierbij gebruik gemaakt van een twee factor authenticatie?	Ja		

11.4.3 Identificatie van (netwerk)apparatuur

Vraag	Antwoord	Advies	Evaluatie en impact
11.4.3.a Is er een vastgestelde policy of richtlijn voor identificatie en authenticatie van netwerkapparatuur?	Ja		

11.4.4 Bescherming op afstand van poorten voor diagnose en configuratie

Vraag	Antwoord	Advies	Evaluatie en impact
11.4.4.a Is er een procedure voor de	Ja		

beheerste toegang tot netwerkpoorten (bv firewalls) en netwerkcomponenten (bv switches) voor beheeractiviteiten (bv diagnose, configureren)?			
--	--	--	--

11.4.5 Scheiding van netwerken

Vraag	Antwoord	Advies	Evaluatie en impact
11.4.5.a Is het netwerk ingedeeld in specifieke zones (compartimenten / segmenten) voor de diverse IT services waarbij de verkeersstromen tussen de zones worden beperkt tot alleen de hoogst noodzakelijke?	Ja		

11.4.6 Beheersmaatregelen voor netwerkverbindingen

Vraag	Antwoord	Advies	Evaluatie en impact
11.4.6.a Is de toegang van gebruikers in een gemeenschappelijk netwerk (met andere organisaties) ingericht volgens het geldende toegangsbeleid van de organisatie?	Ja		

11.4.7 Beheersmaatregelen voor netwerkrouting

Vraag	Antwoord	Advies	Evaluatie en impact
11.4.7.a Zijn netwerken voorzien van beheersmaatregelen voor netwerkrouting, om te bewerkstelligen dat computerverbindingen en informatiestromen niet in strijd zijn met het toegangsbeleid voor de bedrijfstoeepassingen?	Ja		

11.5 Toegangsbeveiliging voor besturingssystemen

11.5.1 Beveiligde inlogprocedures

Vraag	Antwoord	Advies	Evaluatie en impact
11.5.1.a Wordt de toegang tot besturingssystemen beheerst met een beveiligde inlogprocedure?	Ja		
Wordt er gebruik gemaakt van ACL's (Access Control List)?	Ja		

11.5.2 Gebruikersidentificatie en -authenticatie

Vraag	Antwoord	Advies	Evaluatie en impact
11.5.2.a Hebben alle gebruikers en beheerders een unieke inlognaam (identificatie)? Zie ook vraag 11.2.2.	Ja		
11.5.2.b Zijn er geschikte technieken om de identiteit van de gebruiker / beheerder vast te stellen	Ja		
Wordt dit gecontroleerd?	Ja		

11.5.3 Systemen voor wachtwoordbeheer

Vraag	Antwoord	Advies	Evaluatie en impact
11.5.3.a Worden de richtlijnen voor het gebruik en de sterkte van wachtwoorden door het systeem afgedwongen?	Ja		

11.5.4 Gebruik van systeemhulpmiddelen

Vraag	Antwoord	Advies	Evaluatie en impact
11.5.4.a Wordt het gebruik van hulpprogrammatuur waarmee database-, systeem- en toepassingsbeheersmaatregelen zouden kunnen worden gepasseerd, beperkt en beheerst?	Ja		

11.5.5 Time-out van sessies

Vraag	Antwoord	Advies	Evaluatie en impact
11.5.5.a Worden werkstations en sessies op afstand vergrendeld of uitgeschakeld na een vastgestelde periode van inactiviteit?	Ja		
Kunt u aangeven na welke periode?	<ul style="list-style-type: none"> Na 15 minuten vergrendeld 		

11.5.6 Beperking van verbindingstijd

Vraag	Antwoord	Advies	Evaluatie en impact
11.5.6.a Is er een procedure voor de beheerste (beperkt voor de duur van onderhoud) en veilige	Ja		

(two factor authenticatie) toegang van externe leveranciers voor het onderhoud van de IT middelen?			
--	--	--	--

11.6 Toegangsbeheersing voor toepassingen en informatie

11.6.1. Beperking van toegang tot informatie

Vraag	Antwoord	Advies	Evaluatie en impact
11.6.1.a Wordt de toegang tot informatie en functies van toepassingssystemen door gebruikers en ondersteunend personeel beperkt?	Ja		

