



Programmaplan Informatiebeveiliging Gemeente Sluis

Datum: 03-07-2024

Versie: 1.2

Documenthistorie

Versie	Datum	Opgesteld door	Versie informatie	Verspreiding
0.2	05/02/24	Joeri Olierook, Tim Kunst	- Algemene inhoud toegevoegd - Project indeling en eerste uitwerking ingevoegd	Jeroen de Graaf (CISO)
0.3	06/05/24	Joeri Olierook, Tim Kunst	- Reviewcommentaar vo.2 verwerkt - Projectverkaveling nader uitgewerkt - BIO werkpakketten toegevoegd (bijlage)	Jeroen de Graaf (CISO) Steven Debets (Highberg QC, eerste review)
0.4	20/05/24	Tim Kunst	- Eerste opmerkingen QC verwerkt	-
0.8	05/06/24	Joeri Olierook, Tim Kunst	- Review opmerkingen verwerkt - Financiële paragraaf nader gespecificeerd - Highberg QC commentaar verwerkt	Steven Debets (Highberg QC), Jeroen de Graaf (CISO), Arthur Vons (CC), Marc Cauwels (Adviseur ICT)
0.91	10/06/24	Joeri Olierook, Tim Kunst	- Review opmerkingen CISO verwerkt - Opmerkingen Gemeentesecretaris en afdelingshoofd Bedrijfsvoering verwerkt	Opdrachtgever; Afdelingshoofd Bedrijfsvoering
1.0	03/07/24	Joeri Olierook, Tim Kunst	Vastgesteld door opdrachtgever en MT - Programmabesturing i.r.t. nader gespecificeerd	MT gemeente Sluis
1.2	08/10/24	Joeri Olierook, Tim Kunst	- Investerings en kosten in afstemming met Programmaboard in lijn gebracht met Collegenota en dekkingsvoorstel	Programmaboard; College en Raad; Programmadossier

Inhoudsopgave

1.	Inleiding	3
1.1	Aanleiding van het programma	3
1.2	Waarom een programma.....	3
2	Programmadefinitie	4
2.1	Een programma gericht op de hele organisatie	4
2.2	Baten van het programma	5
2.3	Programmadoel	5
2.4	Resultaten	6
2.5	Scope (wat doen we wel, wat doen we niet).....	6
2.6	Afhankelijkheden en omgeving	6
2.7	Uitgangspunten, randvoorwaarden/beperkingen en programmarisico's.....	8
3	Programma- en projectorganisatie (en toekomstige IB-organisatie)	9
3.1	Besturing	9
3.2	Programmaorganisatie en rollen	9
4	Roadmap, projecten en planning	13
4.1	Roadmap	13
4.2	Projecten	14
4.3	Inzet binnen programma en projecten	20
5	Investerings en kosten	21
5.1	Uitwerking en onderbouwing 'out of pocket' kosten op programmaniveau.....	21
6	Programmabeheersing	22
6.1	Risicomanagement.....	22
6.2	Programmarisico's	23
6.3	Kwaliteitsborging (Quality Control).....	24
6.4	Stuur en communicatiemiddelen	24
7	Stakeholdermanagement en communicatie	24
8	Bijlagen	26
8.1	Illustratie BIO-rapportage en Kwetsbaarhedenlog.....	26
8.2	Werkpakketten op basis van BIO hoofdstukken en thema's.....	26

1. Inleiding

1.1 Aanleiding van het programma

De gemeente Sluis dient te voldoen aan de Europese Richtlijn NIS2 die op het moment nog tot een nationale wetgeving vertaald moet worden. De NIS2 ligt in lijn met de eisen die reeds worden gesteld in de Baseline Informatiebeveiliging Overheid (vanaf hier: BIO). Het programma gebruikt daarom de basis die de BIO biedt, om uiteindelijk aan de NIS2 eisen te voldoen.

Dit document bevat het plan van aanpak voor het programma Informatiebeveiliging Sluis. Doel van dit programma is de digitale weerbaarheid van de gemeente te verhogen. Hiertoe zullen geselecteerde beheersmaatregelen worden ingericht 'op werkingsniveau'¹. Dit geheel aan maatregelen zal aangevuld worden met een werkende PDCA-cyclus. Deze PDCA-cyclus biedt continue verbetering en is onderdeel van de reguliere P&C-cyclus. Daarnaast heeft de PDCA-cyclus een belangrijke rol in verantwoording richting intern en externe stakeholders en toezichthouders.

Het Programma Informatiebeveiliging draagt bij aan de invulling van de eisen gesteld in de BIO, zoals uitgewerkt in de werkpakketten in bijlage 8.2.

Om te komen tot een volledige BIO/NIS2 implementatie definieert het Programma vijf projecten, die zowel parallel als volgordeijk invulling geven aan de benodigde ontwikkeling van informatiebeveiliging. Via diverse nulmetingen van het niveau van opzet, bestaan en werking van de beheersmaatregelen uit de BIO hebben wij hiervoor werkpakketten en een roadmap opgesteld.

Het programmanagement beheerst op overkoepelend programmaniveau de afhankelijkheden tussen de projecten en hun (deel)resultaten.

1.2 Waarom een programma

Een programma wordt gedefinieerd als:

“Een tijdelijk organisatieverband, ontworpen om sturing te geven aan diverse onderling verbonden projecten en lijnactiviteiten, met als doel het stapsgewijs realiseren van uitkomsten die baten opleveren voor één of meer organisaties.”

Een belangrijk verschil met projecten is daarbij niet alleen dat een programma integrale sturing geeft over samenhangende deelprojecten, maar vooral dat hierbij ook een combinatie wordt gemaakt met bestaande- en nieuwe lijnactiviteiten. Dit kan verwarrend zijn, zeker omdat projecten ook vaak een bezetting kennen vanuit de lijnorganisatie.

Naast coördinatie over meerdere projecten is er echter nog een belangrijke reden om de uitdaging van de gemeente Sluis programmatisch aan te vliegen: door onderdelen direct als lijnactiviteit op te pakken hoeft op later moment geen overdracht plaats te vinden vanuit een tijdelijke projectorganisatie. Op deze manier is er tevens sprake van een aantoonbare werking en vaardigheden binnen de lijnorganisatie op het gebied van informatiebeveiliging.

Binnen de programma aanpak en roadmap accepteert gemeente Sluis dat de BIO beheersmaatregelen nog niet direct op het gewenste (volwassenheid)niveau zijn, omdat de roadmap ook de route aangeeft waarop de gemeente dit in de komende jaren realiseert. Een programma levert een organisatie namelijk vaardigheden waarmee de organisatie vervolgens grotendeels zelfs de baten zal realiseren. Projecten leveren daarbinnen de resultaten (producten) die deze vaardigheden ondersteunen.

