Stand van zaken en vooruitblik Informatieveiligheid (IV) en Privacy (P) juli 2020

	Deelprojecten en resultaten programma IVenP	2018 1e helft	2018 2e helft	2019 1e helft	2019 2e helft	2020 1e helft	2020 2e helft	2021 1e helft	2021 2e helft	2022 1e helft	2022 2e helft	volgens planning*	knel-punten	toelichting
1	**Inbedden governance**													
1a	**Taken en verantwoordelijkheden AVG en IV**											↑		Programmateam is op sterkte. Stuurgroep en kerngroep ingesteld. Governance is vastgesteld. Eigenaarschap in organisatie is issue.
1b	**Beleid informatieveiligheid**											↑		Gereed. Het beleid wordt Q4 geactualiseerd volgens een jaarlijkse cyclus.
1b1	**Beleid Privacy**											-		De FG bemerkte in 2020 dat het privacybeleid nog niet voldoende was. Er wordt momenteel een verbeterd beleidsplan opgesteld.
1c	**Uitvoeringsbeleid en richtlijnen**											↑		Op schema; Er zijn meerdere richtlijnen opgesteld; de laatste volgen in 2020; daarna proces over naar lijn.
1d	**Positionering IV in organisatie**											↑		Op schema.
1e	**Intern toezicht AVG**											↑		Actie gereed; overgedragen naar lijn.
1f	**Intern toezicht IV**													
1f1	**Audits**											↑		Volgens planning nog niet gestart. Wordt naar voren gehaald; Q4 start.
1f2	**Baseline Informatiebeveiliging Overheden**											↑		Gestart maar gaat traag. De uitrol van het ISMS moet dit versnellen. Deze uitrol is naar voren gehaald.
1f3	**Iso certificeerbaar in 2023**													Door komst BIO overbodig. Actie vervalt.
1f4	**jaarverslag**											↑		Volgens planning nog niet gestart. Is een politieke afspraak. Taak CISO.
1f5	**toezicht op projecten en programma's**											↑		Op dit moment is er toenemend incidenteel toezicht. Inzicht in lopende projecten is nog onvoldoende, maar wordt opgepakt.
1f6	**Third Party management**											↑		Volgens planning nog niet gestart. Eisen gaan onvoldoende mee in aanbestedingen. Er is onvoldoende sturing op afspraken met leveranciers.
1f7	**ISMS-framework**											↑		Doorlooptijd is lang i.v.m. o.a. niet op orde zijn overige processen. Start is naar voren gehaald. Vanaf Q4 start met basisimplementatie.
2	**Processen**													
2a	**Processen IVenP**													
2a1	**Risicoanalyseproces**											↑		Format is gereed. Proces is gestart. Achterstand maakt dat risicobeeld maken meer werk is dan ingeschat. Inhaalslag is ivm Corona vertraagd.
2a2	**Dataclassificatie**											↑		Dit loopt volgens planning; het daadwerkelijk toepassen van classificatie blijkt lastig.
2a3	**Gestandaardiseerde maatr'en IV identificeren**											↑		Door de introductie van de BIO moet een deel herzien worden.Dat veroorzaakt extra doorlooptijd.
2a4	**IB in projecten**											↑		Doordat het changemanagementproces (ITIL) niet op orde is, kan Informatieveiligheid niet vanaf de start meegenomen worden.
2a5	**Proces datalekken / IB incidenten**											↓		Loopt te traag. Incidentregistratie is nog niet op orde.
2a6	**Inkoopproces**											↑		Start volgens planning 1e helft 2020; er is meer afstemming tussen Inkoop en PO's. Geen gestructureerd proces. Achterstand niet in beeld.
2a7	**BCM = Business Continuity Management**											↑		Continuiteit is nu onvoldoende in beeld. Risico's bij calamiteiten zijn groot. Er is een crisiscommunicatieplan.
2b	**Wettelijk verplichte processen ihkv AVG**													
2b1	**Risicomanagement (privacygevoelige info)**											↑		zie 2a1
2b2	**dataclassificatie**											↑		zie 2a2
