sorteersleutel	Compleet	Suwi	Audit	BRP	BAG	Faciltair	HRM	Inkoop	Categorie	Sub-Categorie	Vraag
3	i800.79687								Vragenlijst BIG hs 3: Implementatie van de Tactische Baseline	Vragen hs 3.1 Benoem verantwoordelijkheden	3.1.a Is er een integraal implementatieplan?
4	i800.79689								Vragenlijst BIG hs 3: Implementatie van de Tactische Baseline	Vragen hs 3.1 Benoem verantwoordelijkheden	Wordt er periodiek gerapporteerd over de voortgang?
5	i800.79690								Vragenlijst BIG hs 3: Implementatie van de Tactische Baseline	Vragen hs 3.1 Benoem verantwoordelijkheden	3.1.b Is er een Information Security Management System – (ISMS) waar het plan een onderdeel van is?
7	i800.96506								Vragenlijst hs 4: Samenwerkingsverbanden	Vragen hs 4.1 Risicobeoordeling en risicoafweging	4.1.a Is er met alle samenwerkingsverbanden gemeenschappelijke norm afgesproken zoals de BIG die op gemeenten van toepassing is?
8	i800.96507								Vragenlijst hs 4: Samenwerkingsverbanden	Vragen hs 4.1 Risicobeoordeling en risicoafweging	4.1.b Zijn er met deze samenwerkingsverbanden afspraken gemaakt over de jaarlijkse verantwoording over informatieveiligheid?
10	i800.96508								Vragenlijst hs 4: Samenwerkingsverbanden	Vragen hs 4.1 Risicobeoordeling en risicoafweging	4.1.d Is er ook een vorm van rapportage afgesproken met de samenwerkingsverbanden over de mate waarin zij in control zijn op informatieveiligheid?
12	i800.79691	i800.79691	i800.79691	i800.79691					Vragenlijst BIG hs 5: Beveiligingsbeleid	Vragen hs 5.1: Informatiebeveiligingsbeleid	5.1.1.a Is er een actueel informatiebeveiligingsbeleid (gebaseerd op de BIG)?
13	i800.79692	i800.79692	i800.79692	i800.79692					Vragenlijst BIG hs 5: Beveiligingsbeleid	Vragen hs 5.1: Informatiebeveiligingsbeleid	Is het informatiebeveiligingsbeleid vastgesteld door het College?
14	i800.79693	i800.79693	i800.79693	i800.79693					Vragenlijst BIG hs 5: Beveiligingsbeleid	Vragen hs 5.1: Informatiebeveiligingsbeleid	Is het informatiebeveiligingsbeleid jonger dan drie jaar?
15	i800.79694	i800.79694	i800.79694	i800.79694					Vragenlijst BIG hs 5: Beveiligingsbeleid	Vragen hs 5.1: Informatiebeveiligingsbeleid	Is het informatiebeveiligingsbeleid gepubliceerd en kenbaar gemaakt aan alle medewerkers en externe partijen?

16	i800.79697	i800.79697		i800.79697					Vragenlijst BIG hs 5: Beveiligingsbeleid	Vragen hs 5.1: Informatiebeveiligingsbeleid	5.1.1.b Is er in het gemeentelijk informatiebeveiligingsbeleid expliciet aandacht voor speciale gemeentelijke voorzieningen en wetgeving?
17	i800.79698	i800.79698	i800.79698	i800.79698					Vragenlijst BIG hs 5: Beveiligingsbeleid	Vragen hs 5.1: Informatiebeveiligingsbeleid	Kunt u aangeven voor welke voorzieningen en wetgeving er expliciet aandacht is in het informatiebeveiligingsbeleid?
18	i800.79699			i800.79699					Vragenlijst BIG hs 5: Beveiligingsbeleid	Vragen hs 5.1: Informatiebeveiligingsbeleid	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?
20	i800.79700	i800.79700	i800.79700						Vragenlijst BIG hs 5: Beveiligingsbeleid	Vragen hs 5.1: Informatiebeveiligingsbeleid	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?
22	i800.79638	i800.79638	i800.79638	i800.79638					Vragenlijst BIG hs 6: Organisatie van de informatiebeveiliging	Vragen hs 6.1: Interne organisatie	6.1.1.a Worden de informatiebeveiligingsdoelstellingen vastgesteld door het College?
23	i800.79770	i800.79770	i800.79770	i800.79770					Vragenlijst BIG hs 6: Organisatie van de informatiebeveiliging	Vragen hs 6.1: Interne organisatie	Wordt de voortgang jaarlijks besproken tussen bestuur en management?
24	i800.79771	i800.79771	i800.79771	i800.79771					Vragenlijst BIG hs 6: Organisatie van de informatiebeveiliging	Vragen hs 6.1: Interne organisatie	Wordt er over de voortgang gerapporteerd?
26	i800.79639	i800.79639	i800.79639						Vragenlijst BIG hs 6: Organisatie van de informatiebeveiliging	Vragen hs 6.1: Interne organisatie	6.1.2. a Zijn de informatiebeveiligingsactiviteiten vastgesteld en belegd?
27	i800.80114	i800.80114	i800.80114						Vragenlijst BIG hs 6: Organisatie van de informatiebeveiliging	Vragen hs 6.1: Interne organisatie	Door welke vertegenwoordigers/rollen worden de informatiebeveiligingsactiviteiten (op alle niveaus) uitgevoerd binnen de organisatie?
28	i800.79649	i800.79649	i800.79649						Vragenlijst BIG hs 6: Organisatie van de informatiebeveiliging	Vragen hs 6.1: Interne organisatie	Kunt u aangeven op welke wijze er intern verantwoording wordt afgelegd over de informatiebeveiligingsactiviteiten?

30	i800.79640	i800.79640	i800.79640						Vragenlijst BIG hs 6: Organisatie van de informatiebeveiliging	Vragen hs 6.1: Interne organisatie	6.1.3 a Zijn de beveiligingsrollen voor wat betreft informatiebeveiliging van de (lijn, proces, systeem) manager belegd?
32	i800.79641								Vragenlijst BIG hs 6: Organisatie van de informatiebeveiliging	Vragen hs 6.1: Interne organisatie	6.1.4.a Is er geïmplementeerd beleid voor het goedkeuren van nieuwe ICT-voorzieningen?
33	i800.80115								Vragenlijst BIG hs 6: Organisatie van de informatiebeveiliging	Vragen hs 6.1: Interne organisatie	Is er aandacht voor beveiliging binnen dit proces?
35	i800.79642	i800.79642		i800.79642			i800.79642		Vragenlijst BIG hs 6: Organisatie van de informatiebeveiliging	Vragen hs 6.1: Interne organisatie	6.1.5.a Is er een beleid om de geheimhoudingsverklaring te laten tekenen bij een aanstelling?
36	i800.79643	i800.79643		i800.79643			i800.79643		Vragenlijst BIG hs 6: Organisatie van de informatiebeveiliging	Vragen hs 6.1: Interne organisatie	Kunt u aangeven op welke wijze dit gebeurt?
38	i800.79644								Vragenlijst BIG hs 6: Organisatie van de informatiebeveiliging	Vragen hs 6.1: Interne organisatie	6.1.6 a Worden er contacten onderhouden in relatie tot informatiebeveiliging met relevante (overheids) organisaties en is dit vastgelegd?
39	i800.79645								Vragenlijst BIG hs 6: Organisatie van de informatiebeveiliging	Vragen hs 6.1: Interne organisatie	Kunt u aangeven met welke instanties er contacten worden onderhouden?
41	i800.79646	i800.79646							Vragenlijst BIG hs 6: Organisatie van de informatiebeveiliging	Vragen hs 6.1: Interne organisatie	6.1.7.a Onderhoud de gemeente contacten met relevante expertise groepen en leveranciers om in geval van incidenten snel/juist te kunnen handelen?
42	i800.79647	i800.79647							Vragenlijst BIG hs 6: Organisatie van de informatiebeveiliging	Vragen hs 6.1: Interne organisatie	Kunt u aan geven met welke expertisegroepen uw gemeenten contacten onderhoudt?
44	i800.79648	i800.79648		i800.79648					Vragenlijst BIG hs 6: Organisatie van de informatiebeveiliging	Vragen hs 6.1: Interne organisatie	6.1.8.a Wordt het informatiebeveiligingsbeleid onafhankelijk beoordeeld en wordt hierover intern verantwoording afgelegd?
45	i800.79774	i800.79774							Vragenlijst BIG hs 6: Organisatie van de informatiebeveiliging	Vragen hs 6.1: Interne organisatie	6.1.8.b Wordt over het functioneren van informatiebeveiliging verantwoording afgelegd aan de gemeenteraad?

46	i800.79775	i800.79775							Vragenlijst BIG hs 6: Organisatie van de informatiebeveiliging	Vragen hs 6.1: Interne organisatie	6.1.8.c Heeft u een sluitende IB-verantwoording ingericht binnen uw gemeente?
47	i800.79776	i800.79776							Vragenlijst BIG hs 6: Organisatie van de informatiebeveiliging	Vragen hs 6.1: Interne organisatie	Vraagt u jaarlijks van uw directeuren / afdelingshoofden / samenwerkingsverbanden om een in control verklaring over de op hun van toepassing zijnde maatregelen?
49	i800.79650	i800.79650		i800.79650					Vragenlijst BIG hs 6: Organisatie van de informatiebeveiliging	Vragen hs 6.2: Externe partijen	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?
50	i800.79651	i800.79651							Vragenlijst BIG hs 6: Organisatie van de informatiebeveiliging	Vragen hs 6.2: Externe partijen	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?
51	i800.79652	i800.79652							Vragenlijst BIG hs 6: Organisatie van de informatiebeveiliging	Vragen hs 6.2: Externe partijen	6.2.1.c Als er uitbesteed is, zijn er dan beveiligingsmaatregelen vastgelegd in de (inkoop) contracten?
52	i800.79653	i800.79653							Vragenlijst BIG hs 6: Organisatie van de informatiebeveiliging	Vragen hs 6.2: Externe partijen	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?
53	i800.79654	i800.79654							Vragenlijst BIG hs 6: Organisatie van de informatiebeveiliging	Vragen hs 6.2: Externe partijen	Kunt u aangeven op welke wijze de afspraken zijn gemaakt?
54	i800.79655	i800.79655							Vragenlijst BIG hs 6: Organisatie van de informatiebeveiliging	Vragen hs 6.2: Externe partijen	6.2.1.e Als er persoonsgegevens verwerkt worden, is er dan een wettelijke grondslag en is doelbinding en proportionaliteit gewaarborgd?
55	i800.79656	i800.79656							Vragenlijst BIG hs 6: Organisatie van de informatiebeveiliging	Vragen hs 6.2: Externe partijen	6.2.1.f Is in deze contracten opgenomen dat een leverancier verplicht is om binnen 24 uur alle beveiligingsinbreuken te melden? (WBP-eis).
56	i800.79657	i800.79657		i800.79657					Vragenlijst BIG hs 6: Organisatie van de informatiebeveiliging	Vragen hs 6.2: Externe partijen	6.2.1.g Worden de aan de leverancier opgelegde informatiebeveiligingsmaatregelen jaarlijks gecontroleerd?

57	i800.79658	i800.79658							Vragenlijst BIG hs 6: Organisatie van de informatiebeveiliging	Vragen hs 6.2: Externe partijen	6.2.1.h Worden de rapportages over leveranciers verwerkt in de Collegeverklaring?
58	i800.79659	i800.79659							Vragenlijst BIG hs 6: Organisatie van de informatiebeveiliging	Vragen hs 6.2: Externe partijen	6.2.1.i Worden de rapportages over leveranciers verwerkt in de Collegeverklaring?
60	i800.79660								Vragenlijst BIG hs 6: Organisatie van de informatiebeveiliging	Vragen hs 6.2: Externe partijen	6.2.2.a Wordt aan externe medewerkers pas toegang verleend tot informatie en of bedrijfsmiddelen nadat alle beveiligingseisen geïmplementeerd zijn?
61	i800.79661								Vragenlijst BIG hs 6: Organisatie van de informatiebeveiliging	Vragen hs 6.2: Externe partijen	6.2.2.b Is dat ook vastgesteld en vastgelegd en uitgewerkt in de contracten?
63	i800.79662	i800.79662							Vragenlijst BIG hs 6: Organisatie van de informatiebeveiliging	Vragen hs 6.2: Externe partijen	6.2.3.a Zijn alle ontdekte beveiligingsmaatregelen uit de risicoafweging vastgelegd en geïmplementeerd voordat het product of de dienst in werking gezet wordt?
64	i800.79663	i800.79663							Vragenlijst BIG hs 6: Organisatie van de informatiebeveiliging	Vragen hs 6.2: Externe partijen	Welke van de volgende onderwerpen zijn vastgelegd en geregeld in formele contracten bij de uitbesteding dan wel ontwikkeling van software?
65	i800.79664	i800.79664							Vragenlijst BIG hs 6: Organisatie van de informatiebeveiliging	Vragen hs 6.2: Externe partijen	6.2.3.b Is in contracten vastgelegd hoe wordt omgegaan met wijzigingsbeheer?
66	i800.79665	i800.79665							Vragenlijst BIG hs 6: Organisatie van de informatiebeveiliging	Vragen hs 6.2: Externe partijen	6.2.3.c Is in contracten met externe leveranciers de aansprakelijkheid uitgewerkt?
67	i800.79666	i800.79666							Vragenlijst BIG hs 6: Organisatie van de informatiebeveiliging	Vragen hs 6.2: Externe partijen	6.2.3.d Worden leverancierseisen doorvertaald naar onderaannemers?
68	i800.79667	i800.79667							Vragenlijst BIG hs 6: Organisatie van de informatiebeveiliging	Vragen hs 6.2: Externe partijen	6.2.3.e Is in contracten vastgelegd hoe er wordt omgegaan met geheimhouding?
70	i800.79702	i800.79702							Vragenlijst BIG hs 7: Beheer van bedrijfsmiddelen	Vragen hs 7.1: Beheer van bedrijfsmiddelen	7.1.1.a Is er een actuele registratie van bedrijfsmiddelen?
71	i800.79703	i800.79703							Vragenlijst BIG hs 7: Beheer van bedrijfsmiddelen	Vragen hs 7.1: Beheer van bedrijfsmiddelen	Kunt u aangevenvoor welke bedrijfsmiddelen er een actuele registratie is?
73	i800.79705			i800.79705					Vragenlijst BIG hs 7: Beheer van bedrijfsmiddelen	Vragen hs 7.1: Beheer van bedrijfsmiddelen	7.1.2.a Is er voor elk bedrijfsproces, applicatie, gegevensverzameling en ICT-faciliteit een verantwoordelijke lijnmanager?
74	i800.79706			i800.79706					Vragenlijst BIG hs 7: Beheer van bedrijfsmiddelen	Vragen hs 7.1: Beheer van bedrijfsmiddelen	Is de verantwoordelijke lijnmanger formeel vastgesteld?

76	i800.79708			i800.79708					Vragenlijst BIG hs 7: Beheer van bedrijfsmiddelen	Vragen hs 7.1: Beheer van bedrijfsmiddelen	7.1.3.a Zijn er regels opgesteld voor het juist gebruiken van (ICT-)bedrijfsmiddelen?
78	i800.79710	i800.79710							Vragenlijst BIG hs 7: Beheer van bedrijfsmiddelen	Vragen hs 7.2: Classificatie van informatie	7.2.1.a Zijn er rubricerings- of classificatierichtlijnen opgesteld binnen de gemeente?
79	i800.79711	i800.79711							Vragenlijst BIG hs 7: Beheer van bedrijfsmiddelen	Vragen hs 7.2: Classificatie van informatie	Zijn de richtlijnen opgesteld op basis van het BIG-OP product dataclassificatie?
80	i800.79712	i800.79712							Vragenlijst BIG hs 7: Beheer van bedrijfsmiddelen	Vragen hs 7.2: Classificatie van informatie	Zijn de essentiële gegevensverzamelingen binnen de gemeenten allen geclassificeerd volgens deze richtlijnen?
82	i800.79714	i800.79714							Vragenlijst BIG hs 7: Beheer van bedrijfsmiddelen	Vragen hs 7.2: Classificatie van informatie	7.2.2.a Worden er procedures ontwikkeld op basis van uitgevoerde dataclassificaties, zodat informatie het juiste niveau van bescherming krijgt?
83	i800.79715	i800.79715							Vragenlijst BIG hs 7: Beheer van bedrijfsmiddelen	Vragen hs 7.2: Classificatie van informatie	7.2.2.b Worden de ontwikkelde procedures ook gevolgd?
84	i800.79716	i800.79716							Vragenlijst BIG hs 7: Beheer van bedrijfsmiddelen	Vragen hs 7.2: Classificatie van informatie	Geldt dat ook voor de primaire processen/systemen?
86	i800.79718	i800.79718		i800.79718			i800.79718		Vragenlijst BIG hs 8: Personele beveiliging	Vragen hs 8.1: Voorafgaand aan het dienstverband	8.1.1.a Zijn de rollen en verantwoordelijkheden van werknemers, ingehuurd personeel en externe gebruikers met betrekking tot informatiebeveiliging vastgelegd?
87	i800.79719	i800.79719		i800.79719			i800.79719		Vragenlijst BIG hs 8: Personele beveiliging	Vragen hs 8.1: Voorafgaand aan het dienstverband	Kunt u aangeven met betrekking tot welke van de hiernaast genoemde opties dit wordt vastgelegd en gecommuniceerd?
89	i800.79721	i800.79721					i800.79721		Vragenlijst BIG hs 8: Personele beveiliging	Vragen hs 8.1: Voorafgaand aan het dienstverband	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?
90	i800.79724	i800.79724					i800.79724		Vragenlijst BIG hs 8: Personele beveiliging	Vragen hs 8.1: Voorafgaand aan het dienstverband	Worden deze controles periodiek herhaald?
91	i800.79723	i800.79723					i800.79723		Vragenlijst BIG hs 8: Personele beveiliging	Vragen hs 8.1: Voorafgaand aan het dienstverband	Worden de gegevens die de medewerker opgeeft geverifieerd?
92	i800.79722	i800.79722					i800.79722		Vragenlijst BIG hs 8: Personele beveiliging	Vragen hs 8.1: Voorafgaand aan het dienstverband	Is voor alle medewerkers minimaal een VOG vereist?
94	i800.79726						i800.79726		Vragenlijst BIG hs 8: Personele beveiliging	Vragen hs 8.1: Voorafgaand aan het dienstverband	8.1.3.a Hebben de werknemers, ingehuurd personeel en externe gebruikers de voorwaarden met betrekking tot hun verantwoordelijkheden ten aanzien van informatiebeveiliging en privacyeisen, specifiek ter kennisname gekregen en aanvaard?

96	i800.79728			i800.79728					Vragenlijst BIG hs 8: Personele beveiliging	Vragen hs 8.2: Tijdens het dienstverband	8.2.1.a Bevordert en controleert het lijnmanagement dat gemeenteambtenaren, ingehuurd personeel en externe gebruikers zich houden aan de beveiligingsregels overeenkomstig het beleid en de procedures van de organisatie?
97	i800.79729			i800.79729					Vragenlijst BIG hs 8: Personele beveiliging	Vragen hs 8.2: Tijdens het dienstverband	Waaruit blijkt dat?
99	i800.79731	i800.79731	i800.79731	i800.79731			i800.79731	i800.79731	Vragenlijst BIG hs 8: Personele beveiliging	Vragen hs 8.2: Tijdens het dienstverband	8.2.2.a Zorgt het management ervoor dat de medewerkers voldoende kennis en bewustzijn hebben op het gebied van informatiebeveiliging?
100	i800.79732	i800.79732	i800.79732	i800.79732			i800.79732	i800.79732	Vragenlijst BIG hs 8: Personele beveiliging	Vragen hs 8.2: Tijdens het dienstverband	Hoe zorgt het management hier voor?
101	i800.79733	i800.79733	i800.79733	i800.79733			i800.79733	i800.79733	Vragenlijst BIG hs 8: Personele beveiliging	Vragen hs 8.2: Tijdens het dienstverband	Zijn hier verslagen van?
102	i800.79734	i800.79734	i800.79734	i800.79734			i800.79734	i800.79734	Vragenlijst BIG hs 8: Personele beveiliging	Vragen hs 8.2: Tijdens het dienstverband	Zijn er voldoende middelen gealloceerd voor het bevorderen van kennis en bewustwording van de medewerkers ten aanzien van informatieveiligheid?
104	i800.79736	i800.79736		i800.79736			i800.79736		Vragenlijst BIG hs 8: Personele beveiliging	Vragen hs 8.2: Tijdens het dienstverband	8.2.3.a Is er een disciplinair proces vastgelegd, conform CAR/UWO, voor werknemers die inbreuk maken op het informatiebeveiligingsbeleid?
106	i800.79738	i800.79738					i800.79738		Vragenlijst BIG hs 8: Personele beveiliging	Vragen hs 8.3: Beëindiging of wijziging van het dienstverband	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?
107	i800.97202	i800.97202							Vragenlijst BIG hs 8: Personele beveiliging	Vragen hs 8.3: Beëindiging of wijziging van het dienstverband	8.3.1.b Worden toegangsrechten volgens de procedure ingetrokken als het dienstverband wijzigt dan wel eindigt?
109	i800.79740			i800.79740		i800.79740			Vragenlijst BIG hs 9: Fysieke beveiliging en beveiliging van de omgeving	Vragen hs 9.1: Beveiligde ruimten	9.1.1.a Zijn er gepaste toegangsbeveiligingsmaatregelen genomen voor ruimtes waar zich informatie en ICT-voorzieningen bevinden?

110	i800.79741			i800.79741		i800.79741			Vragenlijst BIG hs 9: Fysieke beveiliging en beveiliging van de omgeving	Vragen hs 9.1: Beveiligde ruimten	Kunt u aangeven voor welke ruimtes er gepaste toegangsbeveiligingsmaatregelen zijn genomen?
111	i800.80116			i800.80116		i800.80116			Vragenlijst BIG hs 9: Fysieke beveiliging en beveiliging van de omgeving	Vragen hs 9.1: Beveiligde ruimten	Wordt hier mee voldaan aan artikel 91 van de PUN?
113	i800.79743	i800.79743		i800.79743		i800.79743			Vragenlijst BIG hs 9: Fysieke beveiliging en beveiliging van de omgeving	Vragen hs 9.1: Beveiligde ruimten	9.1.2. a Is de toegang tot de gebouwen en de beveiligde zones uitsluitend mogelijk voor geautoriseerde personen?
115	i800.79745	i800.79745		i800.79745		i800.79745			Vragenlijst BIG hs 9: Fysieke beveiliging en beveiliging van de omgeving	Vragen hs 9.1: Beveiligde ruimten	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.
116	i800.79746	i800.79746		i800.79746		i800.79746			Vragenlijst BIG hs 9: Fysieke beveiliging en beveiliging van de omgeving	Vragen hs 9.1: Beveiligde ruimten	Kunt u aangeven welke (beschermings) maatregelen er zijn getroffen?
118	i800.79748					i800.79748			Vragenlijst BIG hs 9: Fysieke beveiliging en beveiliging van de omgeving	Vragen hs 9.1: Beveiligde ruimten	9.1.4.a Zijn er verzekeringsmaatregelen genomen die bescherming bieden tegen schade door geweld van buiten?
119	i800.79749					i800.79749			Vragenlijst BIG hs 9: Fysieke beveiliging en beveiliging van de omgeving	Vragen hs 9.1: Beveiligde ruimten	Kunt u aangeven waartegen u bent verzekerd?
121	i800.79751			i800.79751		i800.79751			Vragenlijst BIG hs 9: Fysieke beveiliging en beveiliging van de omgeving	Vragen hs 9.1: Beveiligde ruimten	9.1.5.a Zijn er maatregelen en procedures geïmplementeerd voor het werken in en toezien op beveiligde ruimtes?
122	i800.79752			i800.79752		i800.79752			Vragenlijst BIG hs 9: Fysieke beveiliging en beveiliging van de omgeving	Vragen hs 9.1: Beveiligde ruimten	Kunt u aangeven waarvoor de maatregelen en procedures zijn geïmplementeerd?
124	i800.79754			i800.79754		i800.79754			Vragenlijst BIG hs 9: Fysieke beveiliging en beveiliging van de omgeving	Vragen hs 9.1: Beveiligde ruimten	9.1.6.a Zijn publiek toegankelijke ruimtes afgeschermd zodat onbevoegden zich geen toegang kunnen verschaffen tot bedrijfsmiddelen?
126	i800.79756					i800.79756			Vragenlijst BIG hs 9: Fysieke beveiliging en beveiliging van de omgeving	Vragen hs 9.2: Beveiliging van apparatuur	9.2.1.a Wordt apparatuur overeenkomstig de voorschriften geplaatst en gebruikt zodat het risico van schade, storing en onbevoegde toegang verminderd worden?
127	i800.79757					i800.79757			Vragenlijst BIG hs 9: Fysieke beveiliging en beveiliging van de omgeving	Vragen hs 9.2: Beveiliging van apparatuur	Kunt u aangeven waartegen de apparatuur wordt beschermd?
129	i800.79759					i800.79759			Vragenlijst BIG hs 9: Fysieke beveiliging en beveiliging van de omgeving	Vragen hs 9.2: Beveiliging van apparatuur	9.2.2.a Zijn er maatregelen en procedures geïmplementeerd om uitval van apparatuur te voorkomen door stroomuitval of onderbreking van de nutsvoorzieningen?
131	i800.79761					i800.79761			Vragenlijst BIG hs 9: Fysieke beveiliging en beveiliging van de omgeving	Vragen hs 9.2: Beveiliging van apparatuur	9.2.3.a Zijn de voedings- en telecommunicatiekabels aangelegd conform de NEN 1010?