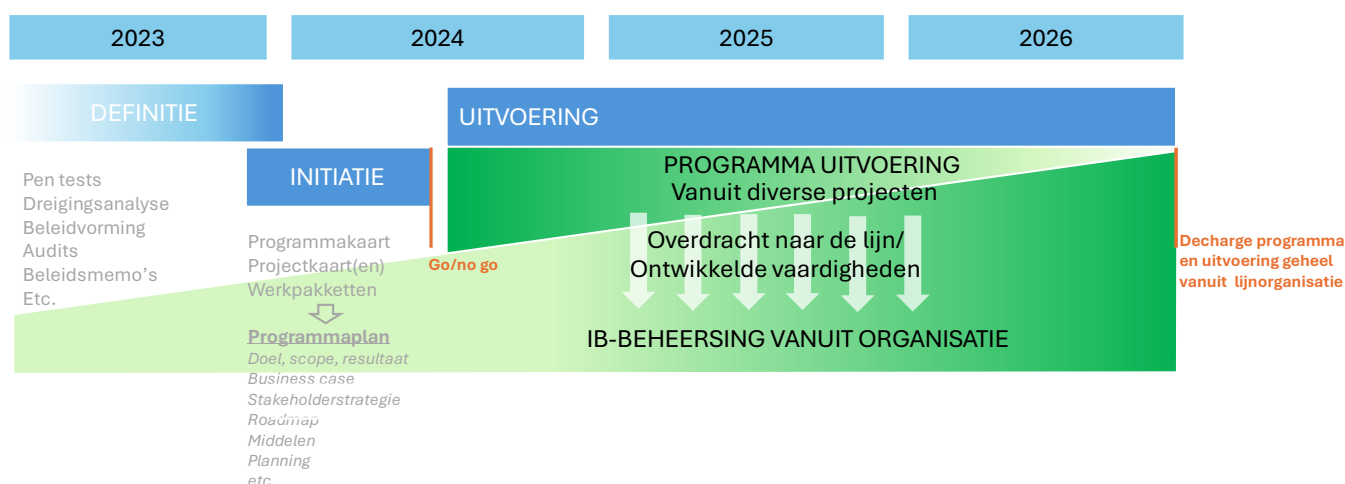
¹ Zie §2.3 voor definitie van werkingsniveau.

2 Programmadefinitie

2.1 Een programma gericht op de hele organisatie

Informatiebeveiliging en een veilige gemeente vereisen activiteiten en verandering in alle onderdelen en lagen van de gemeentelijke organisatie. De Baseline Informatiebeveiliging Overheid (BIO) biedt hiervoor het kader. De uitwerking hiervan geldt dus, in meer- en mindere mate, voor alle betrokken bij de gemeente.

Figuur 1 illustreert hoe het programma en de onderliggende projecten gedurende de looptijd optrekken met de lijnorganisatie, met als doel deze uiteindelijk de complete beheersing te laten uitvoeren.



Figuur 1: samenspel programma- en lijnorganisatie gedurende de looptijd van het programma

Informatiebeveiliging is daarbij geen 'ICT-exercitie'. Zo heeft de VNG bijvoorbeeld naast het inhoudelijke kader van de BIO ook '10 bestuurlijke principes voor informatiebeveiliging' heeft gepubliceerd². Deze worden dan ook meegenomen in de uitwerking van het programma en de deelprojecten:

- Bestuurders bevorderen een veilige cultuur;
- Informatiebeveiliging is van iedereen;
- Informatiebeveiliging is risicomanagement;
- Risicomanagement is onderdeel van de besluitvorming;
- Informatiebeveiliging heeft ook aandacht in (keten)samenwerking;
- Informatiebeveiliging is een proces;
- Informatiebeveiliging kost geld;
- Onzekerheid dient te worden ingecalculeerd;
- Verbetering komt voort uit leren en ervaring;
- Het bestuur controleert en evalueert.

Figuur 2:

Bij de totstandkoming van dit programmaplan zijn diverse bronnen en beschikbare producten gehanteerd. Deze zullen ook gedurende de uitvoering van het programma worden benut.



² De 10 bestuurlijke principes voor informatiebeveiliging, behorende bij de Baseline Informatiebeveiliging Overheid (BIO), VNG 2019 ([link](#))

2.2 Baten van het programma

De belangrijkste baten van het programma betreffen het veilig en weerbaar worden, en het veilig en weerbaar blijven van de gemeente Sluis en alle betrokkenen bij de gemeente (zoals o.a. medewerkers, inwoners en lokale bedrijven). Deze baten worden in de deelprojecten van het programma vertaald naar 'vaardigheden' waar de gemeente over dient te beschikken over weerbaar te worden én te blijven.

De deelprojecten realiseren producten die de gemeente helpen bij het ontwikkelen van deze vaardigheden. Het programma zorgt dat de gezamenlijke resultaten van de projecten ook tot vaardigheden binnen de organisatie leiden.

De ontwikkeling van deze baten zullen ook gepaard gaan met meer nadelige uitkomsten, ook wel 'disbenefits' genoemd. Bijvoorbeeld omdat Veilig werken op gespannen voet kan staan met 'makkelijk' werken, of omdat een afdeling anders moet gaan werken ten gunste van de weerbaarheid van een andere afdeling. Dergelijke zaken kunnen leiden tot demotivatie in de organisatie. In de projecten zal als onderdeel van de communicatie naast de realisatie van de 'positieve baten' dan ook aandacht worden besteed aan deze 'negatieve baten'.

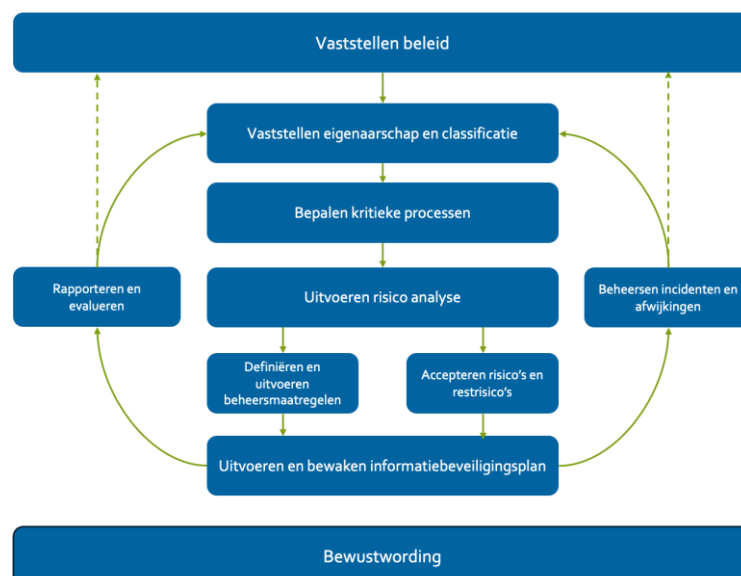
2.3 Programmadoel

Doel van dit programma is **de digitale weerbaarheid van de gemeente te verhogen**. Hiertoe zullen diverse beheersmaatregelen worden ingericht 'op werkingsniveau'. Met werkingsniveau wordt bedoeld dat het proces goed gedefinieerd is, gebruik maakt van middelen van de organisatie en in de praktijk structureel haar doel bereikt, aantoonbaar, continu op georganiseerde wijze.