11.6.2 Isolatie van gevoelige systemen

Vraag	Antwoord	Advies	Evaluatie en impact
11.6.2.a Zijn systemen met risicovolle informatie in een eigen omgeving (netwerksegment) ondergebracht dat 'logisch of fysiek gescheiden' is van de rest van het netwerk?	Ja		
Kunt u aangeven voor welke systemen?	<ul style="list-style-type: none"> Voor verkeer uit de DMZ Voor beheer (actieve) netwerkcomponenten 		

11.7 Draagbare computers en telenetwerken

11.7.1 Draagbare computers en communicatievoorzieningen

Vraag	Antwoord	Advies	Evaluatie en impact
11.7.1.a Is er formeel beleid en zijn geschikte beveiligingsmaatregelen getroffen voor de inrichting en gebruik van laptops, tablets en andere mobiele communicatie apparaten?	Ja		
Kunt u aangeven welke beveiligingsmaatregelen u heeft getroffen?	<ul style="list-style-type: none"> Door middel van MDM/WTR Harddisk encryptie voor laptops 		

Gelden deze maatregelen voor de hele gemeente?	Ja		
Heeft uw gemeente uitgewerkt welke systemen wel en niet geraadpleegd mogen worden?	Ja		

11.7.2 Telewerken

Vraag	Antwoord	Advies	Evaluatie en impact
11.7.2.a Is er beleid en zijn er procedures voor het werken met informatiesystemen buiten de reguliere kantooromgeving?	<ul style="list-style-type: none"> Ja, er is beleid en er zijn procedures 		
Heeft de gemeente een telewerkbeleid?	Ja		
Heeft de gemeente uitgewerkt welke systemen wel en niet mogen worden geraadpleegd?	Ja		
Zijn de telewerkvoorzieningen op basis van zero-footprint ingericht?	Nee		

BIG hoofdstuk 12: Verwerving, ontwikkeling en onderhoud van informatiesystemen

12.1 Beveiligingseisen voor informatiesystemen

12.1.1 Analyse en specificatie van beveiligingseisen

Vraag	Antwoord	Advies	Evaluatie en impact
12.1.1.a Wordt bij het analyseren en specificeren van de eisen voor nieuwe systemen of systeemwijzingen expliciet aandacht besteed aan de eisen voor informatiebeveiliging?	Ja		

12.2 Correcte verwerking in toepassingen

12.2.1 Validatie van invoergegevens (BRP)

Vraag	Antwoord	Advies	Evaluatie en impact
12.2.1.a Vindt er bij invoer van gegevens in (web-)applicaties validatie plaats op aspecten als juistheid en geschiktheid?	Ja		
12.2.1.b Valideert de webapplicatie de inhoud van een HTTP-request voordat deze gebruikt wordt?	Ja		
12.2.1.c Welke BRP specifieke maatregelen heeft u getroffen?	<ul style="list-style-type: none"> Iedere digitale aangifte wordt voor de definitieve verwerking door een medewerker gecontroleerd 	<p>Dit is een BRP-vraag; als u inwoners toestaat om digitaal aangifte te doen, dient de authenticiteit van de inwoner gevalideerd te worden middels DigiD.</p>	

12.2.2 Beheersing van interne gegevensverwerking

Vraag	Antwoord	Advies	Evaluatie en impact
12.2.2.a Is er beleid of zijn er richtlijnen voor verwerking-, en uitvoervalidaties bij de ontwikkeling van (web-) applicaties?	Nee	Er behoren validatiecontroles te worden opgenomen in toepassingen om eventueel corrumperen van informatie door verwerkingfouten of opzettelijke handelingen te ontdekken.	<p>1. Betreft de vraag wetgeving? Indien ja, dan moet ik het implementeren.</p> <p>2. Wat is het risico wanneer ik dit niet implementeer (kans x impact)?</p> <p>3. Wat kost het ons als het risico manifest</p>

			<p>wordt?</p> <p>4. Wat kost het om te implementeren?</p> <p>Dient deze control geïmplementeerd te worden en met welke prioriteit?</p>
--	--	--	--