133	i800.79763					i800.79763			Vragenlijst BIG hs 9: Fysieke beveiliging en beveiliging van de omgeving	Vragen hs 9.2: Beveiliging van apparatuur	9.2.4.a Zijn er procedures voor het beheerst en door bevoegde personen uit te laten voeren van technisch onderhoud aan IT apparatuur?
135	i800.79765			i800.79765			i800.79765		Vragenlijst BIG hs 9: Fysieke beveiliging en beveiliging van de omgeving	Vragen hs 9.2: Beveiliging van apparatuur	9.2.5.a Zijn er maatregelen en procedures geïmplementeerd voor apparatuur als er buiten de vertrouwde omgeving gewerkt wordt?
137	i800.79767					i800.79767			Vragenlijst BIG hs 9: Fysieke beveiliging en beveiliging van de omgeving	Vragen hs 9.2: Beveiliging van apparatuur	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?
139	i800.79769					i800.79769			Vragenlijst BIG hs 9: Fysieke beveiliging en beveiliging van de omgeving	Vragen hs 9.2: Beveiliging van apparatuur	9.2.7.a Is er voor gezorgd dat apparatuur, informatie en programmatuur niet zonder toestemming van de gebruikelijke (werk) locatie kan worden meegenomen?
141	i800.79780			i800.79780					Vragenlijst BIG hs 10: Beheer van Communicatie- en Bedieningsprocessen	Vragen hs 10.1: Bedieningsprocedures en -verantwoordelijkheden	10.1.1.a Zijn er actuele schriftelijke procedures voor het operationeel beheer (en gebruik) van de IT voorzieningen (software, hardware, netwerk, databases)?
142	i800.79783	i800.79783							Vragenlijst BIG hs 10: Beheer van Communicatie- en Bedieningsprocessen	Vragen hs 10.1: Bedieningsprocedures en -verantwoordelijkheden	10.1.1.b Wordt de Suwinetinfrastructuur, servers en netwerkcomponenten, gehardend volgens de vastgestelde configuratie baseline?
144	i800.79785	i800.79785							Vragenlijst BIG hs 10: Beheer van Communicatie- en Bedieningsprocessen	Vragen hs 10.1: Bedieningsprocedures en -verantwoordelijkheden	10.1.2.a Is er een vastgestelde procedure voor het beheerst uitvoeren van wijzigingen op de IT voorzieningen (een wijzigingsbeheerproces)?
145	i800.79786	i800.79786							Vragenlijst BIG hs 10: Beheer van Communicatie- en Bedieningsprocessen	Vragen hs 10.1: Bedieningsprocedures en -verantwoordelijkheden	Zijn hier ook verslagen van?
147	i800.79788	i800.79788	i800.79788	i800.79788			i800.79788		Vragenlijst BIG hs 10: Beheer van Communicatie- en Bedieningsprocessen	Vragen hs 10.1: Bedieningsprocedures en -verantwoordelijkheden	10.1.3.a Zijn de taken en verantwoordelijkheden voor het gebruik en het beheer van IT voorzieningen naar rato van de organisatiegrootte gescheiden?
148	i800.79827	i800.79827	i800.79827	i800.79827			i800.79827		Vragenlijst BIG hs 10: Beheer van Communicatie- en Bedieningsprocessen	Vragen hs 10.1: Bedieningsprocedures en -verantwoordelijkheden	Kunt u aangeven hoe de taken en verantwoordelijkheden voor het gebruik en het beheer van IT voorzieningen zijn gescheiden?

149	i800.79789	i800.79789	i800.79789	i800.79789			i800.79789		Vragenlijst BIG hs 10: Beheer van Communicatie- en Bedieningsprocessen	Vragen hs 10.1: Bedieningsprocedures en -verantwoordelijkheden	10.1.3.b Welke rollen en functiebenamingen zijn er belegd, dan wel aangewezen door het college?
150	i800.79790	i800.79790	i800.79790	i800.79790					Vragenlijst BIG hs 10: Beheer van Communicatie- en Bedieningsprocessen	Vragen hs 10.1: Bedieningsprocedures en -verantwoordelijkheden	10.1.3.c Is er sprake van een scheiding in verantwoordelijkheden tussen: uitvoerder en de beveiligingsfunctionaris en tussen opdrachtgever en de beveiligingsfunctionaris
152	i800.79793	i800.79793							Vragenlijst BIG hs 10: Beheer van Communicatie- en Bedieningsprocessen	Vragen hs 10.1: Bedieningsprocedures en -verantwoordelijkheden	10.1.4.a Wordt er in huis software ontwikkeld of getest?
153	i800.79794	i800.79794							Vragenlijst BIG hs 10: Beheer van Communicatie- en Bedieningsprocessen	Vragen hs 10.1: Bedieningsprocedures en -verantwoordelijkheden	Maakt u daarbij gebruik van een OTAP-omgeving?
155	i800.79796			i800.79796					Vragenlijst BIG hs 10: Beheer van Communicatie- en Bedieningsprocessen	Vragen hs 10.2: Exploitatie door een derde partij	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?

156	i800.79797			i800.79797					Vragenlijst BIG hs 10: Beheer van Communicatie- en Bedieningsprocessen	Vragen hs 10.2: Exploitatie door een derde partij	Kunt u aangeven waar deze beveiligingseisen op zijn gericht?
158	i800.79801			i800.79801					Vragenlijst BIG hs 10: Beheer van Communicatie- en Bedieningsprocessen	Vragen hs 10.2: Exploitatie door een derde partij	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?
159	i800.79872			i800.79872					Vragenlijst BIG hs 10: Beheer van Communicatie- en	Vragen hs 10.2: Exploitatie door een derde partij	Is er door de externe IT leveranchier een TPM opgeleverd?
161	i800.79803								Vragenlijst BIG hs 10: Beheer van Communicatie- en Bedieningsprocessen	Vragen hs 10.2: Exploitatie door een derde partij	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 ?
163	i800.79805	i800.79805							Vragenlijst BIG hs 10: Beheer van Communicatie- en Bedieningsprocessen	Vragen hs 10.3: Systeemplanning en –acceptatie	10.3.1.a Zijn er maatregelen getroffen waarmee de afgesproken actuele en toekomstig systeembelasting inzichtelijk en op voldoende niveau is?
165	i800.79807	i800.79807							Vragenlijst BIG hs 10: Beheer van Communicatie- en Bedieningsprocessen	Vragen hs 10.3: Systeemplanning en –acceptatie	10.3.2.a Is er een formele testprocedure voor accepteren van nieuwe en gewijzigde systemen (zowel door de gebruikersorganisatie als het beheer)?
167	i800.79809								Vragenlijst BIG hs 10: Beheer van Communicatie- en Bedieningsprocessen	Vragen hs 10.4: Bescherming tegen virussen en ‘mobile code’	10.4.1.a Welke antivirus maatregelen heeft u ingevoerd?

169	i800.79811								Vragenlijst BIG hs 10: Beheer van Communicatie- en Bedieningsprocessen	Vragen hs 10.4: Bescherming tegen virussen en 'mobile code'	10.4.2.a Welke maatregelen heeft u genomen tegen het onbedoeld of onbewust uitvoeren van ongewenste mobiele codes, zoals Java en Flash?
171	i800.79813			i800.79813	i800.79813				Vragenlijst BIG hs 10: Beheer van Communicatie- en Bedieningsprocessen	Vragen hs 10.5: Back-up	10.5.1.a Heeft u een actueel back-up beleid en worden back-ups dienovereenkomstig gemaakt, getest en opgeslagen?
172	i800.79814			i800.79814	i800.79814				Vragenlijst BIG hs 10: Beheer van Communicatie- en Bedieningsprocessen	Vragen hs 10.5: Back-up	Kunt u aangeven waarvoor u een actueel back-beleid heeft en waarvoor de back-ups worden gemaakt, getest en opgeslagen?
174	i800.79816	i800.79816		i800.79816					Vragenlijst BIG hs 10: Beheer van Communicatie- en Bedieningsprocessen	Vragen hs 10.6: Beheer van netwerkbeveiliging	10.6.1.a Welke maatregelen heeft u genomen om de aanwezige netwerken adequaat te monitoren en beveiligen?
175	i800.79818	i800.79818							Vragenlijst BIG hs 10: Beheer van Communicatie- en Bedieningsprocessen	Vragen hs 10.6: Beheer van netwerkbeveiliging	10.6.1.b Heeft u al deze maatregelen ook expliciet ingezet in het kader van telewerken in relatie tot BRP en Suwi?
177	i800.79820	i800.79820							Vragenlijst BIG hs 10: Beheer van Communicatie- en Bedieningsprocessen	Vragen hs 10.6: Beheer van netwerkbeveiliging	10.6.2.a Worden de beveiligingskenmerken, de niveaus van dienstverlening en de beheereisen vanuit systemen en processen doorvertaald naar de overeenkomsten voor netwerkdiensten?
179	i800.79822			i800.79822					Vragenlijst BIG hs 10: Beheer van Communicatie- en Bedieningsprocessen	Vragen hs 10.7: Behandeling van media	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 disken en backup tapes?
180	i800.79823			i800.79823					Vragenlijst BIG hs 10: Beheer van Communicatie- en Bedieningsprocessen	Vragen hs 10.7: Behandeling van media	Voldoet u hiermee aan artikel 91 van de PUN?

182	i800.79825								Vragenlijst BIG hs 10: Beheer van Communicatie- en Bedieningsprocessen	Vragen hs 10.7: Behandeling van media	10.7.2.a Heeft u procedures opgesteld voor verwijderen/vernietigen van informatie?
183	i800.79826								Vragenlijst BIG hs 10: Beheer van Communicatie- en Bedieningsprocessen	Vragen hs 10.7: Behandeling van media	Geldt dit ook voor verwijderbare media en het verwijderen van vertrouwelijke data (van harddisken)?
185	i800.79829								Vragenlijst BIG hs 10: Beheer van Communicatie- en Bedieningsprocessen	Vragen hs 10.7: Behandeling van media	10.7.3.a Zijn er procedures voor de behandeling en opslag van informatie?
186	i800.79830								Vragenlijst BIG hs 10: Beheer van Communicatie- en Bedieningsprocessen	Vragen hs 10.7: Behandeling van media	Kunt u aangeven welke procedures en regels er zijn?
188	i800.79833								Vragenlijst BIG hs 10: Beheer van Communicatie- en Bedieningsprocessen	Vragen hs 10.7: Behandeling van media	10.7.4.a Wordt systeem documentatie voldoende beschermd tegen onbevoegde toegang?
189	i800.79834								Vragenlijst BIG hs 10: Beheer van Communicatie- en Bedieningsprocessen	Vragen hs 10.7: Behandeling van media	Staat uw systeemdocumentatie op een logisch afgeschermde omgeving?
190	i800.79835								Vragenlijst BIG hs 10: Beheer van Communicatie- en Bedieningsprocessen	Vragen hs 10.7: Behandeling van media	Is uw systeemdocumentatie geclassificeerd en beveiligd met een wachtwoord?
192	i800.79837	i800.79837							Vragenlijst BIG hs 10: Beheer van Communicatie- en Bedieningsprocessen	Vragen hs 10.8: Uitwisseling van informatie	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?
193	i800.79838	i800.79838							Vragenlijst BIG hs 10: Beheer van Communicatie- en Bedieningsprocessen	Vragen hs 10.8: Uitwisseling van informatie	Kunt u aangeven waarvoor deze procedures en beleid gelden?
194	i800.79839	i800.79839							Vragenlijst BIG hs 10: Beheer van Communicatie- en Bedieningsprocessen	Vragen hs 10.8: Uitwisseling van informatie	Zijn de medewerkers geïnstrueerd over het beleid en procedures voor een beheerste en beveiligde wijze van informatie-uitwisseling?
196	i800.79841	i800.79841							Vragenlijst BIG hs 10: Beheer van Communicatie- en Bedieningsprocessen	Vragen hs 10.8: Uitwisseling van informatie	10.8.2.a Zijn er overeenkomsten afgesloten voor de beheerste en beveiligde wijze van informatie-uitwisseling met andere partijen?
197	i800.79842	i800.79842							Vragenlijst BIG hs 10: Beheer van Communicatie- en Bedieningsprocessen	Vragen hs 10.8: Uitwisseling van informatie	Kunt u aangeven welke van de hiernaast genoemde aspecten zijn meegenomen in de overeenkomst?
198	i800.79843	i800.79843							Vragenlijst BIG hs 10: Beheer van Communicatie- en Bedieningsprocessen	Vragen hs 10.8: Uitwisseling van informatie	Is de overeenkomst bij alle medewerkers bekend?
200	i800.79845	i800.79845							Vragenlijst BIG hs 10: Beheer van Communicatie- en Bedieningsprocessen	Vragen hs 10.8: Uitwisseling van informatie	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 disken en backup tapes maar ook lap-tops) vertrouwelijke informatie op een veilige wijze is opgeslagen?

202	i800.79847	i800.79847							Vragenlijst BIG hs 10: Beheer van Communicatie- en Bedieningsprocessen	Vragen hs 10.8: Uitwisseling van informatie	10.8.4.a Zijn er middelen waarmee vertrouwelijke informatie op adequate wijze is beveiligd bij uitwisseling via berichtenverkeer (bijvoorbeeld XML of e-mail)?
203	i800.79848	i800.79848							Vragenlijst BIG hs 10: Beheer van Communicatie- en Bedieningsprocessen	Vragen hs 10.8: Uitwisseling van informatie	Kunt u aangeven welke middelen hiervoor worden ingezet?
205	i800.79850								Vragenlijst BIG hs 10: Beheer van Communicatie- en Bedieningsprocessen	Vragen hs 10.8: Uitwisseling van informatie	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?
206	i800.79851								Vragenlijst BIG hs 10: Beheer van Communicatie- en Bedieningsprocessen	Vragen hs 10.8: Uitwisseling van informatie	Zijn de risico's in kaart gebracht?
207	i800.79852								Vragenlijst BIG hs 10: Beheer van Communicatie- en Bedieningsprocessen	Vragen hs 10.8: Uitwisseling van informatie	Zijn de onderlinge verbanden inzichtelijk gemaakt?
209	i800.79857	i800.79857							Vragenlijst BIG hs 10: Beheer van Communicatie- en Bedieningsprocessen	Vragen hs 10.9: Diensten voor e-commerce	10.9.1.a Heeft u maatregelen geïmplementeerd voor het beschermen van online transacties of voor het gebruik maken van beveiligde authenticatie mechanismen?
210	i800.79858	i800.79858							Vragenlijst BIG hs 10: Beheer van Communicatie- en Bedieningsprocessen	Vragen hs 10.9: Diensten voor e-commerce	Kunt u aangeven voor welk soort producten en diensten er maatregelen zin geïmplementeerd?
212	i800.79860								Vragenlijst BIG hs 10: Beheer van Communicatie- en Bedieningsprocessen	Vragen hs 10.9: Diensten voor e-commerce	10.9.3.a Heeft u maatregelen geïmplementeerd die er voor zorgen dat openbare informatie beschermd is tegen modificatie?
214	i800.79862	i800.79862	i800.79862	i800.79862					Vragenlijst BIG hs 10: Beheer van Communicatie- en Bedieningsprocessen	Vragen hs 10.10: Controle	10.10.1.a Worden systeemhandelingen gelogd, zodanig dat handelingen van gebruikers en beheerders kunnen worden geanalyseerd onder meer tbv een audittrail?

215	i800.79863	i800.79863	i800.79863	i800.79863					Vragenlijst BIG hs 10: Beheer van Communicatie- en Bedieningsprocessen	Vragen hs 10.10: Controle	Kunt u aangeven voor welke systemen er wordt gelogd?
216	i800.79864	i800.79864	i800.79864	i800.79864					Vragenlijst BIG hs 10: Beheer van Communicatie- en Bedieningsprocessen	Vragen hs 10.10: Controle	Worden storingen gelogd?
217	i800.79865	i800.79865	i800.79865	i800.79865					Vragenlijst BIG hs 10: Beheer van Communicatie- en Bedieningsprocessen	Vragen hs 10.10: Controle	Worden administratieve handelingen gelogd?
218	i800.79866	i800.79866	i800.79866	i800.79866					Vragenlijst BIG hs 10: Beheer van Communicatie- en Bedieningsprocessen	Vragen hs 10.10: Controle	Worden de logginggegevens minimaal 3 maanden bewaard?
220	i800.79868	i800.79868	i800.79868	i800.79868					Vragenlijst BIG hs 10: Beheer van Communicatie- en Bedieningsprocessen	Vragen hs 10.10: Controle	10.10.2.a Is er een procedure voor het structureel controleren van de logbestanden op het netwerk- systeemgebruik?
221	i800.79869	i800.79869	i800.79869	i800.79869					Vragenlijst BIG hs 10: Beheer van Communicatie- en Bedieningsprocessen	Vragen hs 10.10: Controle	Kunt u aangeven of er een procedure is om de handelingen van gebruikers te controleren?
223	i800.80606	i800.80606							Vragenlijst BIG hs 10: Beheer van Communicatie- en Bedieningsprocessen	Vragen hs 10.10: Controle	10.10.3.a Krijgen logbestanden adequate bescherming tegen verminking, verlies en verandering?
226	i800.79871	i800.79871							Vragenlijst BIG hs 10: Beheer van Communicatie- en Bedieningsprocessen	Vragen hs 10.10: Controle	10.10.6.a Wordt er kloksynchronisatie toegepast op alle actieve infrastructuur en informatiesystemen?
228	i800.79877			i800.79877					Vragenlijst BIG hs 11: Toegangsbeveiliging	Vragen hs 11.1: Toegangsbeleid	11.1.1.a Is er beleid vastgesteld dat richting geeft aan de beheerste logische toegang tot gegevens en informatie?

230	i800.79882	i800.79882	i800.79882	i800.79882					Vragenlijst BIG hs 11: Toegangsbeveiliging	Vragen hs 11.2: Beheer van toegangsrechten van gebruikers	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?
231	i800.79883	i800.79883	i800.79883	i800.79883					Vragenlijst BIG hs 11: Toegangsbeveiliging	Vragen hs 11.2: Beheer van toegangsrechten van gebruikers	Is deze procedure belegd bij de betrokken systeem/proces eigenaar?
233	i800.79885	i800.79885		i800.79885					Vragenlijst BIG hs 11: Toegangsbeveiliging	Vragen hs 11.2: Beheer van toegangsrechten van gebruikers	11.2.2.a Wordt de toewijzing en het gebruik van speciale bevoegdheden beperkt en beheerst?
234	i800.79886	i800.79886		i800.79886					Vragenlijst BIG hs 11: Toegangsbeveiliging	Vragen hs 11.2: Beheer van toegangsrechten van gebruikers	Is dit herleidbaar aan een (beheer) principe of doelstelling?
236	i800.79888	i800.79888							Vragenlijst BIG hs 11: Toegangsbeveiliging	Vragen hs 11.2: Beheer van toegangsrechten van gebruikers	11.2.3.a Is er een vastgestelde procedure voor de vormgeving en het (veilig) uitgeven en opslaan van wachtwoorden en andere authenticatie middelen?
238	i800.79890	i800.79890	i800.79890	i800.79890					Vragenlijst BIG hs 11: Toegangsbeveiliging	Vragen hs 11.2: Beheer van toegangsrechten van gebruikers	11.2.4.a Worden de toegangsrechten van gebruikers regelmatig beoordeeld in een formeel proces?
239	i800.79891	i800.79891	i800.79891	i800.79891					Vragenlijst BIG hs 11: Toegangsbeveiliging	Vragen hs 11.2: Beheer van toegangsrechten van gebruikers	Zijn er verslagen van de beoordeling van de toegangsrechten?
241	i800.79893	i800.79893		i800.79893					Vragenlijst BIG hs 11: Toegangsbeveiliging	Vragen hs 11.3: Verantwoordelijkheden van gebruikers	11.3.1.a Worden alle medewerkers regelmatig geïnformeerd over de regels voor het juist en veilig gebruik van wachtwoorden?
242	i800.79894			i800.79894					Vragenlijst BIG hs 11: Toegangsbeveiliging	Vragen hs 11.3: Verantwoordelijkheden van gebruikers	11.3.1.b Welke voorwaarden zijn aan de wachtwoorden gesteld? Geef aan wat voor uw organisatie van toepassing is.

244	i800.79896								Vragenlijst BIG hs 11: Toegangsbeveiliging	Vragen hs 11.3: Verantwoordelijkheden van gebruikers	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?
245	i800.79897								Vragenlijst BIG hs 11: Toegangsbeveiliging	Vragen hs 11.3: Verantwoordelijkheden van gebruikers	11.3.2.b Worden deze regels (waar mogelijk) door een policy afgedwongen?
247	i800.79899			i800.79899					Vragenlijst BIG hs 11: Toegangsbeveiliging	Vragen hs 11.3: Verantwoordelijkheden van gebruikers	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?
248	i800.79900								Vragenlijst BIG hs 11: Toegangsbeveiliging	Vragen hs 11.3: Verantwoordelijkheden van gebruikers	11.3.3.b Is er een clear screen-beleid voor ICT-voorzieningen?
250	i800.79902			i800.79902					Vragenlijst BIG hs 11: Toegangsbeveiliging	Vragen hs 11.4: Toegangsbeheersing voor netwerken	11.4.1.a Is er een formele procedure voor het toekennen van toegangsrechten voor het netwerk en netwerkdiensten?
252	i800.79904	i800.79904							Vragenlijst BIG hs 11: Toegangsbeveiliging	Vragen hs 11.4: Toegangsbeheersing voor netwerken	11.4.2.a Is er een vastgestelde procedure voor het authenticeren van (externe) gebruikers voor toegang tot het netwerk van buiten?
253	i800.79905	i800.79905							Vragenlijst BIG hs 11: Toegangsbeveiliging	Vragen hs 11.4: Toegangsbeheersing voor netwerken	Wordt er hierbij gebruik gemaakt van een twee factor authenticatie?
255	i800.79907								Vragenlijst BIG hs 11: Toegangsbeveiliging	Vragen hs 11.4: Toegangsbeheersing voor netwerken	11.4.3.a Is er een vastgestelde policy of richtlijn voor identificatie en authenticatie van netwerkapparatuur?
257	i800.79909			i800.79909					Vragenlijst BIG hs 11: Toegangsbeveiliging	Vragen hs 11.4: Toegangsbeheersing voor netwerken	11.4.4.a Is er een procedure voor de beheerste toegang tot netwerkpoorten (bv firewalls) en netwerkcomponenten (bv switches) voor beheeractiviteiten (bv diagnose, configureren)?
259	i800.79911	i800.79911							Vragenlijst BIG hs 11: Toegangsbeveiliging	Vragen hs 11.4: Toegangsbeheersing voor netwerken	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?
261	i800.79913	i800.79913							Vragenlijst BIG hs 11: Toegangsbeveiliging	Vragen hs 11.4: Toegangsbeheersing voor netwerken	11.4.6.a Is de toegang van gebruikers in een gemeenschappelijk netwerk (met andere organisaties) ingericht volgens het geldende toegangsbeleid van de organisatie?
263	i800.79915	i800.79915							Vragenlijst BIG hs 11: Toegangsbeveiliging	Vragen hs 11.4: Toegangsbeheersing voor netwerken	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 bedrijfstoepassingen?
265	i800.79938	i800.79938							Vragenlijst BIG hs 11: Toegangsbeveiliging	Vragen hs 11.5: Toegangsbeveiliging voor besturingssystemen	11.5.1.a Wordt de toegang tot besturingssystemen beheerst met een beveiligde inlogprocedure?
266	i800.79939	i800.79939							Vragenlijst BIG hs 11: Toegangsbeveiliging	Vragen hs 11.5: Toegangsbeveiliging voor besturingssystemen	Wordt er gebruik gemaakt van ACL's (Acces Control List)?