Dit geheel aan maatregelen en de beheersorganisatie hieromheen, die onderdeel zijn van het Information Security Management Systeem, zal voorzien zijn van een werkende PDCA-cyclus. De PDCA-cyclus biedt continue verbetering en ten behoeve van verantwoording (intern en richting toezichthouder).

Bij het realiseren van de doelen zal ook gebruik worden gemaakt van de normeringen en definities zoals opgenomen in de ISO27001 normering. Uitgangspunt hierbij is dat alle activiteiten en resultaten binnen het programma bijdragen aan deze normering, of er op zijn minst niet aan afdoen. Compliance of certificering aan ISO-27001 valt echter niet onder de scope van het programma (zie §2.5).

Het Programma Informatiebeveiliging draagt bij aan de invulling van eisen gesteld in de Baseline Informatiebeveiliging Overheid (vanaf hier: BIO). Vanuit de Europese Richtlijn NIS2 worden de eisen uit het BIO-normenkader op dit moment tevens vertaald naar nationale wetgeving. Naar verwachting zal dit uitmonden in de BIO2.0. In de uitwerking van dit programmaplan wordt al rekening gehouden met deze overgang, wanneer de BIO2.0 daadwerkelijk beschikbaar komt zullen programma- en projectplannen hierop worden herijkt.



Figuur 3: grafische weergave van een 'ISMS'

2.4 Resultaten

Veilig worden:

- a) Implementeren van BIO maatregelen, op werkingsniveau en 'ISO27001 proof', tenzij onderbouwd;
- b) Inrichten van de aansturing en rapportage voor informatiebeveiliging (governance);
- c) Technische en procesmatige inventarisatie van kwetsbaarheden, eventueel middels de inzet van (reeds bestaande) periodieke, technische security scan;
- d) Oplossen van openstaande security issues;
- e) Opvolgen van openstaande auditaanbevelingen;
- f) Ondersteunen van projecten op het aspect informatiebeveiliging;
- g) Het geven van awareness trainingen en voorlichting;
- h) Het ondersteunen van proceseigenaren bij het uitvoeren van risicoanalyses;
- i) Opstellen en beheren van een actueel risicoregister, inclusief maatregelen en actiehouders;
- j) Uitwerken en beleggen minimaal noodzakelijke securityprocessen en -procedurebeschrijvingen.

Veilig blijven (information security management):

- a) Evalueren, opstellen, aanpassen, laten goedkeuren en uitdragen van beleid voor informatiebeveiliging en eventuele onderliggende normen wanneer nodig;
- b) Uitwerken en invoeren van security management processen;
- c) Inrichten van toekomstbestendige, interne Informatiebeveiligingsorganisatie passend bij gemeente Sluis;
- d) Afhandelen van security incidenten en adviseren op de security aspecten van datalekken;
- e) Bewaking van de naleving van het beleid voor informatiebeveiliging en de rapportage hierover;
- f) Training en opleiding m.b.t. de processen en beleid die volgen uit de diverse projecten;
- g) Adviseren van het management over actuele risico's en het voorstellen van oplossingen om deze het hoofd te bieden;
- h) Uitvoeren en opstellen marktverkenning/inkoop van diensten en producten die bij ICT nodig zijn;
- i) Onderhouden van de Roadmap;
- j) Inrichten van derde partij risicomanagement richting IT leveranciers;

2.5 Scope (wat doen we wel, wat doen we niet)

In scope, wat doen we wel:

- Implementatie van de Baseline Informatiebeveiliging Overheid (BIO) op werkingsniveau: het proces is goed gedefinieerd, maakt gebruik van middelen van de organisatie en haalt in de praktijk structureel haar doel, aantoonbaar, continu op georganiseerde wijze.

Buiten scope, wat doen we niet:

- Afronden van ISO27001-certificering. Het programma richt zich op voldoen aan de Baseline Informatiebeveiliging Overheid, binnen 2,5 jaar en vooruitlopend op NIS2-wetgeving. In tegenstelling tot de ISO betreft de BIO een verplichte norm. Alle activiteiten en resultaten binnen het programma dragen wel bij aan ISO-normering, die op termijn gevolgd kan worden door certificering. Wanneer, om aan de BIO te voldoen, maatregelen moeten worden genomen die afdoen aan de ISO, wordt dit onderbouwd en geborgt dat dit tijdelijke maatregelen blijven;
- Overige certificeringen die onder het onderwerp Informatiebeveiliging vallen.

2.6 Afhankelijkheden en omgeving

Het programma en de deelprojecten bestaan niet op zichzelf maar moeten hun resultaten behalen in én met de programmaomgeving. Dit betreft om te beginnen de organisatie van de gemeente zelf, die een groot deel van de inspanning en bezetting van programma en projecten zal verzorgen. Op haar beurt is ook de gemeente afhankelijk van haar omgeving, en maakt de organisatie gebruik van dienstverlening door externe partijen.

Deze paragraaf bevat een schets van deze omgeving en externe dienstverlening. Uiteindelijk zullen de afhankelijkheden per project verschillen, en dus ook specifiek ingevuld en beheerst worden.

Interne ontwikkelingen:

- Programma Strategisch Informatiebeleid	Betreft afhankelijkheden en raakvlakken op gebied van beleidsontwikkeling, vervanging legacy systemen (zaaksysteem), ontwikkeling compliance beveiliging informatiestromen (Modernisering Elektronisch Berichtenverkeer) en gezamenlijke claim op schaarse capaciteit.
- Mogelijke verhuizing Gemeentehuis	Betreft lopende ontwikkelingen, betreft voor dit programma vooralsnog vooralsnog impact op gebied fysieke beveiliging, technische maatregelen en als gevolg van keuzes wat betreft mogelijke Cloudstrategie.
- Visie Vernieuwing Dienstverlening	De visie Vernieuwing Dienstverlening is in de maak en wordt in de loop van 2024 gepresenteerd. Deze visie zal komende jaren leidend zijn in een aantal ontwikkelingen binnen de gemeente. Vanuit het programma Strategisch Informatiebeleid wordt momenteel invulling gegeven aan de vernieuwing/implementatie van een zaaksysteem. In de Visie zal ook 'veilige dienstverlening' een aspect zijn. Aan dit onderdeel zal dit programma mede invulling geven. Gedurende de looptijd zal het programma dan ook aan de visie worden getoetst.
- Introductie portfoliomanagement	De gemeente Sluis heeft project- en portfoliomanagement omarmd als methode om als organisatie wendbaar te kunnen zijn. Doel is te komen tot gerichte en transparante besturing in de realisatie van bestuurlijke ambities en organisatiedoelstellingen. Binnen portfoliomanagement zijn inmiddels een aantal kaders, procedures en voorgeschreven (project)producten opgeleverd. Het programma IB Sluis conformeert zich aan deze werkwijze en zal indien mogelijk een bijdrage leveren aan de verdere invulling van portfoliomanagement en de professionalisering van projectmatige werken.
- Project rechtmatigheid	Afhankelijkheid bestaat uit verdere invoering van contractmanagement, waaronder ook borging van IB-aspecten in zowel uitvraag, contract(ering) en contractbewaking. Dit in nauwe afstemming met de in te richten IB-organisatie (i.c. de informatiebeveiligingsadviseur en CISO)