12.2.3 Integriteit van berichten

Vraag	Antwoord	Advies	Evaluatie en impact
12.2.3.a Zijn er maatregelen geïmplementeerd om verandering van berichten in toepassingen te voorkomen?	Nee	Er behoren validatiecontroles te worden opgenomen in toepassingen om eventueel corrumperen van informatie door verwerkingsfouten of opzettelijke handelingen te ontdekken.	<p>1. Betreft de vraag wetgeving? Indien ja, dan moet ik het implementeren.</p> <p>2. Wat is het risico wanneer ik dit niet implementeer (kans x impact)?</p> <p>3. Wat kost het ons als het risico manifest wordt?</p> <p>4. Wat kost het om te implementeren?</p> <p>Dient deze control geïmplementeerd te worden en met welke prioriteit?</p>

12.2.4 Validatie van uitvoergegevens

Vraag	Antwoord	Advies	Evaluatie en impact
12.2.4.a Is er beleid of zijn er richtlijnen voor invoer- en verwerkingvalidaties bij de ontwikkeling van (web-) applicaties?	Nee	Gegevensuitvoer uit een toepassing behoort te worden gevalideerd, om te bewerkstelligen dat de verwerking van opgeslagen gegevens op de juiste manier plaatsvindt en geschikt is gezien de omstandigheden.	<p>1. Betreft de vraag wetgeving? Indien ja, dan moet ik het implementeren.</p> <p>2. Wat is het risico wanneer ik dit niet implementeer (kans x impact)?</p> <p>3. Wat kost het ons als het risico manifest wordt?</p> <p>4. Wat kost het om te implementeren?</p> <p>Dient deze control geïmplementeerd te worden en met welke prioriteit?</p>

12.3 Cryptografische beheersmaatregelen

12.3.1 Beleid voor het gebruik van cryptografische beheersmaatregelen

Vraag	Antwoord	Advies	Evaluatie en impact
12.3.1.a Is er een vastgesteld beleid voor het toepassen en beheren van cryptografische middelen?	Ja		

12.3.2 Sleutelbeheer

Vraag	Antwoord	Advies	Evaluatie en impact
12.3.2.a Zijn er maatregelen getroffen specifiek voor het beheren van cryptografische sleutels?	Ja		

12.4 Beveiliging van systeembestanden

12.4.1 Beheersing van operationele software

Vraag	Antwoord	Advies	Evaluatie en impact
12.4.1.a Zijn er maatregelen getroffen voor het beheren en het beheerst wijzigen van (applicatie-) programmatuur?	Ja		
12.4.1.b Is er een hardeningsproces voor ICT-componenten?	Ja		

12.4.2 Bescherming van testdata

Vraag	Antwoord	Advies	Evaluatie en impact
12.4.2.a Is in het testproces een procedure opgenomen voor het zorgvuldig gebruik van geanonimiseerde testdata?	Ja		
Wordt in het testproces een kopie van de productiedatabase gemaakt, of zijn er geen testplannen met geanonimiseerde testgegevens?	Niet van toepassing		
12.4.2.b Wordt er in het testproces een kopie van de productie database gemaakt?	Ja		

12.4.3 Toegangsbeheersing voor broncode van programmatuur

Vraag	Antwoord	Advies	Evaluatie en impact
12.4.3.a Zijn er maatregelen	Ja		

getroffen voor het beheerst en veilig opslaan van broncode?			
Kunt u aangeven waarom er geen maatregelen zijn getroffen voor het beheerst en veilig opslaan van broncode of waarom dit niet voor u van toepassing is?	Niet van toepassing		

12.5 Beveiliging bij ontwikkeling en ondersteuningsprocessen

12.5.1 Procedures voor wijzigingsbeheer

Vraag	Antwoord	Advies	Evaluatie en impact
12.5.1.a Is binnen de gemeente een formeel proces ingericht voor het uitvoeren van wijzigingen?	Ja		