268	i800.79941	i800.79941	i800.79941						Vragenlijst BIG hs 11: Toegangsbeveiliging	Vragen hs 11.5: Toegangsbeveiliging voor besturingssystemen	11.5.2.a Hebben alle gebruikers en beheerders een unieke inlognaam (identificatie)? Zie ook vraag 11.2.2.
269	i800.79942	i800.79942	i800.79942						Vragenlijst BIG hs 11: Toegangsbeveiliging	Vragen hs 11.5: Toegangsbeveiliging voor besturingssystemen	11.5.2.b Zijn er geschikte technieken om de identiteit van de gebruiker / beheerder vast te stellen
270	i800.79943	i800.79943	i800.79943						Vragenlijst BIG hs 11: Toegangsbeveiliging	Vragen hs 11.5: Toegangsbeveiliging voor besturingssystemen	Wordt dit gecontroleerd?
272	i800.79945	i800.79945							Vragenlijst BIG hs 11: Toegangsbeveiliging	Vragen hs 11.5: Toegangsbeveiliging voor besturingssystemen	11.5.3.a Worden de richtlijnen voor het gebruik en de sterkte van wachtwoorden door het systeem afgedwongen?
274	i800.79947								Vragenlijst BIG hs 11: Toegangsbeveiliging	Vragen hs 11.5: Toegangsbeveiliging voor besturingssystemen	11.5.4.a Wordt het gebruik van hulpprogrammatuur waarmee database-, systeem- en toepassingsbeheersmaatregelen zouden kunnen worden gepasseerd, beperkt en beheerst?
276	i800.79949	i800.79949							Vragenlijst BIG hs 11: Toegangsbeveiliging	Vragen hs 11.5: Toegangsbeveiliging voor besturingssystemen	11.5.5.a Worden werkstations en sessies op afstand vergrendeld of uitgeschakeld na een vastgestelde periode van inactiviteit?
277	i800.79950	i800.79950							Vragenlijst BIG hs 11: Toegangsbeveiliging	Vragen hs 11.5: Toegangsbeveiliging voor besturingssystemen	Kunt u aangeven na welke periode?
279	i800.79952	i800.79952							Vragenlijst BIG hs 11: Toegangsbeveiliging	Vragen hs 11.5: Toegangsbeveiliging voor besturingssystemen	11.5.6.a Is er een procedure voor de beheerste (beperkt voor de duur van onderhoud) en veilige (two factor authenticatie) toegang van externe leveranciers voor het onderhoud van de IT middelen?
281	i800.79954	i800.79954							Vragenlijst BIG hs 11: Toegangsbeveiliging	Vragen hs 11.6: Toegangsbeheersing voor toepassingen en informatie	11.6.1.a Wordt de toegang tot informatie en functies van toepassingssystemen door gebruikers en ondersteunend personeel beperkt?

283	i800.79956			i800.79956					Vragenlijst BIG hs 11: Toegangsbeveiliging	Vragen hs 11.6: Toegangsbeheersing voor toepassingen en informatie	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?
284	i800.79957			i800.79957					Vragenlijst BIG hs 11: Toegangsbeveiliging	Vragen hs 11.6: Toegangsbeheersing voor toepassingen en informatie	Kunt u aangeven voor welke systemen?
286	i800.79959	i800.79959							Vragenlijst BIG hs 11: Toegangsbeveiliging	Vragen hs 11.7: Draagbare computers en telewerken	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?
287	i800.79960	i800.79960							Vragenlijst BIG hs 11: Toegangsbeveiliging	Vragen hs 11.7: Draagbare computers en telewerken	Kunt u aangeven welke beveiligingsmaatregelen u heeft getroffen?
288	i800.79961	i800.79961							Vragenlijst BIG hs 11: Toegangsbeveiliging	Vragen hs 11.7: Draagbare computers en telewerken	Gelden deze maatregelen voor de hele gemeente?
289	i800.79962	i800.79962							Vragenlijst BIG hs 11: Toegangsbeveiliging	Vragen hs 11.7: Draagbare computers en telewerken	Heeft uw gemeente uitgewerkt welke systemen wel en niet geraadpleegd mogen worden?
291	i800.79964	i800.79964		i800.79964					Vragenlijst BIG hs 11: Toegangsbeveiliging	Vragen hs 11.7: Draagbare computers en telewerken	11.7.2.a Is er beleid en zijn er procedures voor het werken met informatiesystemen buiten de reguliere kantooromgeving?
292	i800.79965	i800.79965		i800.79965					Vragenlijst BIG hs 11: Toegangsbeveiliging	Vragen hs 11.7: Draagbare computers en telewerken	Heeft de gemeente een telewerkbeleid?
293	i800.79966	i800.79966		i800.79966					Vragenlijst BIG hs 11: Toegangsbeveiliging	Vragen hs 11.7: Draagbare computers en telewerken	Heeft de gemeente uitgewerkt welke systemen wel en niet mogen worden geraadpleegd?
294	i800.79967	i800.79967		i800.79967					Vragenlijst BIG hs 11: Toegangsbeveiliging	Vragen hs 11.7: Draagbare computers en telewerken	Zijn de telewerkvoorzieningen op basis van zero-footprint ingericht?
296	i800.79970	i800.79970						i800.79970	Vragenlijst BIG hs 12: Verwerving, ontwikkeling en onderhoud van Informatiesystemen	Vragenhs 12.1: Beveiligingseisen voor informatiesystemen	12.1.1.a Worden bij het analyseren en specificeren van de eisen voor nieuwe systemen of systeemwijzingen expliciet aandacht besteed aan de eisen voor informatiebeveiliging?
298	i800.79972								Vragenlijst BIG hs 12: Verwerving, ontwikkeling en onderhoud van Informatiesystemen	Vragen hs 12.2: Correcte verwerking in toepassingen	12.2.1.a Vindt er bij invoer van gegevens in (web-)applicaties validatie plaats op aspecten als juistheid en geschiktheid?
299	i800.79973								Vragenlijst BIG hs 12: Verwerving, ontwikkeling en onderhoud van Informatiesystemen	Vragen hs 12.2: Correcte verwerking in toepassingen	12.2.1.b Valideert de webapplicatie de inhoud van een HTTP-request voordat deze gebruikt wordt?

300	i800.79983			i800.79983					Vragenlijst BIG hs 12: Verwerving, ontwikkeling en onderhoud van Informatiesystemen	Vragen hs 12.2: Correcte verwerking in toepassingen	12.2.1.c Welke BRP specifieke maatregelen heeft u getroffen?
302	i800.79997	i800.79997							Vragenlijst BIG hs 12: Verwerving, ontwikkeling en onderhoud van Informatiesystemen	Vragen hs 12.2: Correcte verwerking in toepassingen	12.2.2.a Is er beleid of zijn er richtlijnen voor verwerking-, en uitvoervalidaties bij de ontwikkeling van (web-) applicaties?
304	i800.80002	i800.80002							Vragenlijst BIG hs 12: Verwerving, ontwikkeling en onderhoud van Informatiesystemen	Vragen hs 12.2: Correcte verwerking in toepassingen	12.2.3.a Zijn er maatregelen geïmplementeerd om verandering van berichten in toepassingen te voorkomen?
306	i800.80014	i800.80014							Vragenlijst BIG hs 12: Verwerving, ontwikkeling en onderhoud van Informatiesystemen	Vragen hs 12.2: Correcte verwerking in toepassingen	12.2.4.a Is er beleid of zijn er richtlijnen voor invoer- en verwerkingvalidaties bij de ontwikkeling van (web-) applicaties?
308	i800.80016	i800.80016	i800.80016						Vragenlijst BIG hs 12: Verwerving, ontwikkeling en onderhoud van Informatiesystemen	Vragen hs 12.3: Cryptografische beheersmaatregelen	12.3.1.a Is er een vastgesteld beleid voor het toepassen en beheren van cryprografische middelen?
310	i800.80024	i800.80024							Vragenlijst BIG hs 12: Verwerving, ontwikkeling en onderhoud van Informatiesystemen	Vragen hs 12.3: Cryptografische beheersmaatregelen	12.3.2.a Zijn er maatregelen getroffen specifiek voor het beheren van cryptografische sleutels?
312	i800.80046	i800.80046							Vragenlijst BIG hs 12: Verwerving, ontwikkeling en onderhoud van Informatiesystemen	Vragen hs 12.4: Beveiliging van systeembestanden	12.4.1.a Zijn er maatregelen getroffen voor het beheren en het beheerst wijzigen van (applicatie-) programmatuur?
313	i800.80047	i800.80047							Vragenlijst BIG hs 12: Verwerving, ontwikkeling en onderhoud van Informatiesystemen	Vragen hs 12.4: Beveiliging van systeembestanden	12.4.1.b Is er een hardeningsproces voor ICT-componenten?
315	i800.80049								Vragenlijst BIG hs 12: Verwerving, ontwikkeling en onderhoud van Informatiesystemen	Vragen hs 12.4: Beveiliging van systeembestanden	12.4.2.a Is in het testproces een procedure opgenomen voor het zorgvuldig gebruik van geanonimiseerde testdata?
316	i800.80110								Vragenlijst BIG hs 12: Verwerving, ontwikkeling en onderhoud van Informatiesystemen	Vragen hs 12.4: Beveiliging van systeembestanden	Wordt in het testproces een kopie van de productiedatabase gemaakt, of zijn er geen testplannen met geanonimiseerde testgegevens?
317	i800.80111								Vragenlijst BIG hs 12: Verwerving, ontwikkeling en onderhoud van Informatiesystemen	Vragen hs 12.4: Beveiliging van systeembestanden	12.4.2.b Wordt er in het testproces een kopie van de productie database gemaakt?
319	i800.80051								Vragenlijst BIG hs 12: Verwerving, ontwikkeling en onderhoud van Informatiesystemen	Vragen hs 12.4: Beveiliging van systeembestanden	12.4.3.a Zijn er maatregelen getroffen voor het beheerst en veilig opslaan van broncode?
320	i800.80052								Vragenlijst BIG hs 12: Verwerving, ontwikkeling en onderhoud van Informatiesystemen	Vragen hs 12.4: Beveiliging van systeembestanden	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?

322	i800.80054	i800.80054							Vragenlijst BIG hs 12: Verwerving, ontwikkeling en onderhoud van Informatiesystemen	Vragen hs 12.5: Beveiliging bij ontwikkelings- en ondersteuningsprocessen	12.5.1.a Is binnen de gemeente een formeel proces ingericht voor het uitvoeren van wijzigingen?
324	i800.80056	i800.80056							Vragenlijst BIG hs 12: Verwerving, ontwikkeling en onderhoud van Informatiesystemen	Vragen hs 12.5: Beveiliging bij ontwikkelings- en ondersteuningsprocessen	12.5.2.a Worden er testen uitgevoerd op kritische toepassingen, na wijzigingen in de besturingssystemen?
325	i800.80057	i800.80057							Vragenlijst BIG hs 12: Verwerving, ontwikkeling en onderhoud van Informatiesystemen	Vragen hs 12.5: Beveiliging bij ontwikkelings- en ondersteuningsprocessen	Kunt u aangeven waarom er geen testen worden uitgevoerd op de kritische toepassingen, na wijzigingen in de besturingssytemen?
326	i800.80058	i800.80058							Vragenlijst BIG hs 12: Verwerving, ontwikkeling en onderhoud van Informatiesystemen	Vragen hs 12.5: Beveiliging bij ontwikkelings- en ondersteuningsprocessen	Kunt u aangeven op welk niveau(s) de testen plaatsvinden?
328	i800.80060								Vragenlijst BIG hs 12: Verwerving, ontwikkeling en onderhoud van Informatiesystemen	Vragen hs 12.5: Beveiliging bij ontwikkelings- en ondersteuningsprocessen	12.5.3.a Is er in de procedure voor het installeren van Servers, OS- en en Ontwikkelplatforms expliciet aandacht voor het uitzetten van niet noodzakelijke functionaliteit en toegang?
329	i800.80112								Vragenlijst BIG hs 12: Verwerving, ontwikkeling en onderhoud van Informatiesystemen	Vragen hs 12.5: Beveiliging bij ontwikkelings- en ondersteuningsprocessen	Kunt u aangeven waarom hier geen aandacht voor is?
331	i800.80062	i800.80062							Vragenlijst BIG hs 12: Verwerving, ontwikkeling en onderhoud van Informatiesystemen	Vragen hs 12.5: Beveiliging bij ontwikkelings- en ondersteuningsprocessen	12.5.4.a Zijn er maatregelen getroffen voor het 'scannen' van in en uitgaand netwerkverkeer (content scanning, IDS, IPS)?
332	i800.80063	i800.80063							Vragenlijst BIG hs 12: Verwerving, ontwikkeling en onderhoud van Informatiesystemen	Vragen hs 12.5: Beveiliging bij ontwikkelings- en ondersteuningsprocessen	Kunt u aangeven waarom er geen maatregelen zijn getroffen?
336	i800.80067	i800.80067							Vragenlijst BIG hs 12: Verwerving, ontwikkeling en onderhoud van Informatiesystemen	Vragen hs 12.6: Beheer van technische kwetsbaarheden	12.6.1.a Zijn er maatregelen getroffen voor het regelmatig controleren op technische kwetsbaarheden in IT Services en Servers?
337	i800.80068	i800.80068							Vragenlijst BIG hs 12: Verwerving, ontwikkeling en onderhoud van Informatiesystemen	Vragen hs 12.6: Beheer van technische kwetsbaarheden	Kunt u aangeven welke maatregelen er zijn getroffen voor het regelmatig controleren op technische kwetsbaarheden in IT Services en Servers?
338	i800.80069	i800.80069							Vragenlijst BIG hs 12: Verwerving, ontwikkeling en onderhoud van Informatiesystemen	Vragen hs 12.6: Beheer van technische kwetsbaarheden	12.6.1.b Krijgt de gemeente kwetsbaarheidswaarschuwingen van de IBD
339	i800.80070	i800.80070							Vragenlijst BIG hs 12: Verwerving, ontwikkeling en onderhoud van Informatiesystemen	Vragen hs 12.6: Beheer van technische kwetsbaarheden	12.6.1.c Zijn de laatste (beveiligings)patches geïnstalleerd en worden deze volgens een patchmanagement proces doorgevoerd?

340	i800.80071	i800.80071							Vragenlijst BIG hs 12: Verwerving, ontwikkeling en onderhoud van Informatiesystemen	Vragen hs 12.6: Beheer van technische kwetsbaarheden	12.6.1.d Worden de penetratietests periodiek uitgevoerd?
341	i800.80072	i800.80072							Vragenlijst BIG hs 12: Verwerving, ontwikkeling en onderhoud van Informatiesystemen	Vragen hs 12.6: Beheer van technische kwetsbaarheden	12.6.1.e Worden de vulnerability assessments (security scans) periodiek uitgevoerd?
343	i800.79669	i800.79669							Vragenlijst BIG hs 13: Beheer van Informatiebeveiligingsincidenten	Vragen hs 13.1: Rapportage van informatiebeveiligingsgebeurtenissen en zwakke plekken	13.1.1.a Is er een incident management procedure?
344	i800.79670	i800.79670							Vragenlijst BIG hs 13: Beheer van Informatiebeveiligingsincidenten	Vragen hs 13.1: Rapportage van informatiebeveiligingsgebeurtenissen en zwakke plekken	Zijn een reactie- en escalatieprocedure en een registratiesysteem onderdeel van de incident management procedure?
346	i800.79671	i800.79671							Vragenlijst BIG hs 13: Beheer van Informatiebeveiligingsincidenten	Vragen hs 13.1: Rapportage van informatiebeveiligingsgebeurtenissen en zwakke plekken	13.1.2.a Kent iedereen zijn/haar verantwoordelijkheden met betrekking tot het melden van verdachte zwakke plekken met betrekking tot informatiebeveiliging?
347	i800.79672	i800.79672							Vragenlijst BIG hs 13: Beheer van Informatiebeveiligingsincidenten	Vragen hs 13.1: Rapportage van informatiebeveiligingsgebeurtenissen en zwakke plekken	Is er een integriteitsprotocol?
348	i800.79673	i800.79673							Vragenlijst BIG hs 13: Beheer van Informatiebeveiligingsincidenten	Vragen hs 13.1: Rapportage van informatiebeveiligingsgebeurtenissen en zwakke plekken	Is de procedure met betrekking tot het melden van verdachte en zwakke plekken met betrekking tot informatiebeveiliging bij iedereen bekend?
350	i800.79677								Vragenlijst BIG hs 13: Beheer van Informatiebeveiligingsincidenten	Vragen hs 13.2: Beheer van informatiebeveiligingsincidenten en verbeteringen	13.2.1.a Is in de incident management procedure ook aandacht besteed aan de reactie op een incident?
351	i800.79679								Vragenlijst BIG hs 13: Beheer van Informatiebeveiligingsincidenten	Vragen hs 13.2: Beheer van informatiebeveiligingsincidenten en verbeteringen	13.2.1.b Is de incident management procedure bekend bij alle verantwoordelijken?
352	i800.79680								Vragenlijst BIG hs 13: Beheer van Informatiebeveiligingsincidenten	Vragen hs 13.2: Beheer van informatiebeveiligingsincidenten en verbeteringen	13.2.1.c Is in de incident management procedure aandacht voor de afhandeling/reactie van een incident?
354	i800.79681								Vragenlijst BIG hs 13: Beheer van Informatiebeveiligingsincidenten	Vragen hs 13.2: Beheer van informatiebeveiligingsincidenten en verbeteringen	13.2.2.a Wordt er lering getrokken uit informatiebeveiligingsincidenten?
355	i800.79683								Vragenlijst BIG hs 13: Beheer van Informatiebeveiligingsincidenten	Vragen hs 13.2: Beheer van informatiebeveiligingsincidenten en verbeteringen	Worden de incidenten opgenomen in de PDCA cyclus?

357	i800.79685	i800.79685							Vragenlijst BIG hs 13: Beheer van Informatiebeveiligingsincidenten	Vragen hs 13.2: Beheer van informatiebeveiligingsincidenten en verbeteringen	13.2.3.a Wordt er rekening gehouden met het verzamelen van bewijsmateriaal als er een incident opgetreden is?
359	i800.80074								Vragenlijst BIG hs 14: Bedrijfscontinuïteitsbeheer	Vragenhs 14.1: Informatiebeveiligingsaspecten van bedrijfscontinuïteitsbeheer	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?
361	i800.80076								Vragenlijst BIG hs 14: Bedrijfscontinuïteitsbeheer	Vragenhs 14.1: Informatiebeveiligingsaspecten van bedrijfscontinuïteitsbeheer	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?
363	i800.80078			i800.80078	i800.80078				Vragenlijst BIG hs 14: Bedrijfscontinuïteitsbeheer	Vragenhs 14.1: Informatiebeveiligingsaspecten van bedrijfscontinuïteitsbeheer	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)?
364	i800.80079			i800.80079	i800.80079				Vragenlijst BIG hs 14: Bedrijfscontinuïteitsbeheer	Vragenhs 14.1: Informatiebeveiligingsaspecten van bedrijfscontinuïteitsbeheer	Kunt u aangeven voor welke systemen en processen u een vastgesteld Continuïteitsplan heeft?
365	i800.80080			i800.80080					Vragenlijst BIG hs 14: Bedrijfscontinuïteitsbeheer	Vragenhs 14.1: Informatiebeveiligingsaspecten van bedrijfscontinuïteitsbeheer	14.1.3.b Wordt er voor BRP rekening gehouden met de tijd tussen de laatste back-up en een mogelijk herstel?
366	i800.80081			i800.80081					Vragenlijst BIG hs 14: Bedrijfscontinuïteitsbeheer	Vragenhs 14.1: Informatiebeveiligingsaspecten van bedrijfscontinuïteitsbeheer	14.1.3.c Is het voor de BRP specifiek mogelijk dat er een volledige reconstructie mogelijk is binnen 24 uur?
368	i800.80083								Vragenlijst BIG hs 14: Bedrijfscontinuïteitsbeheer	Vragenhs 14.1: Informatiebeveiligingsaspecten van bedrijfscontinuïteitsbeheer	14.1.4.a Is er beleid en zijn er richtlijnen vastgesteld voor het vormgeven van de concrete continuïteitsplannen?
370	i800.80085			i800.80085					Vragenlijst BIG hs 14: Bedrijfscontinuïteitsbeheer	Vragenhs 14.1: Informatiebeveiligingsaspecten van bedrijfscontinuïteitsbeheer	14.1.5.a Worden continuïteitsplannen jaarlijks getest of ze actueel en doeltreffend blijven?

371	i800.91329			i800.91329					Vragenlijst BIG hs 14: Bedrijfscontinuïteitsbeheer	Vragenhs 14.1: Informatiebeveiligingsaspecten van bedrijfscontinuïteitsbeheer	Kunt u aangeven voor welke systemen de continuïteitsplannen worden getest?
373	i800.80087			i800.80087					Vragenlijst BIG hs 15: Naleving	Vragen hs 15.1: Naleving van wettelijke voorschriften	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?
374	i800.80088			i800.80088					Vragenlijst BIG hs 15: Naleving	Vragen hs 15.1: Naleving van wettelijke voorschriften	Kunt u aangeven aan welke IB relevante wet- en regelgeving wordt voldaan en waarvoor er contractuele afspraken zijn gemaakt?
376	i800.80090								Vragenlijst BIG hs 15: Naleving	Vragen hs 15.1: Naleving van wettelijke voorschriften	15.1.2.a Controleert uw organisatie actief op het illegaal gebruik van bedrijfsmiddelen?
378	i800.80092	i800.80092							Vragenlijst BIG hs 15: Naleving	Vragen hs 15.1: Naleving van wettelijke voorschriften	15.1.3.a Wordt opslag en archivering van registraties / dossiers volgens vastgesteld beleid uitgevoerd?
380	i800.80094	i800.80094							Vragenlijst BIG hs 15: Naleving	Vragen hs 15.1: Naleving van wettelijke voorschriften	15.1.4.a Wordt de bescherming van gegevens en privacy bewerkstelligd overeenkomstig relevante wetgeving, regelgeving en voorschriften en indien van toepassing contractuele bepalingen?
382	i800.80096								Vragenlijst BIG hs 15: Naleving	Vragen hs 15.1: Naleving van wettelijke voorschriften	15.1.5.a Hoe regelt / bevordert de gemeente het correct gebruik van IT voorzieningen en Informatie?
384	i800.80098	i800.80098							Vragenlijst BIG hs 15: Naleving	Vragen hs 15.1: Naleving van wettelijke voorschriften	15.1.6.a Worden cryptografische beheersmaatregelen toegepast in overeenstemming met relevante wetten en voorschriften?
385	i800.80099	i800.80099							Vragenlijst BIG hs 15: Naleving	Vragen hs 15.1: Naleving van wettelijke voorschriften	Kunt u aangeven volgens welke wetten en voorschriften de cryptografische beheersmaatregelen worden toegepast?
387	i800.80101	i800.80101		i800.80101					Vragenlijst BIG hs 15: Naleving	Vragen hs 15.2: Naleving van beveiligingsbeleid en -normen en technische naleving	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 een BRP en PUN eis.
389	i800.80103	i800.80103							Vragenlijst BIG hs 15: Naleving	Vragen hs 15.2: Naleving van beveiligingsbeleid en -normen en technische naleving	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?

390	i800.80104	i800.80104							Vragenlijst BIG hs 15: Naleving	Vragen hs 15.2: Naleving van beveiligingsbeleid en -normen en technische naleving	Kunt u aangeven voor welke systemen dit wordt gedaan?
391	i800.80105	i800.80105							Vragenlijst BIG hs 15: Naleving	Vragen hs 15.2: Naleving van beveiligingsbeleid en -normen en technische naleving	15.2.2.b Zijn de relevante afgegeven TPM-verklaringen niet ouder dan 1 jaar?
393	i800.80107								Vragenlijst BIG hs 15: Naleving	Vragen hs 15.3: Overwegingen bij audits van informatiesystemen	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?
395	i800.80109								Vragenlijst BIG hs 15: Naleving	Vragen hs 15.3: Overwegingen bij audits van informatiesystemen	15.3.2.a Worden hulpmiddelen voor audits van informatiesystemen beschermd tegen misbruik en compromittering?