Omgeving (programma)organisatie:

- Provincie/gemeenten	Regionale samenwerking, zowel in IB als dienstverlening en bedrijfsvoering, delen best practices.
- Auditors en accountant	Aansluiting op gewenste controls, niveaus en definities.
- VNG/IBD	Handreikingen, kaders, best practices.

Leveranciers:

- Centric	Alle vak applicaties tot betrekking tot lokale overheid financiën sociaal domein gemeentelijke kern applicaties
- Aon	Cyber risico evaluatie en cyber risico verzekering, BCM
- KnowBe4/ECM	Security awareness programma
- CyberCloud	Pentesting en rapportage kwetsbaarheden
- xixo	Support op firewall en wifi (ook exchange naar nieuwe omgeving)
- Aces IT	Vmware support veeam backup (office 356 backup)
- insight	356 omgeving geïmplementeerd en Intune mobile device management Sharepoint
- qmatic	Klantvolgsysteem (in het KZC)
- KPN	Gemnet (beveiligd netwerk gemeenten)
- Delta	Alle internet verbindingen alle locaties en werkplekken
- Telecom security	Camera beveiliging en toegangs controle
- HPS	Telefoon centrale zip trunk
- logius	Certificaten en DigiD

- creaim	E-herkenning (abbonementen)
- Eye-security	Monitoring SIEM oplossing
- BCT	DMS
- Validsign	Digitale ondertekening
- Xential	Software documentgeneratie
- Cognos	Business intelligence (rapportages)
- Koopkracht	
- Eightfence	
- Blaud	
- Insight	
- PCI	
- ECM	Awareness video's
- Enerse	Architectuur en datamanagement

2.7 Uitgangspunten, randvoorwaarden/beperkingen en programmarisico's

- Weinig projectleiders ter beschikking (inhuur als mogelijke maatregel);
- Kennis-, expertise én capaciteit op ICT-gebied is zeer beperkt en komt samen bij dezelfde persoon (backfill als mogelijk deel van oplossing);
- Bezetting medewerkers vereist op meerdere projecten (inhuur of backfill als mogelijke maatregel);
- Afhankelijkheid leveranciers (beheersing via reguliere lijnafspraken en werkwijze);
- Er bestaat een kans dat maatregelen een desinvestering zullen blijken omdat sprake is van mogelijke verhuizing van de gemeentelijke organisatie, dit geldt met name wat betreft fysieke beveiliging.

3 Programma- en projectorganisatie (en toekomstige IB-organisatie)

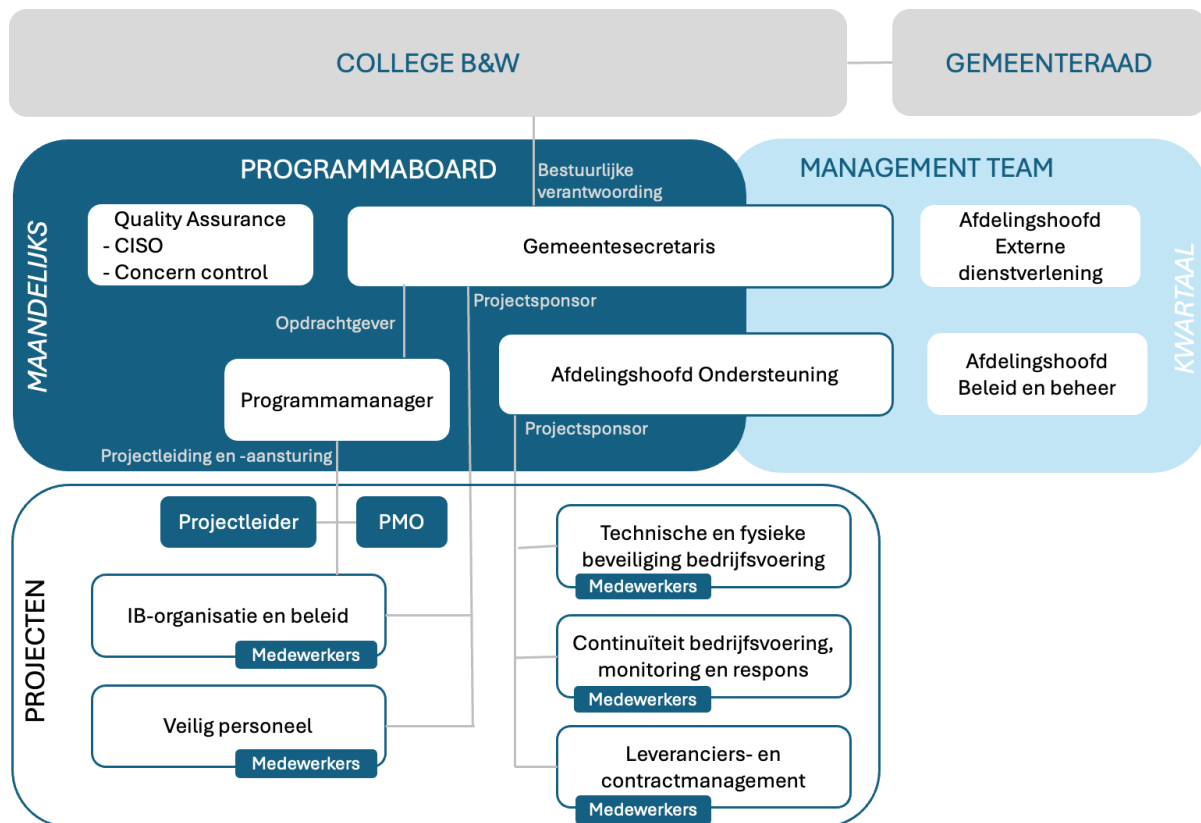
3.1 Besturing

De besturing van het programma en de onderliggende projecten wordt zo 'lean' mogelijk ingevuld binnen een centrale programmaboard, inclusief kwaliteitsborging (Quality Control) en vanzelfsprekend binnen kwalitatieve kaders en methoden. Hiermee wordt voorkomen dat voor ieder project aparte stuurgroepen en stuurgroep meetings worden ingepland. Dit vereist wel dat vanuit de project- en programma coördinatie transparante en gestructureerde informatievoorziening (stuurinformatie) over de diverse projecten wordt verzorgd aan de programmaboard. Deze stuurinformatie behelst zowel de procesmatige voortgang van de geplande activiteiten als inhoudelijke voortgang als gevolg van de resultaten hiervan. Voor de procesmatige voortgang vormen dit programmaplan en de onderliggende projectplannen de basis. Voor de inhoudelijke voortgang zal worden aangesloten op twee producten die in de voorbereiding op dit plan zijn opgezet, te weten de BIO-rapportage en het Kwetsbaarhedenlog (zie voor meer info §6.4).