2b3	**Privacy by design**											↑		PbD is verwerkt in BIA-proces; wordt conform planning uitgerold. Is een wettelijke verplichting.
2b4	**Passende beveiligingsmaatregelen AVG**											↑		Achterstand was groot. Inhaalactie gekoppeld aan actualisatie verwerkingsregister loopt goed.
2b5	**Doelbinding gegevensverwerking**											↑		Deze actie loopt en is naar verwachting eind 2020 gereed.
2b6	**Verwerkingsregister**											↑		Deze actie loopt en is naar verwachting eind 2020 gereed.
2b7	**Rechten van betrokkenen**											↑		Loopt volgens planning; komend jaar evaluatie en bijstellen proces.
2b8	**Informatieverstrekking aan betrokkenen**											↑		Loopt volgens planning; komend jaar evaluatie en bijstellen proces. Privacystatements nog niet op orde. Achterstand niet in beeld.
2b9	**Bewaren van persoonsgegevens**											↑		Start volgens planning begin 2020; register wordt aangevuld met bewaartermijnen. Is een wettelijke verplichting. Is eind 2020 gereed.
2b10	**Verwerkingsovereenkomsten**											↑		Loopt nu volgens planning,
2b11	**Afspraken in Samenwerkingsverbanden**											↑		Samenwerkingsverbanden zijn niet allemaal in beeld. Politiek risico. Nadruk bij Autoriteit Persoonsgegevens.
2b12	**Doorgifte persoonsgegevens**											↑		Geplande start is half jaar vooruit geschoven.
3	**Maatregelen**													
3a	**Technische analyse en evaluatie**											↑		Nieuw opgenomen, eerder gestart. 2e helft 2020 wordt een penetratietest uitgevoerd.
3b	**Preventieve technische maatregelen**											↑		Activiteiten worden volgens planning uitgevoerd.
3c	**Detectieve technische maatregelen**											↑		Delen van de monitoring zijn ingericht. Nog niet volledig. Heeft de noodzakelijke aandacht.
3d	**Responsieve technische maatregelen**											↓		Het is onduidelijk of dit gestart is.
3e	**Facilitaire maatregelen**											-		nieuw op lijst, nog niet gestart.
3f	**Personele maatregelen**											-		nieuw op lijst, nog niet gestart.
4	**Bewustwording en eigenaarschap**													
4a	**Communicatie, uitvoeren plan**											↑		Voor 2020 is een vastgesteld communicatieplan dat vanaf begin 2020 wordt uitgerold.
4b	**Cultuurvolwassenheidsmeting**											↑		Iets vertraagd; is opnieuw ingepland en uitgevoerd.
4c	**Bekwamen van mgt en medewerkers**											↑		Achterstand is groot; vraagt om cultuurverandering. Awareness app, voorlichtingsessies. Financiele middelen voor 2021 aangevraagd.
5	**Lijnactiviteiten**													
												↑		Incidentenafhandeling en ad hoc advisering loopt; vraagt veel inspanning. Na 2021 overdracht aan lijn.

Legenda

	Groen = aanwezig en gereed
	Blauw = aanwezig, is belegd in de lijn, vraagt blijvende aandacht
	Oranje = lopend/bijna gereed
	Rood = nog niet aanwezig/gereed
	Wit = nieuw ingeplande activiteit, nog niet gestart

loopt volgens planning*	↑	= geen knelpunt
loopt niet volgens planning*	↓	= matig knelpunt, tegenmaatregelen zijn reeds genomen
nieuwe activiteit	-	= groot knelpunt, vraagt om (grotere) tegenmaatregel vanuit programma
**vorige rapportage*		= groot knelpunt, vraagt om tegenmaatregel/aandacht vanuit organisatie.

BIA	Business Impact Analyse (risicoanalyse)
BIO	Baseline Informatiebeveiliging Overheden
(C)ISO	(Corporate) Information Security Officer
(D)PIA	Privacy Impact Analyse
FG	Functionaris Gegevensbescherming
IVenP	Informatieveiligheid en privacy, programma
PbD	Privacy bij design
PO	Privacy Officer
ISMS	Sturings- en kwaliteitssysteem