12.5.2 Technische beoordeling van toepassingen na wijzigingen in het besturingssysteem

Vraag	Antwoord	Advies	Evaluatie en impact
12.5.2.a Voert u zelf testen uit op kritische toepassingen, na wijzigingen in de besturingssystemen?	Ja		
Kunt u aangeven waarom er geen testen worden uitgevoerd op de kritische toepassingen, na wijzigingen in de besturingssystemen?	Niet van toepassing		
Kunt u aangeven op welk niveau(s) de testen plaatsvinden?	<ul style="list-style-type: none"> Op applicatieniveau (informatiesysteem) Op gegevensniveau (databasesysteem) 		

12.5.3 Restricties op wijzigingen in programmatuurpakketten

Vraag	Antwoord	Advies	Evaluatie en impact
12.5.3.a Is er in de gemeentelijke procedure voor het installeren van Servers, OS-en en Ontwikkelplatforms expliciet aandacht voor het uitzetten van niet noodzakelijke functionaliteit en toegang?	Ja		
Kunt u aangeven waarom hier geen aandacht voor is?	Niet van toepassing		

12.5.4 Uitlekken van informatie

Vraag	Antwoord	Advies	Evaluatie en impact
12.5.4.a Heeft de gemeente maatregelen getroffen voor het 'scannen' van in en uitgaand netwerkverkeer (content scanning, IDS, IPS)?	Ja		
Kunt u aangeven waarom er geen maatregelen zijn getroffen?	Niet van toepassing		

12.5.5 Uitbestede ontwikkeling van programmatuur

Vraag	Antwoord	Advies	Evaluatie en impact
12.5.5.a Zijn er contracten afgesloten met de IT Leveranciers voor systeemontwikkeling met expliciet aandacht voor informatiebeveiligingseisen, ontwikkelstandaarden en intellectueel eigendom?(zie ook vragen 6.2 en 10.2)	Nee	Uitbestede ontwikkeling van programmatuur behoort onder supervisie te staan van en te worden gecontroleerd door de organisatie.	<p>1. Betreft de vraag wetgeving? Indien ja, dan moet ik het implementeren.</p> <p>2. Wat is het risico wanneer ik dit niet implementeer (kans x impact)?</p> <p>3. Wat kost het ons als het risico manifest wordt?</p> <p>4. Wat kost het om te implementeren?</p> <p>Dient deze control geïmplementeerd te worden en met welke prioriteit?</p>

12.6 Beheer van technische kwetsbaarheden

12.6.1 Beheersing van technische kwetsbaarheden

Vraag	Antwoord	Advies	Evaluatie en impact
12.6.1.a Zijn er maatregelen getroffen voor het regelmatig controleren op technische kwetsbaarheden in IT Services en Servers?	Ja		
Kunt u aangeven welke maatregelen er zijn getroffen voor het regelmatig controleren op technische kwetsbaarheden in IT Services en Servers?	<ul style="list-style-type: none"> Vulnerability scans Pentesten Patchmanagement 		
12.6.1.b Krijgt de gemeente kwetsbaarheidswaarschuwingen van de IBD	Ja		
12.6.1.c Zijn de laatste (beveiligings)patches geïnstalleerd en worden deze volgens een	Ja		

patchmanagement proces doorgevoerd?			
12.6.1.d Worden de penetratietests periodiek uitgevoerd?	Ja		
12.6.1.e Worden de vulnerability assessments (security scans) periodiek uitgevoerd?	Ja		

BIG hoofdstuk 13: Beheer van informatiebeveiligingsincidenten

13.1 Rapportage van informatiebeveiligingsgebeurtenissen en zwakke plekken

13.1.1 Rapportage van informatiebeveiligingsgebeurtenissen

Vraag	Antwoord	Advies	Evaluatie en impact
13.1.1.a Is er een incident management procedure?	Ja		
Zijn een reactie- en escalatieprocedure en een registratiesysteem onderdeel van de incident management procedure?	Ja		

13.1.2 Rapportage van zwakke plekken in de beveiliging

Vraag	Antwoord	Advies	Evaluatie en impact
13.1.2.a Kent iedereen zijn/haar verantwoordelijkheden met betrekking tot het melden van verdachte zwakke plekken met betrekking tot informatiebeveiliging?	Ja		
Is er een integriteitsprotocol?	Ja		
Is de procedure met betrekking tot het melden van verdachte en zwakke plekken met betrekking tot informatiebeveiliging bij iedereen bekend?	Ja		