3.2 Programmaorganisatie en rollen

3.2.1 Programmaorganisatie

Figuur 2 illustreert de programmaorganisatie waarmee de beoogde doelen worden gerealiseerd. Dit behelst zowel de projectinvulling als de generieke besturing en het kwaliteitsmanagement. In het vervolg van deze paragraaf worden de diverse programmarollen nader toegelicht.



Figuur 4: illustratie programmaorganisatie

3.2.2 Besturing vanuit Programmaboard en Managementteam

Programmaboard

De programmaboard bestuurt maandelijks op basis van de door de programmamanager aangeleverde voortgangsrapportage de voortgang en realisatie van het programma en de onderliggende projecten. De programmaboard bestaat uit:

- de direct betrokken MT-leden (opdrachtgever en afdelingshoofs Bedrijfsvoering)
- een quality assurance functie gevormd door de CISO en Concern Controller.

Managementteam

Eens per kwartaal wordt een kwartaalrapportage voorgelegd aan het Managementteam van de gemeente. Onder deze rapportage vallen ook belangrijke mijlpalen binnen het programma, zoals de periodieke herijkingen van dit programmaplan, inclusief de financiële paragraaf, en eventuele projectplannen. De kwartaalrapportage heeft een informerend karakter, waarbij ook eventuele besluitvorming over onderwerpen -na afstemming binnen de programmaboard- aan het MT kan worden voorgelegd.

3.2.3 Rollen binnen het programma

Senior Responsible Owner/Opdrachtgever en 'project sponsor': Gemeentesecretaris

De gemeentesecretaris treedt in het programma op als opdrachtgever en 'senior responsible owner' namens de gemeente. De gemeentesecretaris is tevens voorzitter van de programmaboard en is de verbinding tussen het programma, het College en de Raad.

De belangrijkste verantwoordelijkheid van deze rol is het zorgen dat het programma en haar projecten hun doelen halen en de beoogde baten realiseren. De belangrijkste taak hierbij is verzorgen dat aan de randvoorwaarden wordt voldaan en in de benodigde middelen wordt voorzien.

Lid programmaboard en 'project sponsor': Afdelingshoofd Bedrijfsvoering

De afdelingshoofden zijn lid van de programmaboard en vervullen voor de projecten de rol van project sponsor'.³ Hun belangrijkste verantwoordelijkheid is het realiseren van de gewenste baten vanuit het programma, als resultaat binnen hun organisatieonderdeel. Dit valt grofweg uiteen in drie hoofdtaken, waarbij de projecten logischerwijs op basis van inhoud tussen de afdelingshoofden worden verdeeld:

- vanuit hun onderdeel van de lijnorganisatie beschikbaar stellen van capaciteit en middelen om de benodigde onderliggende projectresultaten op te kunnen leveren;
- zorgdragen dat benodigde lijnactiviteiten die worden gedefinieerd om de programmadoelen te realiseren tijdig en binnen de programma roadmap en projectplanning worden uitgevoerd;
- zorgdragen dat de nieuwe mogelijkheden goed worden ingebed in de bedrijfsvoering en dat hun organisatie onderdeel in staat is met deze nieuwe mogelijkheden de uiteindelijke baten te realiseren.

Bovenstaande betekent dat dit voor de afdelingshoofden met name een sturende en faciliterende rol betreft, maar op bepaalde gebieden of momenten ook de mogelijkheid bestaat dat op uitvoerend niveau specifieke activiteiten of inzet van hen zelf wordt verwacht.

Quality Control: CISO en Concern Controller

De CISO en Concern Controller van de gemeente fungeren binnen het programma als Quality Control. Vanuit deze hoedanigheid nemen zij deel aan de programmaboard, en adviseren zij c.q. stellen zij kaders voor de zowel het programma als de deelprojecten op het gebied van kwaliteit aangaande de (acceptatie van) projectdeliverables.

³ in programmamanagement wordt deze rol ook wel 'Business Change Manager' genoemd, omdat deze als lijnmanager verantwoordelijk blijft voor de verandering in de afdeling van de organisatie zelf.

Programmamanager:

De belangrijkste verantwoordelijkheid van deze rol is de coördinatie en beheersing van het programma en de projecten. De belangrijkste taken hierbij zijn:

- definiëren, toedelen en aansturen van activiteiten van programmateam en projectleiders op basis van programmaplan en specifieke projectplannen of werkpakketten;
- bewaken en bijstellen van de programma activiteiten wat betreft voortgang en afhankelijkheden, binnen de afgesproken tolerantiegrenzen;
- periodieke rapportage over het programma aan opdrachtgever en programmaboard, signaleren en indien noodzakelijk escaleren van knelpunten;
- bewaken van de kwaliteit van het programma en functionaliteit van opgeleverde projectproducten, binnen de afgesproken kaders;
- financieel beheer van het programma en projecten.

Projectleider(s):

De belangrijkste verantwoordelijkheid van deze rol is de coördinatie en beheersing van het deelproject, inhoudelijke advisering en uitvoering, en de tijdige en kwalitatieve oplevering van de projectresultaten. De belangrijkste taken hierbij zijn:

- definiëren, toedelen en aansturen van activiteiten van projectteam op basis van projectplan en specifieke projectplannen of werkpakketten;
- opstellen/ontwikkelen en implementeren van (BIO-)producten
- bewaken en bijstellen van de projectactiviteiten wat betreft voortgang en afhankelijkheden, binnen de afgesproken tolerantiegrenzen;
- periodieke rapportage over het project aan programmamanagement, signaleren en indien noodzakelijk escaleren van knelpunten;
- bewaken van de kwaliteit van het project en functionaliteit van opgeleverde projectproducten, binnen de afgesproken kaders;
- financieel beheer van het project binnen de programmabeheersing.

Programmamanagement Ondersteuning (PMO): Leverancier

De PMO'er administreert, ondersteunt en bewaakt als rechterhand van de programmamanager de processen en voortgang van het programma en de onderliggende projecten op de aspecten Tijd, Geld en Kwaliteit (planning budget en, rapportage). Vanuit het dit continue contact hierover met betrokken partijen behelst deze rol ook de continue optimalisatie van de (beheers)processen.