Datatype	Parameter	Definitie	Tags
Boolean	1:Ja|0:Nee	Een Informatiebeveiligingsplan is een implementatieplan om ontbrekende informatiebeveiligingsmaatregel te implementeren. Dit plan wordt jaarlijks gemaakt op basis van management besluiten, nieuwe risico's, gewijzigde wetgeving, andere organisatietaken. De rapportage is belangrijk voor het management om inzicht te krijgen in de voortgang en om daarop te kunnen sturen. Zie ook hs 3.1 uit de BIG: Benoem verantwoordelijken p.14 Benodigde documentatie Een informatiebeveiligingsplan met daarin de korte en lange termijn doelen en planningen voor het implementeren van maatregelen.	
Boolean	1:Ja|0:Nee	Benodigde documentatie Verslagen van vergaderingen waarin de planning aan de orde gekomen is. Plaats in het opmerkingenveld hieronder de eventuele extra onderbouwing van uw antwoord voor de IT auditor.	
Boolean	1:Ja|0:Nee	De organisatie moet een gedocumenteerd ISMS vaststellen, implementeren, uitvoeren, controleren, beoordelen, bijhouden en verbeteren binnen het kader van de algemene bedrijfsactiviteiten en -risico's van de organisatie. Het proces dat in het kader van deze maatregel wordt gehanteerd, is gebaseerd op het PDCA-model. Zie ook hs 3.1 uit de BIG: Benoem verantwoordelijken p.14 Benodigde documentatie Een spreadsheet met maatregelen, hun statussen, de verantwoordelijken voor de maatregelen, de verwachte planning van implementatie, management besluiten over planning of comply.	
Radiobutton	0:Nee|1:Ja|2:Anders		
Radiobutton	0:Nee|1:Ja|2:In ontwikkeling	Bijvoorbeeld in de instellingsbeschikking door middel van een ICV of een TPM.	
Radiobutton	0:Nee|1:Ja|2:Anders		
Boolean	1:Ja|0:Nee	Een gemeente moet een actueel en door het college vastgesteld informatiebeveiligingbeleid hebben dat bij voorkeur jonger is dan drie jaar. Bij voorkeur is gebruik gemaakt van het voorbeeld informatiebeveiligingsbeleid van de IBD met een eigen invulling / aanvulling op de locale situatie. Dit is een BRP bepaling en een Suwinorm. Wet BRP 1.11, lid 1/Besluit BRP 6 Suwinorm B.01 Zie ook hs 5.1.1. van de BIG: Beleidsdocumenten voor informatiebeveiliging p.19 Benodigde documentatie Een actueel informatiebeveiligingsbeleid, passend bij het gegeven antwoord. Bij voorkeur is gebruik gemaakt van het voorbeeld informatiebeveiligingsbeleid van de IBD met een eigen invulling / aanvulling op de locale situatie. SUWI guidance Onderdeel collegeverklaring: Deze vraag en het antwoord zijn onderdeel van de Collegeverklaring die de gemeente moet afgeven in het kader van Suwinet. Onderdeel SUWI-norm Deze vraag is onderdeel van het specifiek suwinet normenkader voor afnemers en het antwoord wordt gerapporteerd aan SZW. Doelstelling SUWI Richting geven aan en handhaven van beveiliging van de Suwinet aansluiting en de gegevens die worden getransporteerd en ervoor te zorgen dat aansluiting van de organisatie op Suwinet aantoonbaar aan de vereiste beveiligingsvoorwaarden voldoet. Criterium De Afnemer heeft voor de aansluiting op Suwinet expliciet aandacht besteed aan het stelsel van beveiligingsmaatregelen in zijn informatiebeveiligingsbeleid, of hiervoor een apart aansluitingsbeleid ontwikkeld. Nadere toelichting Scope: beveiligingstechniek Betrokken: gemeenten, SVB, UWV Nadere Info: veilige middelen voor data transport via veilige verbindingen, denk daarbij aan TSL en HTTPS. Draag zorg voor documentatie (security architectuur). SUWI-norm: B.01 Plaats in het opmerkingenveld hieronder de eventuele extra onderbouwing van uw antwoord voor de IT auditor.	ensia-rvig|ensia-keycontrol|ensia-itaudit|ensia-isd|ensia-isd|ensia-brp
Boolean	1:Ja|0:Nee		ensia-rvig|ensia-itaudit|ensia-isd|ensia-keycontrol|ensia-brp
Boolean	1:Ja|0:Nee		ensia-rvig|ensia-itaudit|ensia-isd|ensia-brp
Boolean	1:Ja|0:Nee		ensia-rvig|ensia-isd|ensia-itaudit|ensia-brp

Boolean	1:Ja|0:Nee	Een gemeente moet een actueel en door het college vastgesteld informatiebeveiligingbeleid hebben dat bij voorkeur jonger is dan vier jaar. Bij voorkeur is gebruik gemaakt van het voorbeeld informatiebeveiligingsbeleid van de IBD met een eigen invulling / aanvulling op de locale situatie. Dit is een BRP en Suwi eis. Wet BRP 1.11, lid 1/Besluit BRP 6 Suwinorm: B.01 Zie ook hs 5.1.1. van de BIG: Beleidsdocumenten voor informatiebeveiliging p.19 Benodigde documentatie Aantoonbare passages over de respectievelijke speciale gemeentelijke voorzieningen in het gemeentelijk informatiebeveiligingsbeleid.	ensia-rvig|ensia-keycontrol|ensia-isd|ensia-brp
Checkbox	0:Voor de BRP|1:Voor de PUN|2:Voor Suwinet|3:Voor de WBP		ensia-rvig|ensia-isd|ensia-itaudit|ensia-brp
Radiobutton	0:Nee|1:Ja|2:N.v.t.	Het vertalen van maatregelen naar samenwerkingsverbanden is essentieel voor het sluiten krijgen en houden van een adequate beveiliging door de hele organisatie. Dit is een BRP eis. Wet BRP 1.11, lid 1/Besluit BRP 6 Zie ook hs 5.1.2. van de BIG: Beleidsdocumenten voor informatiebeveiliging p.19 Benodigde documentatie Oprichtings dan wel instellingsbeschikkingen van GR'n met daarin specifiek aandacht voor Informatiebeleid. Voor Gemeenschappelijke Regelingen die openbare lichamen zijn: bewerkersovereenkomsten.	ensia-rvig|ensia-keycontrol|ensia-brp
Boolean	1:Ja|0:Nee	Zie ook hs 5.1.2. van de BIG: Beoordeling van het informatiebeveiligingsbeleid p.19 Benodigde documentatie Informatiebeveiligingsbeleid jonger dan 3 jaar SUWI guidance Onderdeel collegeverklaring Deze vraag en het antwoord zijn onderdeel van de Collegeverklaring die de gemeente moet afgeven in het kader van Suwinet. Onderdeel SUWI-norm Deze vraag is onderdeel van het specifiek suwinet normenkader voor afnemers en het antwoord wordt gerapporteerd aan SZW. Doelstelling SUWI Bewerkstellingen dat de getroffen beveiligingsmaatregelen continue voldoen aan het juiste beveiligingsniveau. Criterium (De implementatie van) het aansluitbeleid wordt periodiek beoordeeld op veranderingen in de wetgeving, wijziging van functionaliteit en uit te wisselen gegevens en veranderde technologiën. Nadere toelichting Scope: beveiligingstechniek Betrokken: gemeenten, SVB, UWV Nadere Info: veilige middelen voor data transport via veilige verbindingen, denk daarbij aan TSL en HTTPS. Volg de aanwijzingen in de wetgeving en aangrenzende wetgevingen die van toepassing kunnen zijn (denk aan AVG 2018). Juist= hetgeen je mag verwachten obv best practice. SUWI-norm: C.01 Plaats in het opmerkingenveld hieronder de eventuele extra onderbouwing van uw antwoord voor de IT auditor.	ensia-itaudit|ensia-bkwi|ensia-isd
Boolean	1:Ja|0:Nee	Het hoogste management behoort actief informatiebeveiliging binnen de organisatie te ondersteunen door duidelijk richting te geven, betrokkenheid te tonen en expliciet verantwoordelijkheden voor informatiebeveiliging toe te kennen en te erkennen. Dit is een BRP en een Suwi- eis bepaling. Besluit BRP 6, LO 7.2, 7.4.7, 4.2.4, 3.1 Zie ook hoofdstuk 6.1.1 van de BIG: Betrokkenheid van het College van B&W bij beveiliging van de BIG p.20 Benodigde documentatie In ieder geval verslagen van vergaderingen waarin het onderwerp Informatiebeveilging aan de orde gekomen is. Daarnaast behoort het management voldoende budgetten ter beschikking te stellen die passen bij de jaarlijkse informatieplanning. Ze behoren actief het belang van informatieveiligheid uit te dragen. SUWI guidance Onderdeel collegeverklaring Deze vraag en het antwoord zijn onderdeel van de Collegeverklaring die de gemeente moet afgeven in het kader van Suwinet. Onderdeel SUWI-norm Deze vraag is onderdeel van het specifiek suwinet normenkader voor afnemers en het antwoord wordt gerapporteerd aan SZW. Nadere toelichting Scope: IT Governance Betrokken: gemeenten, SVB, UWV Nadere Info: zorg dragen governance van IT, tone at the top , training, educatie en workshops SUWI-norm: C.01 Plaats in het opmerkingenveld hieronder de eventuele extra onderbouwing van uw antwoord voor de IT auditor.	ensia-rvig|ensia-bkwi|ensia-keycontrol|ensia-itaudit|ensia-isd|ensia-brp
Boolean	1:Ja|0:Nee		ensia-rvig|ensia-bkwi|ensia-itaudit|ensia-isd|ensia-brp
Boolean	1:Ja|0:Nee		ensia-rvig|ensia-bkwi|ensia-itaudit|ensia-isd|ensia-brp
Boolean	1:Ja|0:Nee	Activiteiten voor informatiebeveiliging behoren te worden gecoördineerd door vertegenwoordigers uit de verschillende delen van de organisatie met relevante rollen en functies. Dit is een Suwi eis. Zie ook hs 6.1.2 van de BIG: Betrokkenheid van het college van B&W bij beveilging p.20 Benodigde documentatie: Een actueel informatiebeveiligingsplan, een sanctiebeleid, de aanwezigheid van een crisisteam en een ingericht incidentmanagementproces. SUWI guidance Onderdeel	ensia-isd|ensia-itaudit
Checkbox	0:CISO|1:Vervanger CISO|2:Er zijn op afdelingsniveau en binnen samenwerkingsverbanden IB-contactpersonen		ensia-isd|ensia-itaudit
Radiobutton	0:Er wordt minimaal eens in de drie jaar onafhankelijk getoetst|1:Er vindt niet iedere drie jaar verantwoording plaats en/of er is geen onafhankelijke toets		ensia-isd|ensia-itaudit

Checkbox	0:Nee|1:Ja, in de functiebeschrijvingen|2:Ja, in de taakopdrachten|3:Ja, voor de basisregistraties	Alle verantwoordelijkheden voor informatiebeveiliging behoren duidelijk te zijn gedefinieerd. Dit is een Suwi eis. Suwinorm: B.05 Zie ook hs 6.1.3. van de BIG: Verantwoordelijkheden p.20 Benodigde documentatie Voor relevante rollen en functies behoren de eisen te zijn uitgewerkt in functie dan wel taak omschrijvingen. SUWI guidance Onderdeel collegeverklaring Deze vraag en het antwoord zijn onderdeel van de Collegeverklaring die de gemeente moet afgeven in het kader van Suwinet. Onderdeel SUWI-norm Deze vraag is onderdeel van het specifiek suwinet normenkader voor afnemers en het antwoord wordt gerapporteerd aan SZW. Doelstelling SUWI Ervoor zorgen dat de juiste taken en verantwoordelijkheden binnen de onderkende rollen juist worden uitgevoerd met inachtneming van de juiste functiescheiding voor zover de organisatiegrootte dit toelaat. Criterium De aangesloten organisatie op Suwinet heeft de type-rollen onderkend, de daarbij behorende de taken en verantwoordelijkheden vastgesteld en vastgelegd en noodzakelijke functiescheiding beschreven. Nadere toelichting Scope: ITGC inrichting organigram Betrokken: gemeenten, SVB, UWV Nadere Info: verdeling van verantwoordelijkheden (GeVS) gebaseerd op controle technische CFS SUWI-norm: B.05 Plaats in het opmerkingenveld hieronder de eventuele extra onderbouwing van uw antwoord voor de IT auditor.	ensia-itaudit|ensia-isd|ensia-keycontrol
Boolean	1:Ja|0:Nee	Er behoort een goedkeuringsproces voor nieuwe ICT-voorzieningen te worden vastgesteld en geïmplementeerd. Zie ook hs 6.1.4 van de BIG: Goedkeuringsproces voor ICT-voorzieningen p.21 Benodigde Documentatie: Autorisatieproces nieuwe IT voorzieningen	
Boolean	1:Ja|0:Nee		
Boolean	1:Ja|0:Nee	Eisen voor vertrouwelijkheid of voor een geheimhoudingsovereenkomst die een weerslag vormen van de behoefte van de organisatie aan bescherming van informatie behoren te worden vastgesteld en regelmatig te worden beoordeeld. Het onderteken van een individuele verklaring integriteit / tot geheimhouding of het afleggen van de ambtseed of belofte is een BRP en PUN eis. BRP: WBP 12, lid 2 PUN: WBP 12, lid 2 Zie ook hs 6.1.5 van de BIG: Geheimhoudingsovereenkomst p.21 Benodigde documentatie Geheimhoudingsverklaringen in Personeelsdossiers.	ensia-hrm|ensia-burgerzaken|ensia-bkwi|ensia-pun|ensia-pnikni|ensia-brp
Checkbox	0:Iedere ambtelijk medewerker ondertekent een individuele verklaring integriteit / tot geheimhouding of legt de ambtseed of ambtsbelofte af|1:Externe en tijdelijke medewerkers ondertekenen een geheimhoudingsverklaring|2:Bij de aanstelling wordt een VOG gevraagd		ensia-hrm|ensia-burgerzaken|ensia-bkwi|ensia-rvig|ensia-brp|ensia-pun|ensia-pnikni
Boolean	1:Ja|0:Nee	Er behoren geschikte contacten met relevante overheidsinstanties te worden onderhouden. Zie ook hs 6.1.6 van de BIG: Contact met overheidsinstanties p.21 Benodigde documentatie Calamiteiten procedures, incident management en responsebeleid, noodplannen, BCM.	
Checkbox	0:Met de brandweer|1:Met de politie|2:Met een meldkamer|3:Met de Suwidesk|4:Met de RVIG desk|5:Met Logius		
Boolean	1:Ja|0:Nee	Er behoren geschikte contacten met speciale belangengroepen of andere specialistische platforms voor beveiliging en professionele organisaties te worden onderhouden. Zie ook hs 6.1.7 van de BIG: Contact met speciale belangengroepen p.21 Benodigde documentatie: Aansluitdocumenten stap 1 en 2 van de IBD. SUWI-norm: B.04	ensia-isd
Checkbox	0:IBD|1:BKWI		ensia-isd
Boolean	1:Ja|0:Nee	De benadering van de organisatie voor het beheer van informatiebeveiliging en de implementatie daarvan (d.w.z. beheerdoelstellingen, beheersmaatregelen, beleid, processen en procedures voor informatiebeveiliging) behoren onafhankelijk en met geplande tussenpozen te worden beoordeeld, of zodra zich wijzigingen voordoen in de implementatie van de beveiliging. Dit is een BRP en een Suwi eis. Wet BRP 4.3, lid 1 Suwinorm: C.08 Zie ook hs 6.1.8 van de BIG: Beoordeling van het informatiebeveiligingsbeleid p.21 Benodigde documentatie Audit verslagen, gespreksverslagen, verslag van de beoordeling van het beleid.	ensia-rvig|ensia-isd|ensia-brp
Radiobutton	0:Nee|1:Ja, minimaal 1 keer per jaar|2:Ja, maar niet jaarlijks	De benadering van de organisatie voor het beheer van informatiebeveiliging en de implementatie daarvan (d.w.z. beheerdoelstellingen, beheersmaatregelen, beleid, processen en procedures voor informatiebeveiliging) behoren onafhankelijk en met geplande tussenpozen te worden beoordeeld, of zodra zich wijzigingen voordoen in de implementatie van de beveiliging. Suwinorm: C.08 Zie ook hs 8.1.6 van de BIG: Beoordeling van het informatiebeveiligingsbeleid p.21 Benodigde documentatie Stukken van raadsvergaderingen.	ensia-isd

Boolean	1:Ja|0:Nee	De benadering van de organisatie voor het beheer van informatiebeveiliging en de implementatie daarvan (d.w.z. beheerdoelstellingen, beheersmaatregelen, beleid, processen en procedures voor informatiebeveiliging) behoren onafhankelijk en met geplande tussenpozen te worden beoordeeld, of zodra zich wijzigingen voordoen in de implementatie van de beveiliging. Suwinorm: C.08 Zie ook hs 6.1.8 van de BIG: Beoordeling van het informatiebeveiligingsbeleid p.21 Benodigde documentatie In control verklaringen van samenwerkingsverbanden en directeuren van afdelingen.	ensia-isd
Boolean	1:Ja|0:Nee		ensia-isd
Radiobutton	0:Alleen voor het in standhouden/beheren van ICT-voorzieningen|1:Alleen voor de invulling van bedrijfsprocessen|2:Externe partijen worden niet gebruikt voor het in stand houden/beheer van ICT-voorzieningen en voor de invulling van bedrijfsprocessen|3:Externe partijen worden zowel voor het in standhouden/beheren van ICT-voorzieningen als voor de invulling van bedrijfsprocessen gebruikt	De risico's voor de informatie en ICT-voorzieningen van de organisatie vanuit bedrijfsprocessen waarbij externe partijen betrokken zijn, behoren te worden geïdentificeerd en er behoren geschikte beheersmaatregelen te worden geïmplementeerd voordat toegang wordt verleend. Dit is een eis vanuit BRP en Suwi. Wet BRP 1.10, lid 2 Suwinorm: B.03 Zie ook hs 6.2.1. van de BIG: Identificatie van risico's die betrekking hebben op externe partijen p.22 Plaats in het opmerkingenveld hieronder de eventuele extra onderbouwing van uw antwoord voor de IT auditor.	ensia-rvig|ensia-isd|ensia-brp
Boolean	1:Ja|0:Nee	De risico's voor de informatie en ICT-voorzieningen van de organisatie vanuit bedrijfsprocessen waarbij externe partijen betrokken zijn, behoren te worden geïdentificeerd en er behoren geschikte beheersmaatregelen te worden geïmplementeerd voordat toegang wordt verleend. Zie ook hs 6.2.1. van de BIG: Identificatie van risico's die betrekking hebben op externe partijen p.22 Benodigde documentatie Ingevulde Dataclassificatie verslagen.	ensia-bkwi
Boolean	1:Ja|0:Nee	De risico's voor de informatie en ICT-voorzieningen van de organisatie vanuit bedrijfsprocessen waarbij externe partijen betrokken zijn, behoren te worden geïdentificeerd en er behoren geschikte beheersmaatregelen te worden geïmplementeerd voordat toegang wordt verleend. Zie ook hs 6.2.1 van de BIG: Identificatie van risico's die betrekking hebben op externe partijen p.22 Benodigde documentatie Inkoop dossiers	ensia-bkwi
Boolean	1:Ja|0:Nee	De risico's voor de informatie en ICT-voorzieningen van de organisatie vanuit bedrijfsprocessen waarbij externe partijen betrokken zijn, behoren te worden geïdentificeerd en er behoren geschikte beheersmaatregelen te worden geïmplementeerd voordat toegang wordt verleend. Zie ook hs 6.2.1 van de BIG: Identificatie van risico's die betrekking hebben op externe partijen p.22 Benodigde documentatie Voor iedere uitbesteding met persoonsgegevens moet een bewerkersovereenkomst aanwezig zijn.	ensia-bkwi
Checkbox	0:Conform voorstel van de leverancier|1:Conform het model uit de BIG-OP reeks.|2:Op basis van de BIG en in overleg met de leverancier		ensia-bkwi
Radiobutton	0:Nee|1:Ja, Wettelijke grondslag is vastgesteld er wordt gedaan aan doelbinding en er worden niet meer gegevens vastgelegd dan noodzakelijk|2:Ja, maar we houden daar niet in alle gevallen rekening mee	De risico's voor de informatie en ICT-voorzieningen van de organisatie vanuit bedrijfsprocessen waarbij externe partijen betrokken zijn, behoren te worden geïdentificeerd en er behoren geschikte beheersmaatregelen te worden geïmplementeerd voordat toegang wordt verleend. Zie ook hs 6.2.1. van de BIG: Identificatie van risico's die betrekking hebben op externe partijen p.22 Benodigde documentatie PIA's.	ensia-bkwi
Boolean	1:Ja|0:Nee	De risico's voor de informatie en ICT-voorzieningen van de organisatie vanuit bedrijfsprocessen waarbij externe partijen betrokken zijn, behoren te worden geïdentificeerd en er behoren geschikte beheersmaatregelen te worden geïmplementeerd voordat toegang wordt verleend. Dit is een eis vanuit DigiD. DigiD: B.05 Zie ook hs 6.2.1 van de BIG: Identificatie van risico's die betrekking hebben op externe partijen p.22 Benodige documentatie: Incidentregistratie, relevante passages in bewerkersovereenkomsten en leveringsovereenkomsten, SLA's, voor alle uitbesteedde processen/systemen.	ensia-bkwi
Radiobutton	0:Nee|1:Ja, en we ontvangen een TPM/SAE/SAS|2:Ja, door een onafhankelijk onderzoek, maar niet middels een TPM/SAE of SAS	De risico's voor de informatie en ICT-voorzieningen van de organisatie vanuit bedrijfsprocessen waarbij externe partijen betrokken zijn, behoren te worden geïdentificeerd en er behoren geschikte beheersmaatregelen te worden geïmplementeerd voordat toegang wordt verleend. Dit is een eis vanuit BRP. Besluit BRP 8, 9 Zie ook hs 6.2.1 van de BIG: Identificatie van risico's die betrekking hebben op externe partijen p.22 Benodigde documentatie: Aanwezige TPM's, SAE verklaringen, SAS rapporten, per leverancier.	ensia-rvig|ensia-bkwi|ensia-brp

Boolean	1:Ja|0:Nee	De risico's voor de informatie en ICT-voorzieningen van de organisatie vanuit bedrijfsprocessen waarbij externe partijen betrokken zijn, behoren te worden geïdentificeerd en er behoren geschikte beheersmaatregelen te worden geïmplementeerd voordat toegang wordt verleend. Zie ook hs 6.2.1 van de BIG: Identificatie van risico's die betrekking hebben op externe partijen p.22 Benodigde documentatie Een In Concrol Verklaring (ICV).	ensia-bkwi
Boolean	1:Ja|0:Nee	De risico's voor de informatie en ICT-voorzieningen van de organisatie vanuit bedrijfsprocessen waarbij externe partijen betrokken zijn, behoren te worden geïdentificeerd en er behoren geschikte beheersmaatregelen te worden geïmplementeerd voordat toegang wordt verleend. Dit is een eis vanuit Suwi. Suwinorm: B.06 Zie ook hs 6.2.1 van de BIG: Identificatie van risico's die betrekking hebben op externe partijen p.22 Benodigde documentatie Een In Control Verlaring (ICV).	ensia-isd
Boolean	1:Ja|0:Nee	Alle geïdentificeerde beveiligingseisen behoren te worden beoordeeld voordat externe medewerkers toegang wordt verleend tot de informatie of bedrijfsmiddelen van de organisatie. Zie ook hs 6.2.2 van de BIG: Beveiliging beoordelen in de omgang met klanten p. 23 Benodigde documentatie: Contracten met beveiligingseisen en voorwaarden	
Boolean	1:Ja|0:Nee		
Boolean	1:Ja|0:Nee	In overeenkomsten met derden waarbij toegang tot, het verwerken van, communicatie van of beheer van informatie of ICT-voorzieningen van de organisatie, of toevoeging van producten of diensten aan ICT-voorzieningen, behoren alle relevante beveiligingseisen te zijn opgenomen. Zie ook hs 6.2.3 van de BIG: Beveiliging behandelen in overeenkomsten met een derde partij p.23 Benodigde documentatie Dossier: Contract, SLA, Bewerkersovereenkomst.	ensia-bkwi
Checkbox	0:Intellectueel eigendom|1:Kwaliteitsaspecten|2:Beveiligingseisen|3:Aansprakelijkheid|4:Escrows|5:Reviews	In overeenkomsten met derden waarbij toegang tot, het verwerken van, communicatie van of beheer van informatie of ICT-voorzieningen van de organisatie, of toevoeging van producten of diensten aan ICT-voorzieningen, behoren alle relevante beveiligingseisen te zijn opgenomen. Zie ook hs 6.2.3 van de BIG: Beveiliging behandelen in overeenkomsten met een derde partij p.23 Benodigde documentatie: Dossier: Contract, SLA, Bewerkersovereenkomst.	ensia-bkwi
Boolean	1:Ja|0:Nee	In overeenkomsten met derden waarbij toegang tot, het verwerken van, communicatie van of beheer van informatie of ICT-voorzieningen van de organisatie, of toevoeging van producten of diensten aan ICT-voorzieningen, behoren alle relevante beveiligingseisen te zijn opgenomen. Zie ook hs 6.2.3 van de BIG: Beveiliging behandelen in overeenkomsten met een derde partij p.23 Benodigde documentatie Dossier: Contract, SLA, Bewerkersovereenkomst.	ensia-bkwi
Boolean	1:Ja|0:Nee	In overeenkomsten met derden waarbij toegang tot, het verwerken van, communicatie van of beheer van informatie of ICT-voorzieningen van de organisatie, of toevoeging van producten of diensten aan ICT-voorzieningen, behoren alle relevante beveiligingseisen te zijn opgenomen. Zie ook hs 6.2.3 van de BIG: Beveiliging behandelen in overeenkomsten met een derde partij p.23 Benodigde documentatie Dossier: Contract, SLA, Bewerkersovereenkomst.	ensia-bkwi
Boolean	1:Ja|0:Nee	In overeenkomsten met derden waarbij toegang tot, het verwerken van, communicatie van of beheer van informatie of ICT-voorzieningen van de organisatie, of toevoeging van producten of diensten aan ICT-voorzieningen, behoren alle relevante beveiligingseisen te zijn opgenomen. Dit is een Suwi eis. Suwinorm: B.03 (met name B.03.02), U.01 Zie ook hs 6.2.3. van de BIG: Beveiliging behandelen in overeenkomsten met een derde partij p.23 Benodigde documentatie Dossier: Contract, SLA, Bewerkersovereenkomst.	ensia-isd
Boolean	1:Ja|0:Nee	In overeenkomsten met derden waarbij toegang tot, het verwerken van, communicatie van of beheer van informatie of ICT-voorzieningen van de organisatie, of toevoeging van producten of diensten aan ICT-voorzieningen, behoren alle relevante beveiligingseisen te zijn opgenomen. Zie ook hs 6.2.3. van de BIG: Beveiliging behandelen in overeenkomsten met een derde partij p.23 Benodigde documentatie: Dossier, Contract, SLA, Bewerkersovereenkomst.	ensia-bkwi
Boolean	1:Ja|0:Nee	Alle bedrijfsmiddelen behoren duidelijk te zijn geïdentificeerd en er behoort een inventaris van alle belangrijke bedrijfsmiddelen te worden opgesteld en bijgehouden. Suwinorm: B.06, B.07 Zie ook hs 7.1.1. van de BIG: Inventarisatie van bedrijfsmiddelen p.24 Benodigde documentatie: Een gevulde CMDB (configuratie management database).	ensia-isd
Checkbox	0:Hard- en software|1:Applicaties|2:Informatieverzamelingen		ensia-isd
Boolean	1:Ja|0:Nee	Alle informatie en bedrijfsmiddelen die verband houden met ICT-voorzieningen behoren een eigenaar te hebben in de vorm van een aangewezen deel van de organisatie. Dit is een BRP eis. WBP 8 Zie ook hs 7.1.2 van de BIG: Eigendom van bedrijfsmiddelen p.24 Benodigde documentatie Binnen de CMDB zijn ook eigenaren van (groepen) van processen dan wel oinformatiesystemen benoemd en die eigenaren weten dat. Dit kan blijken uit jaarplannen en begrotingen en gebruikersautorisatiebeheer. Een eigenaar doet de financiele verantwoordingen en tekent op autorisatieformulieren of heeft dat gemandateerd.	ensia-rvig|ensia-brp
Boolean	1:Ja|0:Nee		ensia-rvig|ensia-brp