13.2 Beheer van informatiebeveiligingsincidenten en verbeteringen

13.2.1 Verantwoordelijkheden en procedures

Vraag	Antwoord	Advies	Evaluatie en impact
13.2.1.a Is in de incident management procedure ook aandacht besteed aan de reactie op een incident?	Ja		
13.2.1.b Is de incident management procedure bekend bij alle verantwoordelijken?	Ja		
13.2.1.c Is in de incident management procedure aandacht voor de afhandeling/reactie van een incident?	Ja		

13.2.2. Leren van informatiebeveiligingsincidenten

Vraag	Antwoord	Advies	Evaluatie en impact
13.2.2.a Wordt er lering getrokken uit informatiebeveiligingsincidenten?	Ja		
Worden de incidenten opgenomen in de PDCA cyclus?	Nee		

13.2.3 Verzamelen van bewijsmateriaal

Vraag	Antwoord	Advies	Evaluatie en impact
13.2.3.a Wordt er rekening gehouden met het verzamelen van bewijsmateriaal als er een incident opgetreden is?	Ja		

BIG hoofdstuk 14: Bedrijfscontinuïteitsbeheer

14.1 Informatiebeveiligingsaspecten van bedrijfscontinuïteitsbeheer

14.1.1 Informatiebeveiliging opnemen in het proces van bedrijfscontinuïteitsbeheer

Vraag	Antwoord	Advies	Evaluatie en impact
14.1.1.a Is er een vastgesteld Calamiteitenplan (of Bedrijfscontinuïteitsplan) met daarin expliciet aandacht voor de continuïteit van processen en diensten bij uitval van IT Systemen en andere infrastructurele voorzieningen?	Nee	Er behoort een beheerd proces voor bedrijfscontinuïteit in de gehele organisatie te worden ontwikkeld en bijgehouden, voor de naleving van eisen voor informatiebeveiliging die nodig zijn voor de continuïteit van de bedrijfsvoering.	1. Betreft de vraag wetgeving? Indien ja, dan moet ik het implementeren. 2. Wat is het risico wanneer ik dit niet implementeer (kans x impact)? 3. Wat kost het ons als het risico manifest wordt? 4. Wat kost het om te implementeren? Dient deze control geïmplementeerd te worden en met welke prioriteit?

14.1.2 Bedrijfscontinuïteit en risicobeoordeling

Vraag	Antwoord	Advies	Evaluatie en impact
14.1.2.a Is voor alle (kritische) processen een BIA uitgevoerd, dat inzicht geeft in de afhankelijkheden van het proces of de dienst van de IT systemen en de (financiële) gevolgen bij uitval daarvan?	Nee	Gebeurtenissen die tot onderbreking van bedrijfsprocessen kunnen leiden, behoren te worden geïdentificeerd, tezamen met de waarschijnlijkheid en de gevolgen van dergelijke onderbrekingen en hun gevolgen voor informatiebeveiliging.	1. Betreft de vraag wetgeving? Indien ja, dan moet ik het implementeren. 2. Wat is het risico wanneer ik dit niet implementeer (kans x impact)? 3. Wat kost het ons als het risico manifest wordt? 4. Wat kost het om te implementeren? Dient deze control geïmplementeerd te worden en met welke prioriteit?

14.1.3 Continuïteitsplannen ontwikkelen en implementeren waaronder informatiebeveiliging

Vraag	Antwoord	Advies	Evaluatie en impact
14.1.3.a Is er een vastgesteld Continuïteitsplan (voor het handhaven van de beschikbaarheid van systemen, dan wel het binnen de	Ja		

afgesproken tijd weer opbrengen van IT systemen in het geval van ernstige verstoringen)?			
Kunt u aangeven voor welke systemen en processen u een vastgesteld Continuïteitsplan heeft?	<ul style="list-style-type: none"> Voor wat betreft BRP Voor wat betreft de dienstverlening van de BRP Voor wat betreft BAG 		
14.1.3.b Wordt er voor BRP rekening gehouden met de tijd tussen de laatste back-up en een mogelijk herstel?	Ja		
14.1.3.c Is het voor de BRP specifiek mogelijk dat er een volledige reconstructie mogelijk is binnen 24 uur?	Ja		