De rol van PMO kan worden aangevuld met meer specifieke, inhoudelijke taken, zowel in de beheersing als in de realisatie. Concreet zal de PMO een centrale rol vervullen in de risicobeheersing (van identificatie tot bewaking en rapportage). Ook kan – in overleg – een beroep op de PMO worden gedaan bij te dragen aan de ontwikkeling van beleid, procedures en processen op het gebied van Informatiebeveiliging.

Risicomanager: uitvoering door PMO

De risicomanager is verantwoordelijk voor correcte inrichting en uitvoering van het risicomanagement. Dit betreft taken als het beheren van het risicolog, ondersteunen van risicoanalyse, verzorgen van de risicorapportage en het najagen van risico actiehouders en eigenaren;

Voorstel is deze rol in te laten vullen door PMO, onder verantwoordelijkheid Programmamanager

Stakeholder manager: Communicatie adviseur, gemeente Sluis

De stakeholdermanager organiseert, bewaakt en verbetert het proces waarmee alle belanghebbenden bij het programma en de onderliggende projecten betrokken worden en blijven. Van het systematisch identificeren van belanghebbenden; het analyseren van hun behoeften en verwachtingen tot het plannen en uitvoeren van verschillende taken om met hen in contact te komen en te blijven. Gezien de omvang van de organisatie en de relaties met aanpalende programma's ligt het voor de hand deze rol te combineren binnen de bestaande lijnfunctie die ook de interne communicatie verzorgt. Het systematisch identificeren van belanghebbenden, analyseren van behoeften en verwachtingen en plannen van communicatie zal in de praktijk een samenwerking zijn tussen de stakeholdermanager, de programmamanager en de projectleiders, waarbij de stakeholdermanager coördinerend optreedt en adviseert.

Vertegenwoordiging organisatie afdelingen: leden Informatiebeveiligingsplatform

De leden van het Informatiebeveiligingsplatform zullen, al naar gelang de stakeholderanalyse op projectniveau dit aangeeft, worden betrokken bij de uitvoering dan wel worden geïnformeerd over de uitvoering. Dit vanuit hun reguliere rol en verantwoordelijkheid als lid van dit platform.

4 Roadmap, projecten en planning

4.1 Roadmap

Deze paragraaf bevat de ‘roadmap’ voor de programma Informatiebeveiliging Sluis op het niveau van projecten en onderliggende thema’s uit de BIO. Nadere verdieping vanuit deze thema’s in controls en – uiteindelijk – maatregelen vindt plaats in de projecten. Op control niveau geeft dit programmaplan hiervoor reeds een aanzet, detaillering in daadwerkelijk uit te voeren maatregelen, planning en realisatie daarvan vindt per project plaats als onderdeel van de projectdefinitie. De planvorming van de projecten vindt plaats in lijn met de roadmap van het programma, zodat ook onderlinge relaties in beeld komen én blijven.

De belangrijkste mijlpalen voor het programma en de onderliggende projecten zijn:

FASE 1: Veilig worden

- Gedetailleerde faseplannen voor deze fase op basis van de werkpakketten voor alle projecten.
- Alle ‘critical’ en ‘high’ geclassificeerde risico’s zijn gemitigeerd, doordat de betreffende beheersmaatregelen op werkingsniveau aantoonbaar zijn geïmplementeerd.
- *Er is een proces ingericht voor de beheersing van risico’s en kwetsbaarheden die vanaf dat moment worden geconstateerd.*
- Er is een plan van aanpak (programmaplan en aanvullende projectplannen) voor de periode t/m 2026, *inclusief de overdracht naar de lijnorganisatie vanuit projecten gedurende die periode.*

FASE 2: Veilig blijven

Alle beheersmaatregelen (het geheel van een ISMS) zijn op werkingsniveau geïmplementeerd.

Vanuit deze twee fases en de projectverkaveling gebaseerd op BIO thema’s ontstaat dan op hoofdlijnen onderstaande roadmap voor de periode 2024-2026. Deze roadmap visualiseert tevens - met name op themaniveau – dat de inzet op de projecten over de periode 2024-2026 wordt verdeeld. Dit geldt zowel binnen de totale roadmap en de projecten, als binnen de projecten zelf die in de volgende paragrafen zijn uitgewerkt. Deze verdeling is tot stand gekomen door i) een inschatting van de urgentie van thema’s activiteiten vanuit de gedachte ‘Veilig worden en veilig blijven’, ii) doordat om uiteenlopende redenen realistisch uitgangspunt is voor een aantal thema’s een langere termijn voor realisatie te hanteren en iii) door te kijken naar logische volgorde van activiteiten (zoals eerst beleid opstellen, dan implementeren).

Deze verdeling over de fases en jaren fungeert tevens als mitigerende maatregelen op de schaarste in beschikbare middelen/inzet.

		VEILIG WORDEN		VEILIG BLIJVEN			
		2024		2025		2026	
Project/Thema	BIO-ref	Q2	Q4	Q2	Q4	Q2	Q4
Programmabeheersing en -besturing							
Maandelijkse stuurgroep, incl. rapportage en quality control							
Halfjaarlijkse evaluatie en herijking programmaplan, incl business case							
Programma decharge							
Project IB-organisatie en Beleid							
Aansturing door de directie van de informatiebeveiliging	5.1						
Interne organisatie	6.1						
Mobiele apparatuur en telewerken	6.2						
Informatieclassificatie	8.2						
Cryptografische beheersmaatregelen	10.1						
Project Continuïteit bedrijfsvoering, monitoring & response							
Bedieningsprocedures en verantwoordelijkheden	12.1						
Verslaglegging en monitoren	12.4						
Overwegingen betreffende audits van informatiesystemen	12.7						
Beheer van informatiebeveiligingsincidenten en verbeteringen	16.1						
Informatiebeveiligingscontinuïteit	17.1						
Naleving van wettelijke en contractuele eisen	18.1						
Informatiebeveiligingsbeoordelingen	18.2						
Project Technische & fysieke beveiliging bedrijfsvoering							
Verantwoordelijkheid voor bedrijfsmiddelen	8.1						
Behandelen van media	8.3						
Bedrijfseisen voor toegangsbeveiliging	9.1						
Toegangsbeveiliging van systeem en toepassing	9.4						
Beveiligde gebieden	11.1						
Apparatuur	11.2						
Bescherming tegen malware	12.2						
Back-up	12.3						
Beheersing van operationele software	12.5						
Beheer van technische kwetsbaarheden	12.6						
Beheer van netwerkbeveiliging	13.1						
Informatietransport	13.2						
Redundante componenten	17.2						
Project Veilig personeel							
Voorafgaand aan het dienstverband	7.1						
Tijdens het dienstverband	7.2						
Beëindiging en wijziging van dienstverband	7.3						
Beheer van toegangsrechten van gebruikers	9.2						
Verantwoordelijkheden van gebruikers	9.3						
Project Leveranciers- en contractmanagement							
Beveiligingseisen voor informatiesystemen	14.1						
Beveiliging in ontwikkelings- en ondersteunende processen	14.2						
Testgegevens	14.3						
Informatiebeveiliging in leveranciersrelaties	15.1						
Beheer van dienstverlening van leveranciers	15.2						