Boolean	1:Ja|0:Nee	Er behoren regels te worden vastgesteld, gedocumenteerd en geïmplementeerd voor aanvaardbaar gebruik van informatie en bedrijfsmiddelen die verband houden met ICT-voorzieningen. Dit is een PUN eis. PUN 93 Zie ook hs 7.1.3 van de BIG: Aanvaardbaar gebruik van bedrijfsmiddelen p.24 Benodigde documenten Huisregels en regels gebruik IT voorzieningen, inclusief telewerkbeleid indien toegestaan.	ensia-rvig|ensia-brp|ensia-pun|ensia-pnikni
Boolean	1:Ja|0:Nee	Informatie behoort te worden geclassificeerd met betrekking tot de waarde, wettelijke eisen, gevoeligheid en onmisbaarheid voor de organisatie. Suwinorm: U.06 Zie ook hs 7.2.1. van de BIG: Richtlijnen voor classificatie van informatie p.25 Benodigde documentatie Verslagen van classifciatie onderzoeken/analyses.	ensia-isd
Boolean	1:Ja|0:Nee		ensia-isd
Boolean	1:Ja|0:Nee		ensia-isd
Boolean	1:Ja|0:Nee	Er behoren geschikte, samenhangende procedures te worden ontwikkeld en geïmplementeerd voor de labeling en de verwerking van informatie overeenkomstig het classificatiesysteem dat de organisatie heeft geïmplementeerd. Suwinorm: U.06 Zie ook hs 7.2.2. van de BIG: Labeling en verwerking van informatie p.25 Benodigde documentatie Verwerkingsprocedures voor beveiligd verwerken, opslag, transmissie, declassificatie, en vernietiging. Overeenkomsten met derde partijen waarin wordt uitgelegd hoe classificatie labels moeten worden uitgelegd.	ensia-isd
Boolean	1:Ja|0:Nee		ensia-bkwi
Boolean	1:Ja|0:Nee		ensia-bkwi
Boolean	1:Ja|0:Nee	De rollen en verantwoordelijkheden van werknemers, ingehuurd personeel en externe gebruikers ten aanzien van beveiliging behoren te worden vastgesteld en gedocumenteerd overeenkomstig het beleid voor informatiebeveiliging van de organisatie. Dit is een BRP eis. Besluit BRP 6 Zie ook hs 8.1.1. van de BIG: Rollen en verantwoordelijkheden p.26 Benodigde documentatie Functiebeschrijvingen passend bij het informatiebeveiligingsbeleid.	ensia-hrm|ensia-rvig|ensia-bkwi|ensia-brp
Checkbox	0:m.b.t. het beveiligingsbeleid|1:m.b.t. de bescherming van bedrijfsmiddelen|2:m.b.t. speciale verantwoordelijkheden (ingeval van een BRP, BUN, SUWI rol/functie)|3:m.b.t. de rapportage van beveiligingsincidenten		ensia-hrm|ensia-rvig|ensia-bkwi|ensia-brp
Boolean	1:Ja|0:Nee	Verificatie van de achtergrond van alle kandidaten voor een dienstverband, ingehuurd personeel en externe gebruikers behoort te worden uitgevoerd overeenkomstig relevante wetten, voorschriften en ethische overwegingen, en behoren evenredig te zijn aan de bedrijfseisen, de classificatie van de informatie waartoe toegang wordt verleend, en de waargenomen risico's. Zie ook hs 8.1.2 van de BIG: Screening p.26 Benodigde documentatie Actuele personeels dossiers, VOG's aanwezig in de dossier.	ensia-hrm|ensia-bkwi
Boolean	1:Ja|0:Nee		ensia-hrm|ensia-bkwi
Boolean	1:Ja|0:Nee		ensia-hrm|ensia-bkwi
Boolean	1:Ja|0:Nee		ensia-hrm|ensia-bkwi
Boolean	1:Ja|0:Nee	Als onderdeel van hun contractuele verplichting behoren werknemers, ingehuurd personeel en externe gebruikers de algemene voorwaarden te aanvaarden en te ondertekenen van hun arbeidscontract, waarin hun verantwoordelijkheden en die van de organisatie ten aanzien van informatiebeveiliging behoren te zijn vastgelegd. Zie ook hs 8.1.3 van de BIG: Arbeidsvoorwaarden p.27 Benodigde documentatie Algemene voorwaarden of huisregels bij in diensttreding, ondertekend in in P-dossier.	ensia-hrm

Boolean	1:Ja|0:Nee	Het lijnmanagement behoort van werknemers, ingehuurd personeel en externe gebruikers te eisen dat ze beveiliging toepassen overeenkomstig vastgesteld beleid en vastgestelde procedures van de organisatie. Dit is een BRP eis. Besluit BRP 6 Zie ook hs 8.2.1. van de BIG: Directieverantwoordelijkheid p.27 Benodigde documentatie Controle vragen aan personeel, verslagen van functioneringsgesprekken en werkbesprekingen	ensia-rvig|ensia-brp
Checkbox	0:uit verslagen van (werk)besprekingen|1:uit de verslagen van de functioneringsgesprekken		ensia-rvig|ensia-brp
Boolean	1:Ja|0:Nee	Alle werknemers van de organisatie en, voor zover van toepassing, ingehuurd personeel en externe gebruikers, behoren geschikte training en regelmatige bijscholing te krijgen met betrekking tot beleid en procedures van de organisatie, voor zover relevant voor hun functie. Dit is een BRP eis en een Suwi-norm. Besluit BRP 6 Suwinorm: U.02 Zie ook hs 8.2.2 van de BIG: Bewustwording, opleiding en training ten aanzien van informatiebeveiliging p.28 Benodigde documentatie Verslagen van POP gesprekken, inkoop bewustwording. SUWI guidance Onderdeel collegeverklaring Deze vraag en het antwoord zijn onderdeel van de Collegeverklaring die de gemeente moet afgeven in het kader van Suwinet. Onderdeel SUWI-norm Deze vraag is onderdeel van het specifiek suwinet normenkader voor afnemers en het antwoord wordt gerapporteerd aan SZW. Doelstelling SUWI Gebruikers en beheerders de juiste toegangsrechten geven (niet meer en niet minder) dan welke nodig zijn voor de hen opgedragen (wettelijke)taken. Criterium De Afnemer beheerst de toewijzing van autorisaties op basis van een formeel autorisatie beheerproces waarbij het van essentieel belang is, dat het wijzigen (ook intrekken of blokkeren) van toegangsrechten voor Suwinet tijdig wordt uitgevoerd. Nadere toelichting Scope: logische toegangsbeveiliging Betrokken: gemeenten, SVB, UWV Nadere Info: LTB procedures in place en gekoppeld aan HRM functie? Hanteren van need to know principe, gekoppeld aan HR functie-profielen (privacy uitgangspunten). SUWI-norm: U.02 Plaats in het opmerkingenveld hieronder de eventuele extra onderbouwing van uw antwoord voor de IT auditor.	ensia-hrm|ensia-inkoop|ensia-keycontrol|ensia-rvig|ensia-itaudit|ensia-bkwi|ensia-brp|ensia-pun|ensia-pnikni
Checkbox	0:met opleidingen en trainingen|1:met bewustwordingscampagnes		ensia-hrm|ensia-inkoop|ensia-keycontrol|ensia-rvig|ensia-isd|ensia-itaudit|ensia-brp|ensia-pun|ensia-pnikni
Boolean	1:Ja|0:Nee		ensia-hrm|ensia-inkoop|ensia-keycontrol|ensia-
Boolean	1:Ja|0:Nee		ensia-hrm|ensia-inkoop|ensia-keycontrol|ensia-rvig|ensia-isd|ensia-itaudit|ensia-brp|ensia-pun|ensia-pnikni
Boolean	1:Ja|0:Nee		ensia-hrm|ensia-inkoop|ensia-keycontrol|ensia-rvig|ensia-isd|ensia-itaudit|ensia-brp|ensia-pun|ensia-pnikni
Boolean	1:Ja|0:Nee	Er behoort een formeel disciplinair proces te zijn vastgesteld voor werknemers die inbreuk op de informatiebeveiliging hebben gepleegd. Dit is een BRP eis. Besluit BRP 6 Zie ook hs 8.2.3. van de BIG: Disciplinaire maatregelen p.28 Benodigde documentatie Er is beleid en er is een proces beschreven dat recht doet aan het onderwerp.	ensia-hrm|ensia-rvig|ensia-brp|ensia-bkwi
Boolean	1:Ja|0:Nee	Er behoort een formele procedure te zijn per organisatie (onderdeel) voor het beheerst wijzigen of beindigen van dienstverbanden, contracten of andere overeenkomsten waarin de informatiebeveiligingsaspecten nadrukkelijk aan de orde komen. Zoals bijvoorbeeld geheimhouding en intrekken / wijzigen rechten. Suwinorm: U.02 Zie ook hs 8.3.1. van de BIG: Beëindiging van verantwoordelijkheden p.28 Benodigde documentatie Procedure wijzigen/beindigen dienstverband.	ensia-hrm|ensia-isd
Boolean	1:Ja|0:Nee		ensia-bkwi
Boolean	1:Ja|0:Nee	Er behoren toegangsbeveiligingen (barrières zoals muren, toegangspoorten met kaartsloten of een bemande receptie) te worden aangebracht om ruimten te beschermen waar zich informatie en ICT-voorzieningen bevinden. Dit is een BRP en PUN eis. Besluit BRP 6 PUN 91 Zie ook hs 9.1.1. van de BIG: Fysieke beveiliging van de omgeving p.30 Benodigde documentatie Toegangsbeveiligingsbeleid.	ensia-facilitair|ensia-rvig|ensia-brp|ensia-pun|ensia-pnikni

Checkbox	0:Voor wat betreft de werkruimten|1:Voor de server- en SER-ruimten|2:Voor wat betreft de reisdocumenten|3:Voor wat betreft de ruimten waar persoonsgegevens verwerkt worden		ensia-facilitair|ensia-rvig|ensia-brp|ensia-pun|ensia-pnikni
Boolean	1:Ja|0:Nee		ensia-rvig|ensia-facilitair|ensia-brp|ensia-pun|ensia-pnikni
Boolean	1:Ja|0:Nee	Beveiligde zones behoren te worden beschermd door geschikte toegangsbeveiliging, om te bewerkstelligen dat alleen bevoegd personeel wordt toegelaten. Dit is een BRP eis. Besluit BRP 6 Zie ook hs 9.1.2 van de BIG: Fysieke toegangsbeveiliging p.31 Benodigde documentatie Bezoekersverslagen, autorisatie matrixen, toegangscontrole logging van pasjes en andere middelen en verslagen van de controle daarop.	ensia-facilitair|ensia-rvig|ensia-bkwi|ensia-brp
Boolean	1:Ja|0:Nee	Er behoort fysieke beveiliging van kantoren, ruimten en faciliteiten te worden ontworpen en toegepast. Dit is een BRP en PUN eis. Besluit BRP 6 PUN: 91 Zie ook hs 9.1.3. van de BIG: Beveiliging van kantoren, ruimten en faciliteiten p. 31 Benodigde documentatie Ontwerpen van kantoren, ruimten en faciliteiten.	ensia-facilitair|ensia-rvig|ensia-bkwi|ensia-brp|ensia-pun|ensia-pnikni
Checkbox	0:Voor de opslag van gegevensdragers|1:Er is een actief sleutelplan voor kluizen en sloten|2:Het is bekend waar incidenten gemeld kunnen worden		ensia-facilitair|ensia-rvig|ensia-bkwi|ensia-brp|ensia-pun|ensia-pnikni
Boolean	1:Ja|0:Nee	Er behoort fysieke bescherming tegen schade door brand, overstroming, aardschokken, explosies, oproer en andere vormen van natuurlijke of menselijke calamiteiten te worden ontworpen en toegepast. Zie ook hs 9.1.4 van de BIG: Bescherming tegen bedreigingen van buitenaf p.31 Benodigde documentatie Beleid waarin deze maatregelen staan, ontwerpen van gebouwen en ruimtes waarin deze maatregelen uitgwerkt zijn.	ensia-facilitair
Checkbox	0:Tegen brand|1:Tegen bliksem|2:Tegen overstroming|3:Tegen aardschokken|4:Tegen explosies|5:Tegen oproer		ensia-facilitair
Boolean	1:Ja|0:Nee	Er behoren een fysieke bescherming en richtlijnen voor werken in beveiligde ruimten te worden ontworpen en toegepast. Dit is een BRP en PUN eis en een sleutelmaatregel. Dit is een BRP en PUN eis. Besluit BRP 6 PUN 91 Zie ook hs 9.1.5. van de BIG: Werken in beveiligde ruimten p.32 Benodigde documentatie Voorschriften voor het werken in beveiligde ruimten.	ensia-facilitair|ensia-rvig|ensia-brp|ensia-brp|ensia-pun|ensia-pnikni
Checkbox	0:Voor bezoekers|1:Voor ongeautoriseerd personeel|2:Voor geautoriseerd personeel|3:Voor het maken van foto’s en video’s		ensia-facilitair|ensia-rvig|ensia-brp|ensia-pun|ensia-pnikni
Boolean	1:Ja|0:Nee	Toegangspunten zoals gebieden voor laden en lossen en andere punten waar onbevoegden het terrein kunnen betreden, behoren te worden beheerst en indien mogelijk worden afgeschermd van ICT-voorzieningen, om onbevoegde toegang te voorkomen. Dit is een BRP en PUN eis. Besluit BRP 6 PUN 91 Zie ook hs 9.1.6 van de BIG: Openbare toegang en gebieden voor laden en lossen p.32 Benodigde documentatie Ontwerpplan en procedures.	ensia-facilitair|ensia-rvig|ensia-brp|ensia-pun|ensia-pnikni
Boolean	1:Ja|0:Nee	Apparatuur behoort zo te worden geplaatst en beschermd dat risico's van schade en storing van buitenaf en de gelegenheid voor onbevoegde toegang wordt verminderd. Zie ook hs 9.2.1. van de BIG: Plaatsing en bescherming van apparatuur p.33 Benodigde documentatie Fysieke controle van apparatuur en controle of in de bouw en plaatsingsvoorschriften gebruik gemaakt is van geldende standaarden.	ensia-facilitair
Checkbox	0:Tegen blikseminslag en spanningsschommelingen|1:Tegen brand en waterschade|2:Tegen onbevoegde toegang		ensia-facilitair
Radiobutton	0:Nee|1:Ja, maatregelen|2:Ja, procedures|3:Ja, zowel procedures als maatregelen zijn geïplementeerd	Apparatuur behoort te worden beschermd tegen stroomuitval en andere storingen door onderbreking van nutsvoorzieningen. Zie ook hs 9.2.2. van de BIG: Nutsvoorzieningen p. 33 Benodigde documentatie Procedures en maatregelen stroomuitval (noodstroom, UPS, aggegraten), jaarlijkse testverslagen.	ensia-facilitair
Boolean	1:Ja|0:Nee	Voedings- en telecommunicatiekabels die voor dataverkeer of ondersteunende informatiediensten worden gebruikt, behoren tegen interceptie of beschadiging te worden beschermd conform de norm NEN 1010. Zie ook hs 9.2.3. van de BIG: Beveiliging van kabels p.33 Benodigde documentatie Specificaties van gebouw bekebelingen, gedocmenteerde patchlijst.	ensia-facilitair

Radiobutton	0:Nee|1:Ja, middels procedures|2:Ja, in onderhoudscontracten|3:Ja, middels procedures en onderhoudscontracten	Apparatuur behoort op correcte wijze te worden onderhouden, om te waarborgen dat deze voortdurend beschikbaar is en in goede staat verkeert. Zie ook hs 9.2.4 van de BIG: Onderhoud van apparatuur p.33 Benodigde documentatie Onderhoudscontracten, onderhoudsvoorschriften.	ensia-facilitair
Radiobutton	0:Nee|1:Ja, met maatregelen|2:Ja, met procedures|3:Ja, met maatregelen en procedures	Apparatuur buiten de terreinen behoort te worden beveiligd waarbij rekening wordt gehouden met de diverse risico's van werken buiten het terrein van de organisatie. Dit is een PUN eis. PUN 80, 80a, 90, 91 Zie ook hs 9.2.5 van de BIG: Beveiliging van apparatuur buiten het terrein p.34 Benodigde documentatie Thuiswerk beleid, telewerkbeleid, inrichting werkplek/mobiele devices, encryptiebeleid, gedragscodes.	ensia-hrm|ensia-rvig|ensia-pun|ensia-pnikni
Boolean	1:Ja|0:Nee	Alle apparatuur die opslagmedia bevat, behoort te worden gecontroleerd om te bewerkstelligen dat alle gevoelige gegevens en in licentie gebruikte programmatuur zijn verwijderd of veilig zijn overschreven voordat de apparatuur wordt verwijderd. Zie ook hs 9.2.6 van de BIG: Veilig verwijderen of hergebruiken van apparatuur p.34 Benodigde documentatie Procedure veilig verwijderen van gevoelige bedrijfsinformatie.	ensia-facilitair
Boolean	1:Ja|0:Nee	Apparatuur, informatie en programmatuur van de organisatie mogen niet zonder toestemming vooraf van de locatie worden meegenomen. Zie ook hs 9.2.7 van de BIG: Verwijdering van bedrijfseigendommen p.34 Benodigde documentatie Procedure omgang ICT-middelen.	ensia-facilitair
Boolean	1:Ja|0:Nee	Bedieningsprocedures behoren te worden gedocumenteerd, te worden bijgehouden en beschikbaar te worden gesteld aan alle gebruikers die deze nodig hebben. Bedieningsprocedures bevatten informatie over opstarten, afsluiten, back-up- en herstelacties, afhandelen van fouten, beheer van logs, contactpersonen, noodprocedures en speciale maatregelen voor beveiliging. Er zijn procedures voor de behandeling van digitale media die ingaan op ontvangst, opslag, rubricering, toegangsbeperkingen, verzending, hergebruik en vernietiging. Dit is een BRP eis. Besluit BRP 6, LO 7.4.1 Zie ook hs 10.1.1 van de BIG: Gedocumenteerde bedieningsprocedures p.35 Benodigde documentatie Bedieningsprocedures systeembeheer, netwerkbeheer, applicatiebeheer, opstart handleidingen, afsluit handledingen, back-up en restore procedures, gebruikershandleidingen.	ensia-rvig|ensia-brp
Boolean	1:Ja|0:Nee	Bedieningsprocedures en configuratie beschrijvingen behoren erop te zijn gericht dat netwerkcomponenten en servers alleen de strikt noodzakelijke software en instellingen bevatten (hardening). Dit is een Suwi eis. Suwinorm:U.10 Zie ook hs 10.1.1 van de BIG: Gedocumenteerde bedieningsprocedures p.35 Benodigde documentatie Beheer procedures voor hardenen van infrastructuur en servers.	ensia-isd
Boolean	1:Ja|0:Nee	Wijzigingsbeheer zorgt ervoor dat alle instellingen van de ICT-infrastructuur gecontroleerd en geautoriseerd gewijzigd worden, dit geldt dus ook voor de hardeningsmaatregelen. Wijzigingen moeten eerst worden getest in een test- of acceptatieomgeving om de impact van de maatregelen vast te stellen. Dit zorgt ervoor dat de ICT-infrastructuur aan de gestelde maatregelen blijft voldoen. Het aanbrengen van bijvoorbeeld nieuwe verbindingen tussen netwerkcomponenten kan ervoor zorgen dat routepaden en compartimenteringen 'plotseling' ongewenst wijzigen. Suwinorm: C.03 Zie ook hs 10.1.2 van de BIG: Wijzigingsbeheer p.35 Benodigde documentatie Procedure wijzigingsbeheer, verslagen wijzigingsbeheer vergaderingen.	ensia-isd
Boolean	1:Ja|0:Nee		ensia-isd
Boolean	1:Ja|0:Nee	Taken en verantwoordelijkheidsgebieden behoren te worden gescheiden om gelegenheid voor onbevoegde of onbedoelde wijziging of misbruik van de bedrijfsmiddelen van de organisatie te verminderen. Dit is een BRP en Suwi eis. Besluit BRP 6, LO 7.4.1 Suwinorm: B.05 Zie ook hs 10.1.3 van de BIG: Functiescheiding p.35 Benodigde documentatie Functieprofielen en functie of rollen beschijvingen zijn toegwezen aan natuurlijk en verschillende personen. SUWI guidance Onderdeel collegaverklaring Deze vraag en het antwoord zijn onderdeel van de Collegeverklaring die de gemeente moet afgeven in het kader van Suwinet. Onderdeel SUWI-norm Deze vraag is onderdeel van het specifiek suwinet normenkader voor afnemers en het antwoord wordt gerapporteerd aan SZW. Doelstelling SUWI Ervoor zorgen dat de juiste taken en verantwoordelijkheden binnen de onderkende rollen juist worden uitgevoerd met inachtneming van de juiste functiescheiding voor zover de organisatiegrootte dit toelaat. Criterium De aangesloten organisatie op Suwinet heeft de type-rollen onderkend, de daarbij behorende de taken en verantwoordelijkheden vastgesteld en vastgelegd en noodzakelijke functiescheiding beschreven. Nadere toelichting Scope: ITGC organigram Betrokken: gemeenten, SVB, UWV Nadere Info: verdeling van verantwoordelijkheden (GeVS) gebaseerd op controle technische CFS, gekoppeld aan rules based acces control inrichting (HR). SUWI-norm: B.05 Plaats in het opmerkingenveld hieronder de eventuele extra onderbouwing van uw antwoord voor de IT auditor.	ensia-hrm|ensia-isd|ensia-burgerzaken|ensia-itaudit|ensia-rvig|ensia-brp|ensia-pun|ensia-pnikni
Checkbox	0:Dit hebben we gedaan voor de functies van BRP, PUN en SUWI|1:De rol van CISO of controller informatiebeveiliging is apart, onafhankelijk belegd		ensia-hrm|ensia-burgerzaken|ensia-isd|ensia-itaudit|ensia-brp|ensia-pun|ensia-pnikni