14.1.4 Kader voor de bedrijfscontinuïteitsplanning

Vraag	Antwoord	Advies	Evaluatie en impact
14.1.4.a Is er beleid en zijn er richtlijnen vastgesteld voor het vormgeven van de concrete continuïteitsplannen?	Nee	Er behoort een enkelvoudig kader voor bedrijfscontinuïteitsplannen te worden gehandhaafd om te bewerkstelligen dat alle plannen consistent zijn, om eisen voor informatiebeveiliging op consistente wijze te behandelen en om prioriteiten vast te stellen voor testen en onderhoud.	<p>1. Betreft de vraag wetgeving? Indien ja, dan moet ik het implementeren.</p> <p>2. Wat is het risico wanneer ik dit niet implementeer (kans x impact)?</p> <p>3. Wat kost het ons als het risico manifest wordt?</p> <p>4. Wat kost het om te implementeren? Dient deze control geïmplementeerd te worden en met welke prioriteit?</p>

14.1.5 Testen, onderhoud en herbeoordelen van continuïteitsplannen

Vraag	Antwoord	Advies	Evaluatie en impact
14.1.5.a Worden continuïteitsplannen jaarlijks getest of ze actueel en doeltreffend blijven?	Ja		
Kunt u aangeven voor welke systemen de continuïteitsplannen	<ul style="list-style-type: none"> Alleen voor BRP 		

worden getest?			
----------------	--	--	--

BIG hoofdstuk 15: Naleving

15.1 Naleving van wettelijke voorschriften

15.1.1 Identificatie van toepasselijke wetgeving

Vraag	Antwoord	Advies	Evaluatie en impact
<p>15.1.1.a Heeft de gemeente voor de inrichting en uitvoering van processen / informatiesystemen geregeld dat wordt voldaan aan alle voor IB relevante wet- en regelgeving en contractuele afspraken?</p> <p>Kunt u aangeven aan welke IB relevante wet- en regelgeving wordt voldaan en waarvoor er contractuele afspraken zijn gemaakt?</p>	<p>Ja</p> <ul style="list-style-type: none"> • WBP • PUN • SUW • BRP • BAG • BGT • DigiD • Beveiligingsrichtlijnen voor web applicaties • WABB • BIG 		

15.1.2 Intellectuele eigendomsrechten (Intellectual Property Rights (IPR))

Vraag	Antwoord	Advies	Evaluatie en impact
15.1.2.a Controleert uw organisatie actief op het illegaal gebruik van bedrijfsmiddelen?	Ja		

15.1.3 Bescherming van bedrijfsdocumenten

Vraag	Antwoord	Advies	Evaluatie en impact
15.1.3.a Wordt opslag en archivering van registraties / dossiers volgens vastgesteld beleid uitgevoerd?	Nee	<p>Registraties behoren te worden gecategoriseerd naar type, bijvoorbeeld boekhoudkundige registraties, database-records, transactielogbestanden, auditlogbestanden en operationele procedures. Bij elk type behoort de bewaartermijn en het type opslagmedium te worden</p>	<p>1. Betreft de vraag wetgeving? Indien ja, dan moet ik het implementeren.</p> <p>2. Wat is het risico wanneer ik dit niet implementeer (kans x impact)?</p> <p>3. Wat kost het ons als het risico manifest wordt?</p> <p>4. Wat kost het om te</p>

		<p>Vermeld, bijvoorbeeld papier, microfiche, magnetische of optische opslag. Enige cryptografische sleutels of programmatuur die verband houden met versleutelde archieven of digitale handtekeningen (zie 12.3) behoren ook te worden bewaard om ontcijfering van de registraties mogelijk te maken gedurende de bewaarperiode van de registraties</p>	<p>implementeren? Dient deze control geïmplementeerd te worden en met welke prioriteit?</p>
--	--	---	---