Figuur 5: Roadmap Informatiebeveiliging Sluis (programmaniveau)

4.1.1.1 Projecten

Op basis van de BIO en NIS2 is een verkaveling gevormd van projecten die binnen het programma zullen bijdragen aan de realisatie van de doelen. Deze verkaveling leidt tot 5 projecten waarbinnen de gehele BIO wordt geadresseerd en geïmplementeerd, op zowel opzet- als werkingsniveau. De hoofdstukken van de BIO bevatten meerdere controls die uitgevoerd moeten worden voor het implementeren van de hoofdstukken. Deze controls hebben een directe relatie tot de deliverables op basis waarvan bij oplevering aantoonbaar kan worden gemaakt dat de implementatie op een (op dat moment) afgesproken niveau is uitgevoerd.

De projecten starten niet sequentieel, maar tegelijk. Op niveau van producten en controls wordt vervolgens een volgorde vastgesteld die met name gebaseerd zal zijn op onderlinge afhankelijkheden tussen 1) de op te leveren resultaten en 2) de beschikbare capaciteit om deze resultaten te realiseren (niet te veel tegelijk).

Per project zal een verdere verdieping plaatsvinden van benodigde inzet, specifieke afhankelijkheden, acceptatiecriteria van de producten en verantwoordelijkheid bij- en besturing van de realisatie op productniveau. Hiervoor wordt gebruik gemaakt van generiek opgestelde werkpakketten die aansluiten op de projectscope én de hoofdstukken, thema's en controls van de BIO. In bijlage 8.2 is een eerste invulling voor alle werkpakketten opgenomen. Deze zullen in de respectievelijke projectdefinities verder worden uitgewerkt en vastgesteld. Bronnen hiervoor zijn onder andere de nieuw opgezette BIO-rapportage en Kwetsbaarhedenlog.

Om de projectdefinitie en prioritering van projectactiviteiten te kunnen maken (en daarna besturen) is het van belang de rapportageproducten 'BIO-rapportage' en 'Kwetsbaarhedenlog' inhoudelijke te blijven vullen en hanteren.

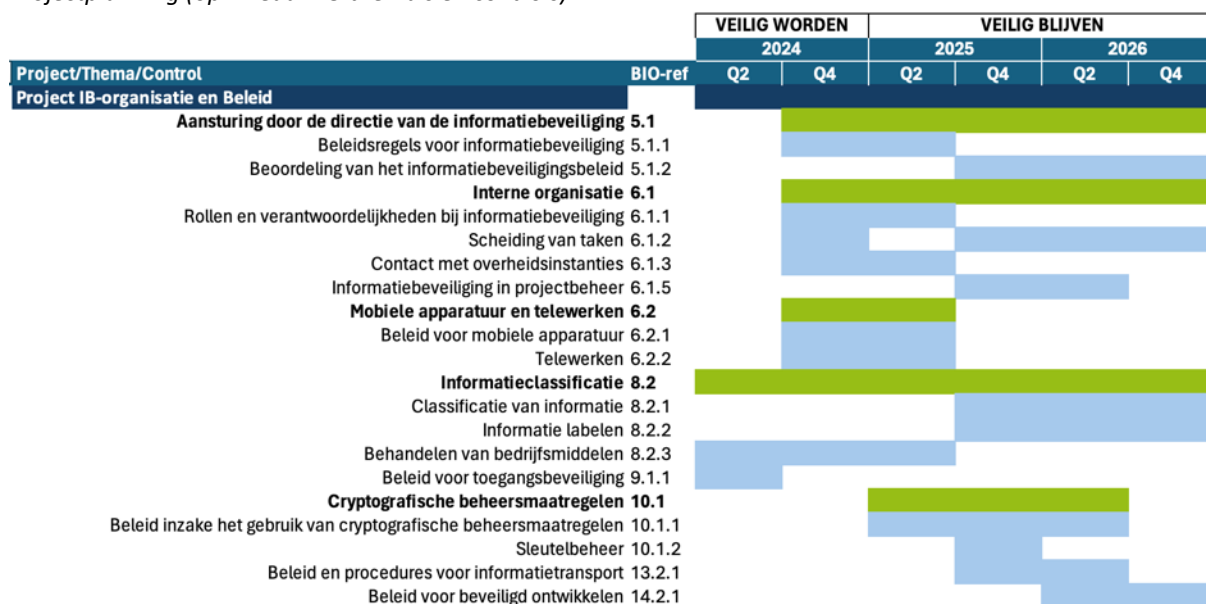
Project 1: IB-organisatie en Beleid

In dit project worden de hoofdstukken 5, 6, 8 en 9 van de BIO aangepakt. Deze hoofdstukken richten zich meer op het opstellen van beleidsstukken voor de organisatie.

Projectdoelen (incl. BIO-verwijzing):

1. Het verschaffen van directieaansturing van en -steun voor informatiebeveiliging in overeenstemming met bedrijfseisen en relevante wet- en regelgeving. (5.1)
2. Een beheerkader vaststellen om de implementatie en uitvoering van de informatiebeveiliging binnen de organisatie te initiëren en te beheersen. (6.1)
3. Het waarborgen van de veiligheid van telewerken en het gebruik van mobiele apparatuur. (6.2)
4. Bewerkstelligen dat informatie een passend beschermingsniveau krijgt dat in overeenstemming is met het belang ervan voor de organisatie. (8.2)
5. Zorgen voor correct en doeltreffend gebruik van cryptografie om de vertrouwelijkheid, authenticiteit en/of integriteit van informatie te beschermen. (10.1)

Projectplanning (op niveau BIO thema's en controls)



Figuur 6 Hoofdpijnenplanning project Organisatie en beleid (niveau thema en controls)

Projectdeliverables (incl. Bio verwijzing):

Uit de controls en maatregelen zoals beschreven onder dit thema van de BIO volgen voor dit project op hoofdlijnen de volgende voorbeelden van projectproducten (deliverables), welke in de werkpakketten van het project nader zullen worden gespecificeerd:

Projectproduct/deliverable	BIO control
Informatiebeveiligingsbeleid, periodieke beoordeling van beleid	5.1
Ontwerp IB-organisatie (Beheerkader om implementatie en uitvoering van de informatiebeveiliging binnen organisatie te kunnen beheersen) ⁴	6.1
Beleid voor mobiele apparatuur, beleid voor thuiswerken/ op afstand werken	6.2

⁴ Vanuit VNG/IBD is een handreiking "Team op sterkte" opgeleverd van een minimaal benodigde invulling en rollen die geborgd dienen te zijn in een IB-organisatie om de informatiebeveiliging in gemeenten te kunnen beheersen. Vanuit deze handreiking zal de ontwerp IB-organisatie voor de gemeente Sluis worden vormgegeven, in de meerjarige programmabegroting is hier reeds op geanticipeerd.