Checkbox	0:Systeembeheerder|1:Applicatiebeheerder BRP|2:Gegevensbeheerder BRP|3:Privacybeheerder BRP|4:Security Officer SUWI|5:Toezichthouder BRP|6:Geen van bovenstaande	Taken en verantwoordelijkheidsgebieden behoren te worden gescheiden om gelegenheid voor onbevoegde of onbedoelde wijziging of misbruik van de bedrijfsmiddelen van de organisatie te verminderen. Dit is een BRP en Suwi eis. Besluit BRP 6, LO 7.4.1 Suwinorm: B.05 Zie ook hs 10.1.3 uit de BIG: Functiescheiding p.35 Benodigde documentatie Beleidsnotitie, functiebeschrijvingen van de in de vraag genoemde functies/rollen. SUWI guidance Onderdeel collegaverklaring Deze vraag en het antwoord zijn onderdeel van de Collegeverklaring die de gemeente moet afgeven in het kader van Suwinet. Onderdeel SUWI-norm Deze vraag is onderdeel van het specifiek suwinet normenkader voor afnemers en het antwoord wordt gerapporteerd aan SZW. Doelstelling SUWI Ervoor zorgen dat de juiste taken en verantwoordelijkheden binnen de onderkende rollen juist worden uitgevoerd met inachtneming van de juiste functiescheiding voor zover de organisatiegrootte dit toelaat. Criterium De aangesloten organisatie op Suwinet heeft de type-rollen onderkend, de daarbij behorende de taken en verantwoordelijkheden vastgesteld en vastgelegd en noodzakelijke functiescheiding beschreven. Nadere toelichting Scope: ITGC organigram Betrokken: gemeenten, SVB, UWV Nadere Info: verdeling van verantwoordelijkheden (GeVS) gebaseerd op controle technische CFS, gekoppeld aan rules based acces control inrichting (HR). SUWI-norm: B.05 Plaats in het opmerkingenveld hieronder de eventuele extra onderbouwing van uw antwoord voor de IT auditor.	ensia-isd|ensia-burgerzaken|ensia-hrm|ensia-itaudit|ensia-rvig|ensia-brp|ensia-pun|ensia-pnikni
Radiobutton	0:Ja, tussen de uitvoerder en de beveiligingsfunctionaris|1:Ja, tussen de opdrachtgever en de beveiligingsfunctionaris|2:Er is geen scheiding in verantwoordelijkheden	Het gaat hierbij om de beveiligingsfunctionaris reisdocumenten. Dit is een BRP en PUN eis. Besluit BRP 6, LO 7.4.1 PUN 11 Zie ook hs 10.1.3 van de BIG: Functiescheiding p.35 SUWI guidance Onderdeel collegaverklaring Deze vraag en het antwoord zijn onderdeel van de Collegeverklaring die de gemeente moet afgeven in het kader van Suwinet. Onderdeel SUWI-norm Deze vraag is onderdeel van het specifiek suwinet normenkader voor afnemers en het antwoord wordt gerapporteerd aan SZW. Doelstelling SUWI Ervoor zorgen dat de juiste taken en verantwoordelijkheden binnen de onderkende rollen juist worden uitgevoerd met inachtneming van de juiste functiescheiding voor zover de organisatiegrootte dit toelaat. Criterium De aangesloten organisatie op Suwinet heeft de type-rollen onderkend, de daarbij behorende de taken en verantwoordelijkheden vastgesteld en vastgelegd en noodzakelijke functiescheiding beschreven. Nadere toelichting Scope: ITGC organigram Betrokken: gemeenten, SVB, UWV Nadere Info: verdeling van verantwoordelijkheden (GeVS) gebaseerd op controle technische CFS, gekoppeld aan rules based acces control inrichting (HR). SUWI-norm: B.05 Plaats in het opmerkingenveld hieronder de eventuele extra onderbouwing van uw antwoord voor de IT auditor.	ensia-burgerzaken|ensia-isd|ensia-itaudit|ensia-rvig|ensia-brp|ensia-pun|ensia-pnikni
Radiobutton	0:Nee|1:Er wordt alleen software ontwikkeld|2:Er wordt alleen software getest|3:Er wordt zowel software ontwikkeld als getest	Faciliteiten voor ontwikkeling, testen en productie behoren te zijn gescheiden om het risico van onbevoegde toegang tot of wijzigingen in het productiesysteem te verminderen. Er zijn minimaal logisch gescheiden systemen voor Ontwikkeling, Test en/of Acceptatie en Productie (OTAP). De systemen en applicaties in deze zones beïnvloeden systemen en applicaties in andere zones niet. Gebruikers hebben gescheiden gebruiksprofielen voor Ontwikkeling, Test en/of Acceptatie en Productiesystemen om het risico van fouten te verminderen. Het moet duidelijk zichtbaar zijn in welk systeem gewerkt wordt. Indien er een experimenteer of laboratorium omgeving is, is deze fysiek gescheiden van de productieomgeving. Suwinorm: U.09 Zie ook hs 10.1.4 van de BIG: Scheiding van faciliteiten voor ontwikkeling, testen en productie p.36 Benodigde documentatie Organisatie beschrijving, bedieningsprocedures, ICT landschap.	ensia-isd
Boolean	1:Ja|0:Nee		ensia-isd
Boolean	1:Ja|0:Nee	Er behoort te worden bewerkstelligd dat de beveiligingsmaatregelen, definities van dienstverlening en niveaus van dienstverlening zoals vastgelegd in de overeenkomst voor dienstverlening door een derde partij worden geïmplementeerd en uitgevoerd en worden bijgehouden door die derde partij. Dit is een BRP eis. Besluit BRP 8,9 Zie ook hs 10.2.1 van de BIG: Dienstverlening p.36 Benodigde documentatie Bewerkersovereenkomsten voor iedere uitbestede verwerking volgens model van de IBD. Inkoopcontracten, leveranciersmanagement ingericht, pentest rapporten, jaarlijkse TPM's, getekende geheimhoudingsverklaringen, geheimhoudingsparagraaf in inkoopcontracten.	ensia-rvig|ensia-brp

Checkbox	0:Maatregelen gericht op medewerkers|1:Maatregelen gericht op de toegang tot gebouwen en ruimten|2:Maatregelen gericht op een deugdelijke werking van de apparatuur en programmatuur|3:Maatregelen gericht op de beveiliging van de apparatuur en programmatuur|4:Maatregelen gericht op het gegevensbeheer|5:Maatregelen ingeval van schending van de geheimhouding|6:Maatregelen ingeval van calamiteiten|7:Gebruik van gegevens uitsluitend voor de afgesproken werkzaamheden|8:De bewerker houdt zich aan de wettelijke voorschriften|9:De bewerker staat toe dat de gemeente controles uitvoert|10:Werkzaamheden worden opgeschort op vordering van de gemeente|11:Werkzaamheden worden zonder toestemming van de gemeente door de bewerker niet uitbesteed		ensia-rvig|ensia-brp
Checkbox	0:Er is intern door de gemeente zelf een controle uitgevoerd|1:De IT-leverancier heeft een toets uit laten voeren|2:Een externe deskundige heeft een controle uitgevoerd|3:Een een externe IT-leverancier heeft een controle uitgevoerd|4:Er is niet getoetst	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. Dit is een BRP eis. Besluit BRP 8,9 Zie ook hs 10.2.2 van de BIG Controle en beoordeling van dienstverlening door een derde partij p.37 Benodigde documentatie TPM's van leveranciers, niet ouder dan 1 jaar.	ensia-rvig|ensia-brp
Boolean	1:Ja|0:Nee		ensia-rvig|ensia-brp
Boolean	1:Ja|0:Nee	Wijzigingen in de dienstverlening door derden, waaronder het bijhouden en verbeteren van bestaande beleidslijnen, procedures en maatregelen voor informatiebeveiliging, behoren te worden beheerd, waarbij rekening wordt gehouden met de mogelijke onmisbaarheid van de betrokken bedrijfssystemen en -processen en met heroverweging van risico's. Zie ook hs 10.2.3 van de BIG: Beheer van wijzigingen in dienstverlening door een derde partij p.37 Benodigde documentatie Verslagen van gesprekken met leveranciers, TPM's.	
Boolean	1:Ja|0:Nee	Het gebruik van middelen behoort te worden gecontroleerd en afgestemd en er behoren verwachtingen te worden opgesteld voor toekomstige capaciteitseisen, om de vereiste systeemprestaties te bewerkstelligen. Zie ook hs 10.3.1 van de BIG: Capaciteitsbeheer p.37 Benodigde documentatie Informatieplan en capaciteitsplan.	ensia-bkwi
Boolean	1:Ja|0:Nee	Er behoren aanvaardingscriteria te worden vastgesteld voor nieuwe informatiesystemen, upgrades en nieuwe versies en er behoort een geschikte test van het systeem of de systemen te worden uitgevoerd tijdens ontwikkeling en voorafgaand aan de acceptatie. Suwinorm: C.03 Zie ook hs 10.3.2 van de BIG: Systeem acceptatie p.38 Benodige documentatie Architectuur principes, bij systemen moet een testdossier aanwezig zijn (testplannen, testverslagen, acceptatie verslagen).	ensia-isd
Checkbox	0:Detectieve maatregelen (scanners)|1:Preventieve maatregelen (patching en hardening)|2:Recovery maatregelen (back-up)|3: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. Dit is een sleutelmaatregel. Zie ook hs 10.4.1 van de BIG: Maatregelen tegen virussen p.38 Benodigde documentatie Antivirus beleid en procedures.	

Radiobutton	0:Java/Flash wordt door ons niet beschikbaar gesteld|1:Java/Flash wordt door ons met minimale rechten beschikbaar gesteld|2:Java/Flash wordt in een logisch geïsoleerde omgeving uitgevoerd|3:Java/Flash wordt door ons vrij beschikbaar gesteld	Als gebruik van 'mobile code' is toegelaten, behoort de configuratie te bewerkstelligen dat de geautoriseerde 'mobile code' functioneert volgens een duidelijk vastgesteld beveiligingsbeleid, en behoort te worden voorkomen dat onbevoegde 'mobile code' wordt uitgevoerd. Zie ook hs 10.4.2 van de BIG: Maatregelen tegen 'mobile code' p.39 Benodigde documentatie Systeembeheer documentatie, beleid, testverslagen.	
Boolean	1:Ja|0:Nee	Er behoren back-upkopieën van informatie en programmatuur te worden gemaakt en regelmatig te worden getest overeenkomstig het vastgestelde back-upbeleid. Dit is een BRP en PUN eis en een BAG eis.. Besluit BRP 6 PUN 92 BAG: 5.4.2 Zie ook hs 10.5.1 van de BIG: 10.5.1 Reservekopieën maken (back-ups) p.39 Benodigde documentatie Backup procedures, backup verslagen.	ensia-burgerzaken|ensia-bouwenenwonen|ensia-pun|ensia-pnikni
Checkbox	0:Voor de BRP|1:Voor RAAS ingevolge art 92 PUN|2:Voor de BAG|3:Deze is generiek ingericht voor alle data en informatie		ensia-burgerzaken|ensia-bouwenenwonen|ensia-rvig|ensia-brp|ensia-pun|ensia-pnikni
Checkbox	0:Wij hebben geen maatregelen genomen|1:Wij hebben dit uitbesteed bij een andere gemeente/leverancier|2:Wij hebben op alle vertrouwde koppelvlakken een beheerde firewall|3:Wij maken generiek gebruik van een IDS|4:Wij doen aan content scanning|5:Wij maken gebruik van een SIEM|6:De gegevensuitwisseling tussen vertrouwde en onvertrouwde zones worden inhoudelijk geautomatiseerd en gecontroleerd op de aanwezigheid van malware|7:Bij transport van vertrouwelijke informatie over onvertrouwde netwerken (zoals het internet), wordt geschikte encryptie toegepast. Zie ook vraag 12.3.1.|8:Er zijn procedures voor beheer van apparatuur op afstand	Netwerken behoren adequaat te worden beheerd en beheerst om ze te beschermen tegen bedreigingen en om beveiliging te handhaven voor de systemen en toepassingen die gebruikmaken van het netwerk, waaronder informatie die wordt getransporteerd. Dit is een BRP bepaling. Circulaire BPR/U59776 Zie ook hs 10.6.1 van de BIG: Maatregelen voor netwerken p.40 Benodigde documentatie Netwerkplan, beleid, controle verslagen, ingericht proces netwerkbeheer, rapportages.	ensia-rvig|ensia-keycontrol|ensia-pun|ensia-pnikni|ensia-isd
Boolean	1:Ja|0:Nee	Netwerken behoren adequaat te worden beheerd en beheerst om ze te beschermen tegen bedreigingen en om beveiliging te handhaven voor de systemen en toepassingen die gebruikmaken van het netwerk, waaronder informatie die wordt getransporteerd. Zie ook hs 10.6.1 van de BIG: Maatregelen voor netwerken p.40 Benodigde documentatie Netwerk beveiligingsplan.	ensia-isd
Boolean	1:Ja|0:Nee	Beveiligingskenmerken, niveaus van dienstverlening en beheereisen voor alle netwerkdiensten behoren te worden geïdentificeerd en opgenomen in elke overeenkomst voor netwerkdiensten, zowel voor diensten die intern worden geleverd als voor uitbestede diensten. Zie ook hs 10.6.2 van de BIG: Beveiliging van netwerkdiensten p.40 Benodigde documentatie Overeenkomsten voor netwerkdiensten, SLA's, bewerkeringsovereenkomsten.	ensia-isd
Boolean	1:Ja|0:Nee	Er behoren procedures te zijn vastgesteld voor het beheer van verwijderbare media. Zie ook vraag 10.8.3 Dit is een PUN eis en een sleutelmaatregel. PUN 91 Zie ook hs 10.7.1 van de BIG: Beheer van verwijderbare media p.40 Benodigde documentatie Procedure gebruik, beheer en afvoer van verwijderbare media, zoals harddisken, mobiele devices, usb sticks, cd-roms.	ensia-burgerzaken|ensia-rvig|ensia-pun|ensia-pnikni
Boolean	1:Ja|0:Nee	Artikel 91 Paspoortuitvoeringsregeling Nederland 2001	ensia-burgerzaken|ensia-rvig|ensia-pun|ensia-pnikni

Boolean	1:Ja|0:Nee	Media behoren op een veilige en beveiligde manier te worden verwijderd als ze niet langer nodig zijn, overeenkomstig formele procedures. Zie ook hs 10.7.2. van de BIG: Verwijdering van media p.41 Benodigde documentatie Media behoren op een veilige en beveiligde manier te worden verwijderd als ze niet langer nodig zijn, overeenkomstig formele procedures.	
Radiobutton	0:Nee|1:Ja|2:Alleen voor verwijderbare media|3:Alleen voor het verwijderen van vertrouwelijke data (van harddisken)		
Boolean	1:Ja|0:Nee	Er behoren procedures te worden vastgesteld voor de behandeling en opslag van informatie om deze te beschermen tegen onbevoegde openbaarmaking of misbruik. Zie ook hs 10.7.3 van de BIG: Procedures voor de behandeling van informatie p.41 Benodigde documentatie behandelplan, classificatieverslagen, registratie van gegevensverzamelingen, markeringen op kopieen.	
Checkbox	0:Gevoelige en vertrouwelijke informatie mag niet buiten het gemeentelijke netwerk (DMZ) opgeslagen worden|1:Gevoelige en vertrouwelijke informatie mag alleen encrypted op losse draagbare media of in clouddiensten opgeslagen worden|2:Er is clean desk policy		
Boolean	1:Ja|0:Nee	Systeemdocumentatie behoort te worden beschermd tegen onbevoegde toegang. Zie ook hs 10.7.4 van de BIG: Beveiliging van systeemdocumentatie p.41 Benodigde documentatie Beheer procedures voor systeem documentatie.	
Boolean	1:Ja|0:Nee		
Boolean	1:Ja|0:Nee		
Boolean	1:Ja|0:Nee	Er behoren formeel beleid, formele procedures en formele beheersmaatregelen te zijn vastgesteld om de uitwisseling van informatie via het gebruik van alle typen communicatiefaciliteiten te beschermen. Suwinorm: U.07, U.08 Zie ook hs 10.8.1 van de BIG: Beleid en procedures voor informatie-uitwisseling p.42 Benodigde documentatie Antivirusbeleid, antivirus maatregelen, antispam, content filterin, firewall/appliances.	ensia-isd
Checkbox	0:Voor transport van geclassificeerde informatie|1:Voor faxen en e-mail|2:Voor mobiele apparaten|3:Voor printers		ensia-isd
Boolean	1:Ja|0:Nee		ensia-isd
Boolean	1:Ja|0:Nee	Er behoren overeenkomsten te worden vastgesteld voor de uitwisseling van informatie en programmatuur tussen de organisatie en externe partijen. De beveiligingsinhoud van elke overeenkomst behoort in overeenstemming te zijn met de gevoeligheid van de desbetreffende bedrijfsinformatie. Zie ook hs 10.8.2. van de BIG: Uitwisselingsovereenkomsten p.42 Benodigde documentatie Bewerkersovereenkomsten, overeenkomst informatie uitwisseling.	ensia-bkwi
Checkbox	0:Onweerlegbaarheid|1:Betrouwbaarheid|2:Eigenaarschap		ensia-bkwi
Boolean	1:Ja|0:Nee		ensia-bkwi
Boolean	1:Ja|0:Nee	Media die informatie bevatten behoren te worden beschermd tegen onbevoegde toegang, misbruik of corrumperen tijdens transport buiten de fysieke begrenzing van de organisatie. Zie ook hs 10.8.3 van de BIG: Fysieke media die worden getransporteerd p.43 Benodigde documentatie Procedure omgang gevoelige media.	ensia-bkwi

Boolean	1:Ja|0:Nee	Informatie die een rol speelt bij elektronische berichtuitwisseling behoort op geschikte wijze te worden beschermd. Suwinorm: U.07, U.08 Zie ook hs 10.8.4 van de BIG: Elektronisch berichtenuitwisseling p.43 Benodigde documentatie Procedure / aanwijzing / protocol uitwisseling van vertrouwelijke informatie.	ensia-isd
Checkbox	0:PKI|1:Encryptie|2:PKI-Overheid		ensia-isd
Boolean	1:Ja|0:Nee	Beleid en procedures behoren te worden ontwikkeld en geïmplementeerd om informatie te beschermen die een rol speelt bij de onderlinge koppeling van systemen voor bedrijfsinformatie. Zie ook hs 10.8.5 van de BIG: Systemen voor bedrijfsinformatie p.43 Benodigde documentatie Beleid en procedures voor koppeling van bedrijfssystemen.	
Boolean	1:Ja|0:Nee		
Boolean	1:Ja|0:Nee		
Boolean	1:Ja|0:Nee	Informatie die een rol speelt bij e-commerce en die via openbare netwerken wordt uitgewisseld, behoord te worden beschermd tegen frauduleuze activiteiten, geschillen over contracten en onbevoegde openbaarmaking en modificatie. Zie ook hs 10.8.9 van de BIG: E-commerce p.44 Benodigde documentatie Cryptografie beleid en procedures.	ensia-isd
Radiobutton	0:Voor producten en diensten waarvoor authenticatie nodig is (digid)|1:Voor producten en diensten met financiële transacties(ogone)|2:Voor andere diensten dan DigiD en bijvoorbeeld Ogone|3:Geen van de hieroven genoemde antwoorden	Voor producten en diensten waarvoor authenticatie nodig is (digid) Voor producten en diensten met financiële transacties(ogone) Geen van de hieroven genoemde antwoorden	ensia-isd
Boolean	1:Ja|0:Nee	De betrouwbaarheid van de informatie die beschikbaar wordt gesteld op een openbaar toegankelijk systeem behoort te worden beschermd om onbevoegde modificatie te voorkomen. Zie ook hs 10.9.3. van de BIG: Openbaar beschikbare informatie p.44 Benodigde documentatie Beheerprocedures webservers, inrichtingsdocumentatie.	
Radiobutton	0:Nee (dat is uitbesteed)|1:Ja	Activiteiten van gebruikers, uitzonderingen en informatiebeveiligingsgebeurtenissen behoren te worden vastgelegd in audit-logbestanden. Deze logbestanden behoren gedurende een overeengekomen periode te worden bewaard, ten behoeve van toekomstig onderzoek en toegangscontrole. Dit is een eis vanuit Suwi en BRP. Besluit BRP 6, LO 4.2 Suwinorm: C.05 Zie ook hs 10.10.1 van de BIG: Aanmaken audit-logbestanden p.44 Benodigde documentatie Logging procedure met aandacht voor bescherming en autorisatie op logging. SUWI guidance Onderdeel collegeverklaring Deze vraag en het antwoord zijn onderdeel van de Collegeverklaring die de gemeente moet afgeven in het kader van Suwinet. Onderdeel SUWI-norm Deze vraag is onderdeel van het specifiek suwinet normenkader voor afnemers en het antwoord wordt gerapporteerd aan SZW. SUWI doelstelling Alle handelingen die betrekking hebben op gebruikers en beheerders moe-ten herleidbaar zijn naar individuele personen. De log-informatie wordt regelmatig gemonitord (signaleren, analyseren rapporteren en bijsturen) Criterium Activiteiten van gebruiker en beheerders, uitzonderingen en informatiege-beurtenissen behoren te worden vastgelegd in audit-logbestanden en te worden bewaard, ten behoeve van controles. Bewerkstellingen dat tijdig correctieve maatregelen kunnen worden getroffen en informatie te kunnen verschaffen over activiteiten van gebruikers en beheerders van de Suwinet diensten en vaststellen of oneigenlijk gebruik of misbruik is gemaakt van autorisatie. Nadere toelichting Scope: logische toegangsbeveiliging Betrokken: gemeenten, SVB, UWV Nadere Info: credentials, persoonsgebonden, uitgifte gekoppekd aan HR processen. Gebruik maken van logging van alle bijzondere transacties in beveiligde bestanden, met in achtneming van de bewaartermijnen, volgens privacy uitgangspunten. Procedure voor bijzondere handelingen benoemen. Nadere Info: interne controle functie moet beschikken over controle lijsten en controleren tbv tbv bestuur/management. Dit ism systeembeheer / IB coordinatie die op weekbasis loggen en indien ad hoc ingrijpen. Rapportering over te nemen maatregelen, scenario moet gedocumenteerd klaar liggen. SUWI-norm: C.05, C.06 Plaats in het opmerkingenveld hieronder de eventuele extra onderbouwing van uw antwoord voor de IT auditor.	ensia-itaudit|ensia-isd|ensia-rvig|ensia-brp