15.1.4 Bescherming van gegevens en geheimhouding van persoonsgegevens

Vraag	Antwoord	Advies	Evaluatie en impact
15.1.4.a Wordt de bescherming van gegevens en privacy bewerkstelligd overeenkomstig relevante wetgeving, regelgeving en voorschriften en indien van toepassing contractuele bepalingen?	Ja, middels Privacy functionaris		

15.1.5 Voorkomen van misbruik van ICT-voorzieningen

Vraag	Antwoord	Advies	Evaluatie en impact
15.1.5.a Hoe regelt / bevordert de gemeente het correct gebruik van IT voorzieningen en Informatie?	<ul style="list-style-type: none"> • Procedureel met instructie • Bewustwordingsacties 		

15.1.6 Voorschriften voor het gebruik van cryptografische beheersmaatregelen

Vraag	Antwoord	Advies	Evaluatie en impact
<p>15.1.6.a Worden cryptografische beheersmaatregelen toegepast in overeenstemming met relevante wetten en voorschriften?</p> <p>Kunt u aangeven volgens welke wetten en voorschriften de cryptografische beheersmaatregelen worden toegepast?</p>	<p>Ja</p> <ul style="list-style-type: none"> • Volgens de ICT-beveiligingsrichtlijnen voor webapplicaties van het NCSC • Volgens SUWI • Volgens BRP 		

	<ul style="list-style-type: none"> Conform de pas-toe-of-leg-uit lijst van het forum standaardisatie 		
--	---	--	--

15.2 Naleving van beveiligingsbeleid en -normen en controle op technische naleving

15.2.1 Naleving van beveiligingsbeleid en -normen

Vraag	Antwoord	Advies	Evaluatie en impact
15.2.1.a Hoe ziet het verantwoordelijke (lijn) management er op toe dat de IB maatregelen afgeleid van het IB beleid worden uitgevoerd? Dit is Suwi en een BRP en PUN eis.	<ul style="list-style-type: none"> Door middel van P&C rapportages Door middel van interne controle Door middel van self assessments Door middel van audits 		

15.2.2 Controle op technische naleving

Vraag	Antwoord	Advies	Evaluatie en impact
15.2.2.a Zorgen lijnmanagers en proceseigenaren dat de voor hun relevante informatiesystemen jaarlijks onderzocht worden op zwakheden door het laten uitvoeren van penetratietesten en kwetsbaarheidsanalyses?	Nee	<p>Informatiesystemen behoren regelmatig te worden gecontroleerd op naleving van implementatie van beveiligingsnormen. Penetratieproeven en kwetsbaarheidsbeoordelingen geven een momentopname van een systeem in een bepaalde toestand op een bepaald tijdstip. De momentopname blijft beperkt tot die delen van het systeem die werkelijk zijn getest tijdens de penetratiepoging(en). Penetratieproeven en kwetsbaarheidsbeoordelingen zijn geen vervanging van een risicobeoordeling.</p>	<p>1. Betreft de vraag wetgeving? Indien ja, dan moet ik het implementeren.</p> <p>2. Wat is het risico wanneer ik dit niet implementeer (kans x impact)?</p> <p>3. Wat kost het ons als het risico manifest wordt?</p> <p>4. Wat kost het om te implementeren?</p> <p>Dient deze control geïmplementeerd te worden en met welke prioriteit?</p>
Kunt u aangeven voor welke systemen dit wordt gedaan?	Niet van toepassing		
15.2.2.b Zijn de relevante afgegeven TPM-verklaringen niet ouder dan 1 jaar?	Ja		

15.3 Overwegingen bij audits van informatiesystemen

15.3.1 Beheersmaatregelen voor audits van informatiesystemen

Vraag	Antwoord	Advies	Evaluatie en impact
15.3.1.a Worden technische audits en andere technische onderzoeksactiviteiten zo gepland, goedgekeurd en uitgevoerd dat het risico op verstoring van bedrijfsactiviteiten tot een minimum wordt beperkt?	Ja		

15.3.2 Bescherming van hulpmiddelen voor audits van informatiesystemen

Vraag	Antwoord	Advies	Evaluatie en impact
15.3.2.a Worden hulpmiddelen voor audits van informatiesystemen beschermd tegen misbruik en compromittering?	Ja		