Checkbox	0:Nee|1:Ja, voor wat betreft Suwinet-inlezen en DKD-inlezen|2:Ja, voor wat betreft BRP|3:Ja, voor wat betreft DigiD|4:Ja, voor overige systemen		ensia-itaudit|ensia-isd|ensia-rvig|ensia-brp
Boolean	1:Ja|0:Nee		ensia-itaudit|ensia-isd|ensia-rvig|ensia-brp
Boolean	1:Ja|0:Nee	Onder administratieve handelingen wordt verstaan: het vastleggen van handelingen die niet in het systeem gelogd worden. bijvoorbeeld emails, verslagen van vergaderingen, wijzigingsvoorstellen.	ensia-itaudit|ensia-isd|ensia-rvig|ensia-brp
Boolean	1:Ja|0:Nee		ensia-itaudit|ensia-isd|ensia-rvig|ensia-brp
Boolean	1:Ja|0:Nee	Er behoren procedures te worden vastgesteld om het gebruik van ICT-voorzieningen te controleren. Het resultaat van de controleactiviteiten behoort regelmatig te worden beoordeeld. Dit is een Suwi en BRP eis. Besluit BRP 6, LO 4.2 Suwinorm: C.06 Zie ook hs 10.10.2 van de BIG: Controle van systeemgebruik p.45 Benodigde documentatie Er moeten controle verslagen zijn van de controle van het gebruik van belangrijke personnsgegevens verzamelingen zoals die van Suwi en BRP. Er moet een proces zijn waarin de procedure is uitgewerkt. SUWI guidance Onderdeel collegeverklaring Deze vraag en het antwoord zijn onderdeel van de Collegeverklaring die de gemeente moet afgeven in het kader van Suwinet. Onderdeel SUWI-norm Deze vraag is onderdeel van het specifiek suwinet normenkader voor afnemers en het antwoord wordt gerapporteerd aan SZW. SUWI doelstelling De log-informatie wordt regelmatig gemonitord (signaleren, analyseren rapporteren en bijsturen) Bewerkstelligen dat zich geen leemtes in de beveiliging van IAA mechanismen voordoen. Criterium Bewerkstellingen dat tijdig correctieve maatregelen kunnen worden getroffen en informatie te kunnen verschaffen over activiteiten van gebruikers en beheerders van de Suwinet diensten en vaststellen of oneigenlijk gebruik of misbruik is gemaakt van autorisatie. De Afnemer voert periodiek evaluaties op de technische en organisatorische beoordelingsrapportages en neemt noodzakelijke verbeteracties. Nadere toelichting Scope: logische toegangsbeveiliging en verantwoording afleggen (tevens preventief) // systeembeheer Betrokken: gemeenten, SVB, UWV Nadere Info: interne controle functie moet beschikken over controle lijsten en controleren tbv tbv bestuur/management. Dit ism systeembeheer / IB coordinatie die op weekbasis loggen en indien ad hoc ingrijpen. Rapportering over te nemen maatregelen, scenario moet gedocumenteerd klaar liggen. Uitgangspunt is dat de uitvoering van deze evaluaties maandelijks plaatsvindt; in specifieke situaties kan hiervan worden afgeweken, hetgeen in dat geval in de verantwoordings-/transparantierapportage dient te worden toegelicht SUWI-norm: C.06, C.07 Plaats in het opmerkingenveld hieronder de eventuele extra onderbouwing van uw antwoord voor de IT auditor.	ensia-isd|ensia-itaudit|ensia-rvig|ensia-brp
Checkbox	0:Voor wat betreft SUWI|1:Voor wat betreft BRP|2:Voor wat betreft DigiD		ensia-isd|ensia-itaudit|ensia-rvig|ensia-brp
Boolean	1:Ja|0:Nee	Logfaciliteiten en informatie in logbestanden behoren te worden beschermd tegen inbreuk en onbevoegde toegang. Suwinorm: C.05 Zie ook hs 10.10.3 van de BIG: Bescherming van informatie in logbestanden p.46	ensia-isd
Boolean	1:Ja|0:Nee	De klokken van alle relevante informatiesystemen binnen een organisatie of beveiligingsdomein behoren te worden gesynchroniseerd met een overeengekomen nauwkeurige tijdsbron. Zie ook hs 10.10.6 van de BIG: Synchronisatie van systeemklokken p.46 Benodigde documentatie Procedure controle systeemklokken.	ensia-bkwi
Boolean	1:Ja|0:Nee	Er behoort toegangsbeleid te worden vastgesteld, gedocumenteerd en beoordeeld op basis van bedrijfseisen en beveiligingseisen voor toegang. Dit is een BRP en PUN eis. Besluit BRP 6 PUN 90 Zie ook hs 11.1.1 van de BIG: Toegangsbeleid p.47 Benodigde documentatie Kopie van toegangsbeleid, kopie van notulen waarin de toegangsbeleid is goedgekeurd door ma-nagement, kopie flyers, nieuwsbrieven of e-mails waaruit blijkt dat de gebruikers op de hoogte zijn van de goedgekeurde toegangsbeleid, kopie van informatie waarin is beoordeeld dat de bedrijfseisen en beveiligingseisen voor toegang zijn meegenomen in het beleid. Te denken aan:kopie risicoanalyse, kopie de toegepaste normenkader of wetregelgeving voor het beleid.	ensia-rvig|ensia-brp|ensia-pun|ensia-pnikni

Boolean	1:Ja|0:Nee	Er behoren formele procedures voor het registreren en afmelden van gebruikers te zijn vastgesteld, voor het verlenen en intrekken van toegangsrechten tot alle informatiesystemen en -diensten. Dit is een BRP, PUN en Suwi eis. Besluit BRP 6 PUN 90 Suwinorm: U.02, U.03 Zie ook hs 11.2.1. van de BIG: Registratie van gebruikers p.47 Benodigde documentatie Procedurebeschrijvingen die beschikbaar zijn voor registreren en afmelden van gebruikers voor enkele informatiesystemen of -diensten, kopie procedurebeschrijving voor de registratie van gebruikers en be-heerders, kopie van informatie waaruit blijkt dat de organisatie gebruiker-id's conform de procedures heeft toegekend. Te denken aan: kopie van aanvraagformulieren voor gebruikers-id's, kopie uit systeem waaruit blijkt dat de gebruikers een unieke gebruikersidentificatie (ID) hebben,kopie twee meest recente rapportage waaruit blijkt dat de organisa-tie controle uitvoert op verwijderen of blokkeren van overtollige gebruiker-id's en accounts. SUWI guidance Onderdeel collegeverklaring Deze vraag en het antwoord zijn onderdeel van de Collegeverklaring die de gemeente moet afgeven in het kader van Suwinet. Onderdeel SUWI-norm Deze vraag is onderdeel van het specifiek suwinet normenkader voor afnemers en het antwoord wordt gerapporteerd aan SZW. Doelstelling SUWI Gebruikers en beheerders de juiste toegangsrechten geven (niet meer en niet minder) dan welke nodig zijn voor de hen opgedragen (wettelijke)taken. Bewerkstelligen dat de geclaimde identiteit van de gebruiker kan worden bewezen en dat daardoor alleen bevoegde gebruikers toegang krijgen tot Suwinet diensten. Criterium De Afnemer beheerst de toewijzing van autorisaties op basis van een formeel autorisatie beheerproces waarbij het van essentieel belang is, dat het wijzigen (ook intrekken of blokkeren) van toegangsrechten voor Suwinet tijdig wordt uitgevoerd. Elke gebruiker/beheerder behoort over een unieke identificatiecode te beschikken (User-ID) voor uitsluitend persoonlijk gebruik, ook behoort een geschikte authenticatie techniek te worden gekozen. Nadere toelichting Scope: logische toegangsbeveiliging Betrokken: gemeenten, SVB, UWV Nadere Info: LTB procedures in place en gekoppeld aan HRM functie? Hanteren van need to know principe, gekoppeld aan HR functie-profielen (privacy uitgangspunten). Nadere Info: zorg dragen voor strong authentication (two factor authentication) dan wel ayer multi factor authentication SUWI-norm U.02, U.03 Plaats in het opmerkingenveld hieronder de eventuele extra onderbouwing van uw antwoord voor de IT auditor.	ensia-isd|ensia-itaudit|ensia-rvig|ensia-brp|ensia-pun|ensia-pnikni
Boolean	1:Ja|0:Nee		ensia-isd|ensia-itaudit|ensia-rvig|ensia-brp|ensia-pun|ensia-pnikni
Boolean	1:Ja|0:Nee	De toewijzing en het gebruik van speciale bevoegdheden behoren te worden beperkt en beheerst. Dit is een BRP bepaling. Besluit BRP 6 Suwinorm: U.03 Zie ook hs 11.2.2 van de BIG: Beheer van (speciale) bevoegdheden p.47 Benodigde documentatie Kopie beleid of procesbeschrijving voor het beheer van speciale bevoegdheden, kopie functie- of rolbeschrijvingen van de beheerders van speciale bevoegdheden.;	ensia-rvig|ensia-isd|ensia-brp
Boolean	1:Ja|0:Nee		ensia-rvig|ensia-isd|ensia-brp
Boolean	1:Ja|0:Nee	De toewijzing van wachtwoorden behoort met een formeel beheerproces te worden beheerst. Suwinorm: U.03 Zie ook hs 11.2.3 van de BIG: Beheer van gebruikerswachtwoorden p.48 Benodigde documentatie Procedurebeschrijving van de beheerste wachtwoord toewijzing, kopie van informatie waaruit blijkt dat de organisatie conform het beleid heeft uitgevoerd. Te denken aan: kopie verklaring waaruit blijkt dat de gebruikers een verklaring on-dertekenen dat zij hun persoonlijke wachtwoorden geheimhouden, kopie uit systeem waaruit blijkt dat bepaalde minimale gestelde parameters zijn ingesteld.	ensia-isd
Boolean	1:Ja|0:Nee	Het (lijn)management behoort de toegangsrechten van gebruikers regelmatig te beoordelen in een formeel proces. Dit is een BRP en Suwi eis. Besluit BRP 6 Suwinorm: C.04 Zie ook hs 11.2.4 van de BIG: Beoordeling van toegangsrechten van gebruikers p.48 Benodigde documenatie Verslagen van de controle op de toegangsrechten per proceseigenaar/systeemeigenaar met een focus op basisregistraties, suwi en DigiD. Plaats in het opmerkingenveld hieronder de eventuele extra onderbouwing van uw antwoord voor de IT auditor.	ensia-isd|ensia-rvig|ensia-itaudit|ensia-brp
Boolean	1:Ja|0:Nee		ensia-isd|ensia-rvig|ensia-itaudit|ensia-brp
Boolean	1:Ja|0:Nee	Medewerkers dienen op juiste wijze gebruik van te maken van de aan hen toegekende wachtwoorden, pincodes, tokens of certificaten. Dit wordt bereikt door gebruikers te informeren over de wijze waarop zij met deze geheime authenticatie informatie dienen om te gaan.Dit is een BRP bepaling. Besluit BRP 6 Zie ook hs 11.3.1. van de BIG: Gebruik van wachtwoorden p.48 Benodigde documentatie Gespreksverslag beheerder, kopie brief of mail met uitleg gewenst gebruik.	ensia-rvig|ensia-isd|ensia-brp
Checkbox	0:Geen|1:Wachtwoorden bestaan uit minimaal 8 karakters, waarvan tenminste 1 hoofdletter, 1 cijfer en 1 vreemd teken|2:Wachtwoorden zijn maximaal 60 dagen geldig en mogen niet binnen 6 keer herhaald worden|3:Tijdelijke of standaard wachtwoorden worden bij het eerste gebruik vervangen|4:Het wachtwoord is alleen bij de gebruiker bekend	Medewerkers dienen op juiste wijze gebruik van te maken van de aan hen toegekende wachtwoorden, pincodes, tokens of certificaten. Dit wordt bereikt door gebruikers te informeren over de wijze waarop zij met deze geheime authenticatie informatie dienen om te gaan. Dit is een BRP eis Besluit BRP 6 Zie ook hs 11.3.1 van de BIG: Gebruik van wachtwoorden p.48 Benodigde documentatie Gespreksverslag beheerder, kopie brief of mail met uitleg gewenst gebruik.	ensia-rvig|ensia-brp

Boolean	1:Ja|0:Nee	Gebruikers behoren te bewerkstelligen dat onbeheerde apparatuur passend is beschermd. Zie ook hs 11.3.2 van de BIG: Onbeheerde gebruikersapparatuur p.49 Benodigde documentatie Huisregels veilig gebruik van computers en mobiele apparatuur.	
Boolean	1:Ja|0:Nee		
Boolean	1:Ja|0:Nee	Er behoort een clear desk-beleid voor papier en verwijderbare opslagmedia te worden ingesteld. Dit is een BRP eis. Besluit BRP 6 Zie ook hs 11.3.3 van de BIG: Clear desk en clear screen p.49 Benodigde documentatie Kopie 'Clear desk'- en 'clear screen'-beleid,, kopie e-mails, flyers, of nieuwsbrief waaruit het blijkt dat de organisatie met de eindgebruikers heeft gecommuniceerd omtrent het volgende: elke dag dossiers opbergen bij vertrek naar huis en pc vergrendelen bij verlaten van werkplek.	ensia-rvig|ensia-brp
Boolean	1:Ja|0:Nee	Er behoort een clear screen-beleid voor ICT-voorzieningen te worden ingesteld. Dit is een BRP eis BRP: 65 Zie ook hs 11.3.3 van de BIG: Clear desk en clear screen p.49 Benodigde documentatie Kopie 'Clear desk'- en 'clear screen'-beleid, kopie e-mails, flyers, of nieuwsbrief waaruit het blijkt dat de organisatie met de eindgebruikers heeft gecommuniceerd omtrent het volgende: elke dag dossiers opbergen bij vertrek naar huis, pc vergrendelen bij verlaten van werkplek.	
Boolean	1:Ja|0:Nee	Gebruikers behoort alleen toegang te worden verleend tot diensten waarvoor ze specifiek bevoegd zijn. Dit is een BRP en PUN eis Besluit BRP 6 PUN 90 Zie ook hs 11.4.1 van de BIG: Beleid ten aanzien van het gebruik van netwerkdiensten p.49 Benodigde documentatie Kopie vastgesteld toegangsbeleid met daarin de te onderscheiden toegangspaden en toegangsmethode(n) per type gebruiker, kopie materiaal waaruit blijkt dat beleid is gecommuniceerd, registratie van aanvragen en toekenningen is aanwezig.	ensia-rvig|ensia-brp|ensia-pun|ensia-pnikni
Boolean	1:Ja|0:Nee	Er behoren geschikte authenticatiemethoden te worden gebruikt om toegang van gebruikers op afstand te beheersen. Zie ook hs 11.4.2 van de BIG: Authenticatie van gebruikers bij externe verbindingen p.50 Benodigde documentatie Kopie vastgesteld toegangsbeleid met daarin de te onderscheiden toegangspaden en toegangsmethode(n) per type gebruiker, kopie materiaal waaruit blijkt dat beleid is gecommuniceerd, registratie van aanvragen en toekenningen is aanwezig.	ensia-bkwi
Boolean	1:Ja|0:Nee		ensia-bkwi
Boolean	1:Ja|0:Nee	Automatische identificatie van apparatuur behoort te worden overwogen als methode om verbindingen vanaf specifieke locaties en apparatuur te authenticeren. Zie ook hs 11.4.3 van de BIG: Identificatie van (netwerk)apparatuur p.50 Benodigde documentatie Netwerk plan, infrastructuur plan, cryptografie ensleutelbeheerplan.	
Boolean	1:Ja|0:Nee	De fysieke en logische toegang tot poorten voor diagnose en configuratie behoort te worden beheerst. Dit is een BRP eis. Besluit BRP 6 Zie ook hs 11.4.4 van de BIG: Bescherming op afstand van poorten voor diagnose en configuraties p.50 Benodigde documentatie Netwerkbeheer beleid, netwerkbeheerplan.	ensia-rvig|ensia-brp
Boolean	1:Ja|0:Nee	Groepen informatiediensten, gebruikers en informatiesystemen behoren op netwerken te worden gescheiden. Zie ook hs 11.4.5 van de BIG: Scheiding van netwerken p.50 Benodigde documentatie Kopie van beleid en procedurebeschrijving voor scheiding van netwerken, kopie van informatie waaruit blijkt dat de organisatie conform het beleid of procedure heeft gehanteerd. Te denken aan: kopie uit systeem waaruit blijkt dat de productienetwerkdomeinen en administratienetwerkdomein gescheiden zijn, kopie overzicht landscape en infrastructuur.	ensia-bkwi
Boolean	1:Ja|0:Nee	Voor gemeenschappelijke netwerken, vooral waar deze de grenzen van de organisatie overschrijden, behoren de toegangsmogelijkheden voor gebruikers te worden beperkt, overeenkomstig het toegangsbeleid en de eisen van bedrijfstoepassingen (zie 11.1). Suwinorm: U.11 Zie ook hs 11.4.6 van de BIG: Beheersmaatregelen voor netwerkverbindingen p.51 Benodigde documentatie Toegangsbeleid en eisen voor bedrijfsprocessen.	ensia-isd
Boolean	1:Ja|0:Nee	Netwerken behoren te zijn voorzien van beheersmaatregelen voor netwerkroutering, om te bewerkstelligen dat computerverbindingen en informatiestromen niet in strijd zijn met het toegangsbeleid voor de bedrijfstoepassingen. Zie ook hs 11.4.7 van de BIG: Beheersmaatregelen voor netwerkroutering p.51 Benodigde documentatie Netwerkbeheer beleid, netwerkbeheerplan.	ensia-bkwi
Boolean	1:Ja|0:Nee	Toegang tot besturingssystemen behoort te worden beheerst met een beveiligde inlogprocedure. Zie ook hs 11.5.1. van de BIG: Beveiligde inlogprocedures p.51 Benodigde documentatie Schermprint vanuit een besturingssysteem waaruit blijkt dat de toegang beheerst wordt door een beveiligde inlogprocedure.Kopie beleid voor beveiligde inlogprocedures.	ensia-bkwi
Boolean	1:Ja|0:Nee		ensia-bkwi

Boolean	1:Ja|0:Nee	Elke gebruiker behoort over een unieke identificatiecode te beschikken (gebruikers-ID) voor uitsluitend persoonlijk gebruik, en er behoort een geschikte authenticatietechniek te worden gekozen om de geclaimde identiteit van de gebruiker te bewijzen. Dit is een Suwi eis. Suwinorm: U.03 Zie ook hs 11.5.2 van de BIG: Gebruikersidentificatie en –authenticatie p.51 Benodigde documentatie Bij gebruik van een SSO of een centraal geregelde wachtwoordbewaarkluis, een uitdraaiKopie van de active directory of gelijkwaardigeen beschijving van het gebruik van authenticatiemiddelen. SUWI guidance Onderdeel collegeverklaring Deze vraag en het antwoord zijn onderdeel van de Collegeverklaring die de gemeente moet afgeven in het kader van Suwinet. Onderdeel SUWI-norm Deze vraag is onderdeel van het specifiek suwinet normenkader voor afnemers en het antwoord wordt gerapporteerd aan SZW. Doelstelling SUWI-norm Bewerkstelligen dat de geclaimde identiteit van de gebruiker kan worden bewezen en dat daardoor alleen bevoegde gebruikers toegang krijgen tot Suwinet diensten. Criterium Elke gebruiker/beheerder behoort over een unieke identificatiecode te beschikken (User-ID) voor uitsluitend persoonlijk gebruik, ook behoort een geschikte authenticatie techniek te worden gekozen. Nadere toelichting Scope: logische toegangsbeveiliging Betrokken: gemeenten, SVB, UWV Nadere Info: zorg dragen voor strong authentication (two factor authentication) dan wel ayer multi factor authentication SUWI-norm: U.03 Plaats in het opmerkingenveld hieronder de eventuele extra onderbouwing van uw antwoord voor de IT auditor.	ensia-isd|ensia-itaudit
Boolean	1:Ja|0:Nee	Elke gebruiker behoort over een unieke identificatiecode te beschikken (gebruikers-ID) voor uitsluitend persoonlijk gebruik, en er behoort een geschikte authenticatietechniek te worden gekozen om de geclaimde identiteit van de gebruiker te bewijzen. Dit is een Suwi eis. Suwinorm: U.03 Zie ook hs 11.5.2 van de BIG: Gebruikersidentificatie en –authenticatie p.51 Benodigde documentatie Bij gebruik van een SSO of een centraal geregelde wachtwoordbewaarkluis, een uitdraaiKopie van de active directory of gelijkwaardigeen beschijving van het gebruik van authenticatiemiddelen. SUWI guidance Onderdeel collegeverklaring Deze vraag en het antwoord zijn onderdeel van de Collegeverklaring die de gemeente moet afgeven in het kader van Suwinet. Onderdeel SUWI-norm Deze vraag is onderdeel van het specifiek suwinet normenkader voor afnemers en het antwoord wordt gerapporteerd aan SZW. Doelstelling SUWI-norm Bewerkstelligen dat de geclaimde identiteit van de gebruiker kan worden bewezen en dat daardoor alleen bevoegde gebruikers toegang krijgen tot Suwinet diensten. Criterium Elke gebruiker/beheerder behoort over een unieke identificatiecode te beschikken (User-ID) voor uitsluitend persoonlijk gebruik, ook behoort een geschikte authenticatie techniek te worden gekozen. Nadere toelichting Scope: logische toegangsbeveiliging Betrokken: gemeenten, SVB, UWV Nadere Info: zorg dragen voor strong authentication (two factor authentication) dan wel ayer multi factor authentication SUWI-norm: U.03 Plaats in het opmerkingenveld hieronder de eventuele extra onderbouwing van uw antwoord voor de IT auditor.	ensia-isd|ensia-itaudit
Boolean	1:Ja|0:Nee		ensia-isd|ensia-itaudit
Boolean	1:Ja|0:Nee	Systemen voor wachtwoordbeheer behoren interactief te zijn en moeten bewerkstelligen dat wachtwoorden van geschikte kwaliteit worden gekozen. Zie ook hs 11.5.3 van de BIG: Systemen voor wachtwoordenbeheer p.52 Benodigde documentatie Uitdraaien van systemen zoals bijvoorbeeld de beleidsregels voor sterke wachtwoorden uit de AD en andere relevante systemen.	ensia-bkwi
Boolean	1:Ja|0:Nee	Het gebruik van hulpprogrammatuur waarmee systeem- en toepassingsbeheersmaatregelen zouden kunnen worden gepasseerd behoord te worden beperkt en behoord strikt te worden beheerst. Zie ook hs 11.5.4. van de BIG: Gebruik van systeemhulpmiddelen p.52 Benodigde documentatie Procedures gebruik hulpprogammatuur	
Boolean	1:Ja|0:Nee	Inactieve sessies behoren na een vastgestelde periode van inactiviteit te worden uitgeschakeld. Zie ook hs 11.5.5. van de BIG: Time-out van sessies p.52 Benodigde documentatie ICT-beleid en procedure beeindigen inactieve sessies.	ensia-bkwi
Checkbox	0:Na 15 minuten vergrendeld|1:Na 4 uur beëindigd		ensia-bkwi
Boolean	1:Ja|0:Nee	De verbindingstijd behoort te worden beperkt als aanvullende beveiliging voor toepassingen met een verhoogd risico. Zie ook hs 11.5.6 van de BIG: Beperking van verbindingstijd p.53 Benodigde documentatie Contracten met leveranciers, beheer procedures, logging van toegang.	ensia-bkwi
Boolean	1:Ja|0:Nee	Toegang tot informatie en functies van toepassingssystemen door gebruikers en ondersteunend personeel behoort te worden beperkt overeenkomstig het vastgestelde toegangsbeleid. Zie ook hs 11.6.1. van de BIG: Beperken van toegang tot informatie p.53 Benodigde documentatie Toegangsbeleidprocedure per systeemautorisatiesystemen en autorisatie matrixen per proces/systeem.	ensia-bkwi

Boolean	1:Ja|0:Nee	Gevoelige systemen behoren een eigen, vast toegewezen (geïsoleerde) computeromgeving te hebben. Dit is een PUN eis. Circulaire BPR/U59776 Zie ook hs 11.6.2 van de BIG: Isoleren van gevoelige systemen p.53 Benodigde documentatie ICT beleid, classificatie van systemen, infrastructuur of netwerk plan.	ensia-rvig|ensia-pun|ensia-pnikni
Checkbox	0:Voor de RAAS|1:Voor verkeer uit de DMZ|2:Voor beheer (actieve) netwerkcomponenten		ensia-rvig|ensia-pun|ensia-pnikni
Boolean	1:Ja|0:Nee	Er behoort formeel beleid te zijn vastgesteld en er behoren geschikte beveiligingsmaatregelen te zijn getroffen ter bescherming tegen risico's van het gebruik van draagbare computers en communicatiefaciliteiten. Zie ook hs 11.7.1 van de BIG: Draagbare computers en communicatievoorzieningen p.54 Benodigde documentatie Beleid waarin aandacht is voor het gebruik van mobiele apparatuur, een ingericht en beheert mobiel device management systeem, gebruikersvoorwaarden mobiele systemen.	ensia-isd
Checkbox	0:Door middel van MDM/WTR|1:Zero footprint voor mobiele devices|2:Harddisk encryptie voor laptops		ensia-isd
Boolean	1:Ja|0:Nee		ensia-isd
Boolean	1:Ja|0:Nee		ensia-isd
Checkbox	0:Nee, er is geen beleid en er zijn geen procedures|1:Ja, er is beleid en er zijn procedures|2:Er is wel beleid, maar geen procedures|3:Er is geen beleid, maar er zijn wel procedures	Er behoort beleid, operationele plannen en procedures voor telewerken te worden ontwikkeld en geïmplementeerd. Dit is een BRP. Besluit BRP 6 Suwinorm: U.12 Zie ook hs 11.7.2 van de BIG: Telewerken p.54 Benodigde documentatie Telewerk beleid, huisregels computer gebruik, geheimhoudingsverklaringen, zonering, inrichting systemen. SUWI guidance Onderdeel SUWI-norm Deze vraag is onderdeel van het specifiek suwinet normenkader voor afnemers en het antwoord wordt gerapporteerd aan SZW. Doelstelling SUWI-norm Bewerkstelligen van Suwinet gegevensbeveiliging bij transport en gebruik van telewerkvoorzieningen. Criterium Afnemer heeft beleid, operationele richtlijnen en procedures voor telewerken ontwikkeld en geïmplementeerd. Nadere toelichting Scope: beveiligingstechniek Betrokken: gemeenten, SVB, UWV Nadere Info: veilige middelen voor data transport via veilige verbindingen, denk daarbij aan TSL en HTTPS. Draag zorg voor documentatie (security architectuur). Denk ook aan VPN gecombineerd met multi factor authentication. Gedragscode voor data verzending alleen beveiligd en dus ook niet per post of ed. Pdf documenten kunnen beveiligen SUWI-norm: U.12	ensia-burgerzaken|ensia-isd|ensia-rvig|ensia-brp
Boolean	1:Ja|0:Nee		ensia-burgerzaken|ensia-isd|ensia-rvig|ensia-brp
Boolean	1:Ja|0:Nee		ensia-burgerzaken|ensia-isd|ensia-rvig|ensia-brp
Boolean	1:Ja|0:Nee		ensia-burgerzaken|ensia-isd|ensia-rvig|ensia-brp
Boolean	1:Ja|0:Nee	In bedrijfseisen voor nieuwe informatiesystemen of uitbreidingen van bestaande informatiesystemen behoren ook eisen voor beveiligingsmaatregelen te worden opgenomen. Zie ook hs 12.1.1 van de BIG: Analyse en specificatie van beveiligingseisen p.55 Benodigde documentatie Beleid waarin bedrijfseisen en beveiligingsmaatregelen voor nieuwe informatiesystemen of uitbreiding van bestaande informatiesystemen zijn beschreven, kopie van het vaste programma van eisen t.a.v. beveiliging; kopie van informatie waaruit blijkt dat de organisatie conform de vaste programma uitvoeren. Te denken aan: kopie checklist voor het beoordelen van bedrijfseisen bij aanschaf of uitbreiding.	ensia-inkoop|ensia-bkwi
Boolean	1:Ja|0:Nee	Gegevens die worden ingevoerd in toepassingen behoren te worden gevalideerd om te bewerkstelligen dat deze gegevens juist en geschikt zijn. Zie ook hs 12.2.1 van de BIG: Validatie van invoergegevens p.56 Benodigde documentatie Systeem documentatie, webapplicaties.	ensia-keycontrol
Radiobutton	0:Nee|1:Ja|2:Ja, voor webpagina’s met een DigiD koppeling	Gegevens die worden ingevoerd in toepassingen behoren te worden gevalideerd om te bewerkstelligen dat deze gegevens juist en geschikt zijn. Zie ook hs 12.2.1 van de BIG: Validatie van invoergegevens p.56 Benodigde documentatie Testverslagen van applicaties, pentest rapportages, verslagen van codereviews.	ensia-keycontrol

Checkbox	0:Digitale aangifte kan alleen via DigiD plaatsvinden|1:Er vindt automatische signalering plaats op risicoadressen en/of -personen|2:Iedere digitale aangifte wordt voor de definitieve verwerking door een medewerker gecontroleerd	Gegevens die worden ingevoerd in toepassingen behoren te worden gevalideerd om te bewerkstelligen dat deze gegevens juist en geschikt zijn. Dit is een BRP eis. Besluit BRP 6 Zie ook hs 12.2.1 van de BIG: Validatie van invoergegevens p.56 Benodigde documentatie Testverslagen van applicaties, pentest rapportages, verslagen van codereviews.	ensia-keycontrol|ensia-rvig|ensia-brp
Boolean	1:Ja|0:Nee	Er behoren validatiecontroles te worden opgenomen in toepassingen om eventueel corrumperen van informatie door verwerkingsfouten of opzettelijke handelingen te ontdekken. Zie ook hs 12.2.2 van de BIG: Beheersing van interne gegevensverwerking p.56 Benodigde documentatie Testverslagen van applicaties, pentest rapportages, verslagen van codereviews.	ensia-keycontrol|ensia-bkwi
Boolean	1:Ja|0:Nee	Er behoren validatiecontroles te worden opgenomen in toepassingen om eventueel corrumperen van informatie door verwerkingsfouten of opzettelijke handelingen te ontdekken. Zie ook hs 12.2.3 van de BIG: Integriteit van berichten p.56 Benodigde documentatie Testverslagen van applicaties, pentest rapportages, verslagen van codereviews.	ensia-keycontrol|ensia-bkwi
Boolean	1:Ja|0: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. Zie ook hs 12.2.4 van de BIG: Validatie van uitvoergegevens p.56 Documentatie De gemeente heeft zich geconformeerd aan Gemma en aan Stuf.	ensia-keycontrol|ensia-bkwi
Boolean	1:Ja|0:Nee	Er behoort beleid te worden ontwikkeld en geïmplementeerd voor het gebruik van cryptografische beheersmaatregelen voor de bescherming van informatie. Dit is een Suwi eis. Suwinorm: U.11 Zie ook hs 12.3.1 van de BIG: Beleid voor het gebruik van cryptografische beheersmaatregelen p.57 Benodigde documentatie Cryptografiebeleid, dataclassificatieverslagen, sleutelbeheerprocedure. Plaats in het opmerkingenveld hieronder de eventuele extra onderbouwing van uw antwoord voor de IT auditor.	ensia-isd|ensia-itaudit
Boolean	1:Ja|0:Nee	Er behoort sleutelbeheer te zijn vastgesteld ter ondersteuning van het gebruik van cryptografische technieken binnen de organisatie. Zie ook hs 12.3.2 van de BIG: Sleutelbeheer p.57 Benodigde documentatie Sleutelbeheerprocedure, een taak of functiebeschrijving waaruit naar voren komt dat iemand verantwoordelijk is.	ensia-bkwi
Boolean	1:Ja|0:Nee	Er behoren procedures te zijn vastgesteld om de installatie van programmatuur op productiesystemen te beheersen. Zie ook hs 12.4.1 van de BIG: Beheersing van operationele programmatuur p.57 Benodigde documentatie Procedure installatie nieuwe software, change management proces (ITIL) Procedures worden periodiek gevalideerd,changes worden vooraf geaccordeerd, Fall back plannen zijn aanwezig, uitvoering vindt plaats door getrainde beheerders, uit configuratiedetails blijkt dat alle programmatuur is geautoriseerd.	ensia-bkwi
Boolean	1:Ja|0:Nee	Er behoren procedures te zijn vastgesteld om de installatie van programmatuur op productiesystemen te beheersen. Zie ook hs 12.4.1 van de BIG: Beheersing van operationele programmatuur p.57 Benodigde documentatie Procedure hardenen, configuratie verslagen van servers en platvormen.	ensia-bkwi
Radiobutton	0:Nee|1:Ja|2:Anders	Testgegevens behoren zorgvuldig te worden gekozen, beschermd en beheerst. Zie ook hs 12.4.2 van de BIG: Bescherming van testdata p.58 Benodigde documentatie estverslagen van applicaties, testdossiers	
Radiobutton	0:Wij testen niet|1:Wij hebben alles uitbesteed		
Boolean	1:Ja|0:Nee		
Radiobutton	0:Nee|1:Ja|2:N.v.t.	De toegang tot broncode van programmatuur behoort te worden beperkt. Zie ook hs 12.4.3 Toegangsbeheersing voor broncode van programmatuur p.58 Benodigde documentatie Procedure beschrijvingen voor de opslag van broncode, applicatie beheer procedures.	
Radiobutton	0:Wij bouwen zelf geen software|1:Wij hebben alles uitbesteed		

Boolean	1:Ja|0:Nee	De implementatie van wijzigingen behoort te worden beheerst door middel van formele procedures voor wijzigingsbeheer. Zie ook hs 12.5.1 van de BIG: Procedures voor wijzigingsbeheer p.58 Benodigde documentatie Wijzigingsbeheerprocedure, ITIL, verslagen van vergaderingen.	ensia-bkwi
Boolean	1:Ja|0:Nee	Bij wijzigingen in besturingssystemen behoren bedrijfskritische toepassingen te worden beoordeeld en getest om te bewerkstelligen dat er geen nadelige gevolgen zijn voor de activiteiten of beveiliging van de organisatie. Zie ook hs 12.5.2 van de BIG: Technische beoordeling van toepassingen na wijzigingen in het besturingssysteem p.59 Benodigde documentatie Procedure wijziging besturingssystemen, testverslagen.	ensia-bkwi
Checkbox	0:Wij beheren onze systemen niet zelf|1:Wij hebben alles uitbesteed		ensia-bkwi
Checkbox	0:Op systeemniveau (besturingssysteem)|1:Op applicatieniveau (informatiesysteem)|2:Op gegevensniveau (databasesysteem)		ensia-bkwi
Boolean	1:Ja|0:Nee	Wijzigingen in programmatuurpakketten behoren te worden ontmoedigd, te worden beperkt tot noodzakelijke wijzigingen, en alle wijzigingen behoren strikt te worden beheerst. Zie ook hs 12.5.3 van de BIG: Restricties op wijzigingen in programmatuurpakketten p.59 Benodigde documentatie Beheer documenten.	
Radiobutton	0:Wij beheren onze programmatuur niet zelf|1:Wij hebben alles uitbesteed		
Boolean	1:Ja|0:Nee	Er behoort te worden voorkomen dat zich gelegenheden voordoen om informatie te laten uitlekken. Zie ook hs 12.5.4 van de BIG: Uitlekken van informatie p.59 Benodigde documentatie Beleid content scanning, beheer documentatie en controle documentatie.	ensia-bkwi
Checkbox	0:Wij beheren onze programmatuur niet zelf|1:Wij hebben alles uitbesteed		ensia-bkwi
Boolean	1:Ja|0:Nee	Er behoort tijdig informatie te worden verkregen over technische kwetsbaarheden van de gebruikte informatiesystemen. De mate waarin de organisatie bloot staat aan dergelijke kwetsbaarheden behoort te worden geëvalueerd en er behoren geschikte maatregelen te worden genomen voor behandeling van daarmee samenhangende risico's. Zie ook hs 12.6.1 van de BIG: Beheersing van technische kwetsbaarheden p.60 Benodigde documentatie Beleid voor technische kwetsbaarheden, verslagen van vulnarability scans en pentesten en is er een patchmanagement procedure .	ensia-keycontrol|ensia-bkwi
Checkbox	0:Vulnerability scans|1:Pentesten|2:Patchmanagement		ensia-keycontrol|ensia-bkwi
Boolean	1:Ja|0:Nee		ensia-keycontrol|ensia-bkwi
Boolean	1:Ja|0:Nee	Er behoort tijdig informatie te worden verkregen over technische kwetsbaarheden van de gebruikte informatiesystemen. De mate waarin de organisatie bloot staat aan dergelijke kwetsbaarheden behoort te worden geëvalueerd en er behoren geschikte maatregelen te worden genomen voor behandeling van daarmee samenhangende risico's. Zie ook hs 12.6.1 van de BIG: Beheersing van technische kwetsbaarheden p.60 Benodigde documentatie Patchmanagement proces, actuele vulnerability scan rapporten.	ensia-keycontrol|ensia-bkwi

Boolean	1:Ja|0:Nee	Er behoort tijdig informatie te worden verkregen over technische kwetsbaarheden van de gebruikte informatiesystemen. De mate waarin de organisatie bloot staat aan dergelijke kwetsbaarheden behoort te worden geëvalueerd en er behoren geschikte maatregelen te worden genomen voor behandeling van daarmee samenhangende risico's. Zie ook hs 12.6.1 van de BIG: Beheersing van technische kwetsbaarheden p.60 Benodigde documentatie: Pentest jaarplanning, pentest verslagen.	ensia-keycontrol|ensia-bkwi
Boolean	1:Ja|0:Nee	Er behoort tijdig informatie te worden verkregen over technische kwetsbaarheden van de gebruikte informatiesystemen. De mate waarin de organisatie bloot staat aan dergelijke kwetsbaarheden behoort te worden geëvalueerd en er behoren geschikte maatregelen te worden genomen voor behandeling van daarmee samenhangende risico's. Zie ook hs 12.6.1 van de BIG: Beheersing van technische kwetsbaarheden p.60 Benodigde documentatie Planning security scans en verslagen van security scans.	ensia-keycontrol|ensia-bkwi
Boolean	1:Ja|0:Nee	Informatiebeveiligingsgebeurtenissen behoren zo snel mogelijk via de juiste leidinggevende niveaus te worden gerapporteerd. Zie ook hs 13.1.1 van de BIG: Rapportage van informatiebeveiligingsgebeurtenissen p.61 Benodigde documentatie Procedurebeschrijving voor het melden en registreren van incidenten op een afdeling of in een bepaald bedrijfsproces.	ensia-bkwi
Radiobutton	0:Nee|1:Ja|2:Alleen de reactie-en escalatieprocedure|3:Alleen een registratiesysteem		ensia-bkwi
Boolean	1:Ja|0:Nee	Van alle werknemers, ingehuurd personeel en externe gebruikers van informatiesystemen en –diensten behoort te worden geëist dat zij alle waargenomen of verdachte zwakke plekken in systemen of diensten registreren en rapporteren. Zie ook hs 13.1.2 van de BIG: Rapportage van zwakke plekken in de beveiliging p.62 Benodigde documentatie rocedurebeschrijving voor het melden en registreren van incidenten op een afdeling of in een bepaald bedrijfsproces. beleid of procedurebeschrijving voor het melden en registreren van incidenten"	ensia-isd
Boolean	1:Ja|0:Nee		ensia-isd
Boolean	1:Ja|0:Nee		ensia-isd
Boolean	1:Ja|0:Nee		ensia-isd
Boolean	1:Ja|0:Nee	Er behoren verantwoordelijkheden en procedures te worden vastgesteld om een snelle, doeltreffende en ordelijke reactie op informatiebeveiligingsincidenten te bewerkstelligen. Zie ook hs 13.2.1 van de BIG: Verantwoordelijkheden en procedures p.62 Benodigde documentatie Functie profielen voor het aantonen van de verantwoordelijkheid informatie waaruit blijkt dat de organisatie conform de proce-dure uitvoert.	ensia-keycontrol
Boolean	1:Ja|0:Nee		ensia-keycontrol
Boolean	1:Ja|0:Nee		ensia-keycontrol
Boolean	1:Ja|0:Nee	Er behoren mechanismen te zijn ingesteld waarmee de aard, omvang en kosten van informatiebeveiligingsincidenten kunnen worden gekwantificeerd en gecontroleerd. Zie ook hs 13.2.2 van de BIG: Leren van informatiebeveiligingsincidenten p.62 Benodigde documentatie Een beschreven organisatiestructuur en geaccordeerde mandatenregeling of RASCI-schema waaruit de TVB's van de betrokken medewerkers blijken Eigen waarneming dat de rapportage beveiligingsincidenten bestaat met daarin opgenomen de evaluatie van deze incidenten.	ensia-keycontrol
Boolean	1:Ja|0:Nee		ensia-keycontrol

Boolean	1:Ja|0:Nee	Waar een vervolgprocedure tegen een persoon of organisatie na een informatiebeveiligingsincident juridische maatregelen omvat (civiel of strafrechtelijk), behoort bewijsmateriaal te worden verzameld, bewaard en gepresenteerd overeenkomstig de voorschriften voor bewijs die voor het relevante rechtsgebied zijn vastgelegd. Zie ook hs 13.2.3 van de BIG: Verzamelen van bewijsmateriaal p.62 Benodigde documentatie - Een beleid- of procedurebeschrijving voor het verzamelen van bewijsmateriaal; - Bewijsstukken dat de informatiesystemen in overeenstemming zijn met gepubliceerde normen of praktijkcodes voor het genereren van toelaatbaar bewijsmateriaal; - Een registerboek waarin alle papieren documenten zijn geregistreerd (wie, wat, waar, wanneer); - Waarneming ter plaatse (aantonen dat originele stukken zorgvuldig wordt bewaard).	ensia-keycontrol|ensia-bkwi
Boolean	1:Ja|0: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. Zie ook hs 14.1.1 van de BIG: Informatiebeveiliging opnemen in het proces van bedrijfscontinuïteitsbeheer p.63 Benodigde documentatie Calamiteitenplan met aandacht voor informatiebeveiliging.	ensia-keycontrol
Boolean	1:Ja|0: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. Zie ook hs 14.1.2 van de BIG: Bedrijfscontinuïteit en risicobeoordeling p.63 Benodigde documentatie Uitgevoerde BIA's.	ensia-keycontrol
Boolean	1:Ja|0:Nee	Er behoren plannen te worden ontwikkeld en geïmplementeerd om de bedrijfsactiviteiten te handhaven of te herstellen en om de beschikbaarheid van informatie op het vooraf afgesproken niveau en binnen in de vereiste tijdspanne te bewerkstelligen na onderbreking of uitval van kritische bedrijfsprocessen. Dit is een BRP en BAG eis. BRP LO 7.4 BAG: 5.4.2 Zie ook hs 14.1.3 van de BIG: Continuïteitsplannen ontwikkelen en implementeren waaronder informatiebeveiliging p.63 Benodigde documentatie Calamiteitenplan ICT verstoringen	ensia-bouwenenwonen|ensia-keycontrol|ensia-rvig|ensia-brp
Checkbox	0:Voor wat betreft BRP|1:Voor wat betreft de dienstverlening van de BRP|2:Voor wat betreft BAG|3:Voor al onze primaire processen		ensia-bouwenenwonen|ensia-keycontrol|ensia-rvig|ensia-brp
Boolean	1:Ja|0:Nee	Er behoren plannen te worden ontwikkeld en geïmplementeerd om de bedrijfsactiviteiten te handhaven of te herstellen en om de beschikbaarheid van informatie op het vooraf afgesproken niveau en binnen in de vereiste tijdspanne te bewerkstelligen na onderbreking of uitval van kritische bedrijfsprocessen. Dit is een BRP eis. BRP LO 7.4 Zie ook hs 14.1.3 van de BIG: Continuïteitsplannen ontwikkelen en implementeren waaronder informatiebeveiliging p.63 Documentatie De BRP backup is afgestemd op de continuiteitseisen en de vereiste hersteltijd.	ensia-keycontrol|ensia-rvig|ensia-brp
Boolean	1:Ja|0:Nee	Er behoren plannen te worden ontwikkeld en geïmplementeerd om de bedrijfsactiviteiten te handhaven of te herstellen en om de beschikbaarheid van informatie op het vooraf afgesproken niveau en binnen in de vereiste tijdspanne te bewerkstelligen na onderbreking of uitval van kritische bedrijfsprocessen. Dit is een BRP eis. BRP LO 7.4 Zie ook hs 14.1.3 van de BIG: Continuïteitsplannen ontwikkelen en implementeren waaronder informatiebeveiliging p.63 Benodigde documentatie Een gesteste uitwijk waarbij binnen 24 uur BRP kan worden herstart.	ensia-keycontrol|ensia-rvig|ensia-brp
Boolean	1:Ja|0: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. Zie ook hs 14.1.4 van de BIG: Kader voor de bedrijfscontinuïteitsplanning p.64 Benodigde documentatie Een kader voor continuiteitsplannen.	ensia-keycontrol
Boolean	1:Ja|0:Nee	Bedrijfscontinuïteitsplannen behoren regelmatig te worden getest en geüpdate, om te bewerkstelligen dat ze actueel en doeltreffend blijven. Dit is een BRP eis. BRP LO 7.4 Zie ook hs 14.1.5 van de BIG: Testen, onderhoud en herbeoordelen van bedrijfscontinuïteitsplannen p.64 Benodigde documentatie Testverslagen van uitwijk en calamiteittesten.	ensia-keycontrol|ensia-rvig|ensia-brp

Checkbox	0:Alleen voor BRP|1:Voor kritische systemen|2:Voor alle systemen		ensia-rvig|ensia-keycontrol|ensia-brp
Boolean	1:Ja|0:Nee	Alle relevante wettelijke en regelgevende eisen en contractuele verplichtingen en de benadering van de organisatie in de naleving van deze eisen, behoren expliciet te worden vastgesteld, gedocumenteerd en actueel te worden gehouden voor elk informatiesysteem en voor de organisatie. Dit is een BRP en PUN eis. Besluit BRP 6 PUN 91 Zie ook hs 15.1.1 van de BIG: Identificatie van toepasselijke wetgeving p.65 Benodigde documentatie Vastgelegd in het beleid.	ensia-rvig|ensia-brp|ensia-pun|ensia-pnikni
Checkbox	0:WBP|1:PUN|2:SUWI|3:BRP|4:BAG|5:BGT|6:DigiD|7:Beveiligingsrichtlijnen voor web applicaties|8:WABB|9:BIG|10:Andere		ensia-rvig|ensia-brp|ensia-pun|ensia-pnikni
Boolean	1:Ja|0:Nee	Er behoren geschikte procedures te worden geïmplementeerd om te bewerkstelligen dat wordt voldaan aan de wettelijke en regelgevende eisen en contractuele verplichtingen voor het gebruik van materiaal waarop intellectuele eigendomsrechten kunnen berusten en het gebruik van programmatuur waarop intellectuele eigendomsrechten berusten. Zie ook hs 15.1.2 van de BIG: Intellectuele eigendomsrechten (Intellectual Property Rights (IPR)) p.65 Benodigde documenatie Procedure controle systeem en ICT gebruik, CMDB.	ensia-keycontrol
Boolean	1:Ja|0:Nee	Belangrijke registraties behoren te worden beschermd tegen verlies, vernietiging en vervalsing, overeenkomstig wettelijke en regelgevende eisen, contractuele verplichtingen en bedrijfsmatige eisen. Zie ook hs 15.1.3 van de BIG: Bescherming van bedrijfsdocumenten p.65 Benodigde documentatie Data opslag beleid.	ensia-keycontrol|ensia-bkwi
Radiobutton	0:Nee|1:Ja, middels compliance officer|2:Ja, middels Privacy functionaris	De bescherming van gegevens en privacy behoort te worden bewerkstelligd overeenkomstig relevante wetgeving, voorschriften en indien van toepassing contractuele bepalingen. Zie ook hs 15.1.4 van de BIG: Bescherming van gegevens en geheimhouding van persoonsgegevens p.65 Benodigde documentatie Privacy beleid.	ensia-keycontrol|ensia-bkwi
Checkbox	0:Procedureel met instructie|1:Bewustwordingsacties|2:Controle op systeem niveau (logging en monitoring)|3:Sancties	Gebruikers behoren ervan te worden weerhouden ICT-voorzieningen te gebruiken voor onbevoegde doeleinden. Zie ook hs 15.1.1 van de BIG: Voorkomen van misbruik van ICT-voorzieningen p.66 Benodigde documentatie Controleplannen, toegangsbeleid, autorisatiebeschikkingen, instemmingsbeschikkingen ICT middelen, IDS IPS systemen.	
Boolean	1:Ja|0:Nee	Cryptografische beheersmaatregelen behoren overeenkomstig alle relevante overeenkomsten, wetten en voorschriften te worden gebruikt. Zie ook hs 15.1.6 van de BIG: Voorschriften voor het gebruik van cryptografische beheersmaatregelen p.66 Benodigde documentatie Cryptografie beleid, aantoonbaar gebruik van cryptografische beheersmaatregelen.	ensia-bkwi
Checkbox	0:Volgens de ICT-beveiligingsrichtlijnen voor webapplicaties van het NCSC|1:Volgens SUWI|2:Volgens BRP|3:Conform de pas-toe-of-leg-uit lijst van het forum standaardisatie|4:Op basis van de Wet digitale handtekening		ensia-bkwi
Checkbox	0:Door middel van P&C rapportages|1:Door middel van interne controle|2:Door middel van self assessments|3:Door middel van audits	Managers behoren te bewerkstelligen dat alle beveiligingsprocedures die binnen hun verantwoordelijkheid vallen correct worden uitgevoerd om naleving te bereiken van beveiligingsbeleid en -normen. Dit is een BRP en PUN eis. Besluit BRP 6 PUN 91 Zie ook hs 15.2.1 van de BIG: Naleving van beveiligingsbeleid en -normen p.66 Benodigde documentatie Controle verslagen, selfassessment rapporten, auditverslagen.	ensia-rvig|ensia-bkwi|ensia-brp|ensia-pun|ensia-pnikni
Boolean	1:Ja|0:Nee	Informatiesystemen behoren regelmatig te worden gecontroleerd op naleving van implementatie van beveiligingsnormen. Zie ook hs 12.6.1 van de BIG: Beheersing van technische kwetsbaarheden p.60 & hs 15.2.1 van de BIG: Controle op technische naleving p.66 Benodigde documentatie Uitgevoerde risicoanalyses, pentestverslagen, auditverslagen.	ensia-bkwi

Checkbox	0:Voor BRP-systemen|1:Voor Suwi-systemen|2:Voor PUN-systemen|3:Voor webpagina's met een DigiD login|4:Voor BAG- en BGT-systemenoor BRP-systemen		ensia-bkwi
Boolean	1:Ja|0:Nee	Informatiesystemen behoren regelmatig te worden gecontroleerd op naleving van implementatie van beveiligingsnormen. Zie ook hs 15.2.1 van de BIG: Controle op technische naleving p.66 Benodigde documentatie Uitgevoerde risicoanalyses, pentestverslagen, auditverslagen.	ensia-bkwi
Boolean	1:Ja|0:Nee	Eisen voor audits en andere activiteiten waarbij controles worden uitgevoerd op productiesystemen, behoren zorgvuldig te worden gepland en goedgekeurd om het risico van verstoring van bedrijfsprocessen tot een minimum te beperken. Zie ook hs 15.3.1 van de BIG: Beheersmaatregelen voor audits van informatiesystemen p.67 Benodigde documentatie Controle plan.	
Boolean	1:Ja|0:Nee	Toegang tot hulpmiddelen voor audits van informatiesystemen behoort te worden beschermd om mogelijk misbruik of compromitteren te voorkomen. Zie ook hs 15.3.2 van de BIG: Bescherming van hulpmiddelen voor audits van informatiesystemen p.67 Benodigde documentatie Beveligingsmaatregelen voor hulpmiddelen voor systeemaudits.	