Classificeren van informatie	8.2
Beleid voor toegangsbeveiliging	9.1.1
Cryptografiebeleid	10.1
Beleid en procedures voor informatietransport	13.2.1
Beleid voor beveiligd ontwikkelen	14.2.1

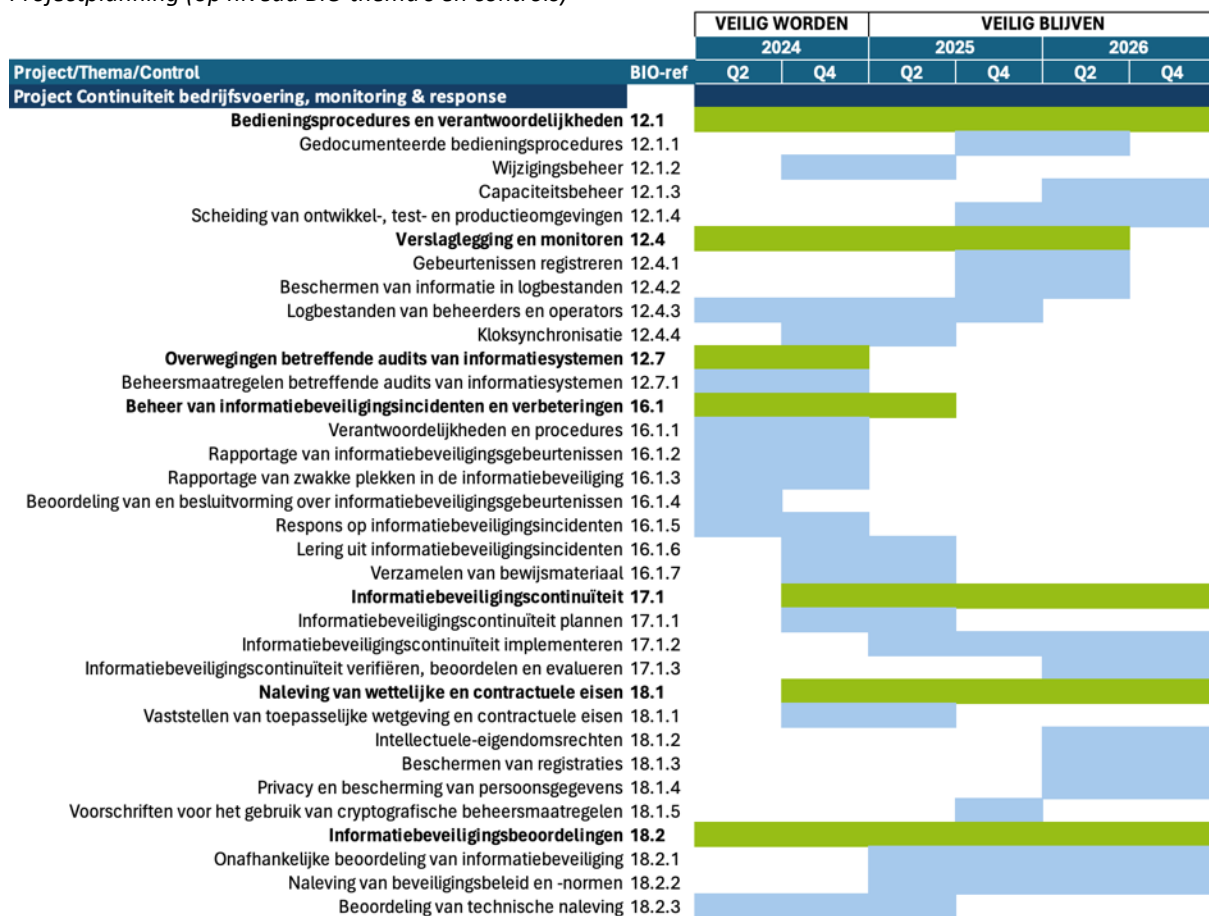
Project 2: Continuïteit bedrijfsvoering, monitoring & response

In dit project worden de hoofdstukken 12, 16, 17 en 18 van de BIO aangepakt. Deze hoofdstukken richten zich meer op de continuïteit & beheersing van de organisatie.

Projectdoelen (incl. BIO-verwijzing):

1. Correcte en veilige bediening van informatie verwerkende faciliteiten waarborgen. (12.1)
2. Gebeurtenissen vastleggen en bewijs verzamelen. (12.4)
3. De impact van auditactiviteiten op uitvoeringssystemen zo gering mogelijk maken. (12.7)
4. Een consistente en doeltreffende aanpak bewerkstelligen van het beheer van informatiebeveiligingsincidenten, met inbegrip van communicatie over beveiligingsgebeurtenissen en zwakke plekken in de beveiliging. (16.1)
5. Informatiebeveiligingscontinuïteit behoort te worden ingebed in de systemen van het bedrijfscontinuïteitsbeheer van de organisatie. (17.1)
6. Voorkomen van schendingen van wettelijke, statutaire, regelgevende of contractuele verplichtingen betreffende informatiebeveiliging en beveiligingseisen. (18.1)
7. Verzekeren dat informatiebeveiliging wordt geïmplementeerd en uitgevoerd in overeenstemming met de beleidsregels en procedures van de organisatie. (18.2)

Projectplanning (op niveau BIO thema's en controls)



Figuur 7 Hoofddijnenplanning project Continuïteit bedrijfsvoering, monitoring en respons (niveau thema en controls)

Projectdeliverables (incl. BIO-verwijzing):

Uit de controls en maatregelen zoals beschreven onder dit thema van de BIO volgen voor dit project op hoofdlijnen de volgende voorbeelden van projectproducten (deliverables), welke in de werkpakketten van het project nader zullen worden gespecificeerd:

Projectproduct/deliverable	BIO control
Gedocumenteerde Bedieningsprocedure, procedure wijzigingsbeheer,	12.1
Logregels en logbestanden maken en beschermen	12.4
Directiebeoordeling, incidentenlog,	12.7
Classificeren van informatie	16.1
Informatiebeveiligingscontinuïteit ingebed in het bedrijfscontinuïteitsbeheer van de organisatie.	17.1
Registratie en beheer van alle relevante wettelijke statutaire, regelgevende, contractuele eisen voor elk informatiesysteem en de organisatie, inclusief de aanpak van de organisatie om aan deze eisen te voldoen.	18.1
ISMS beoordeling en naleven van IB	18.2

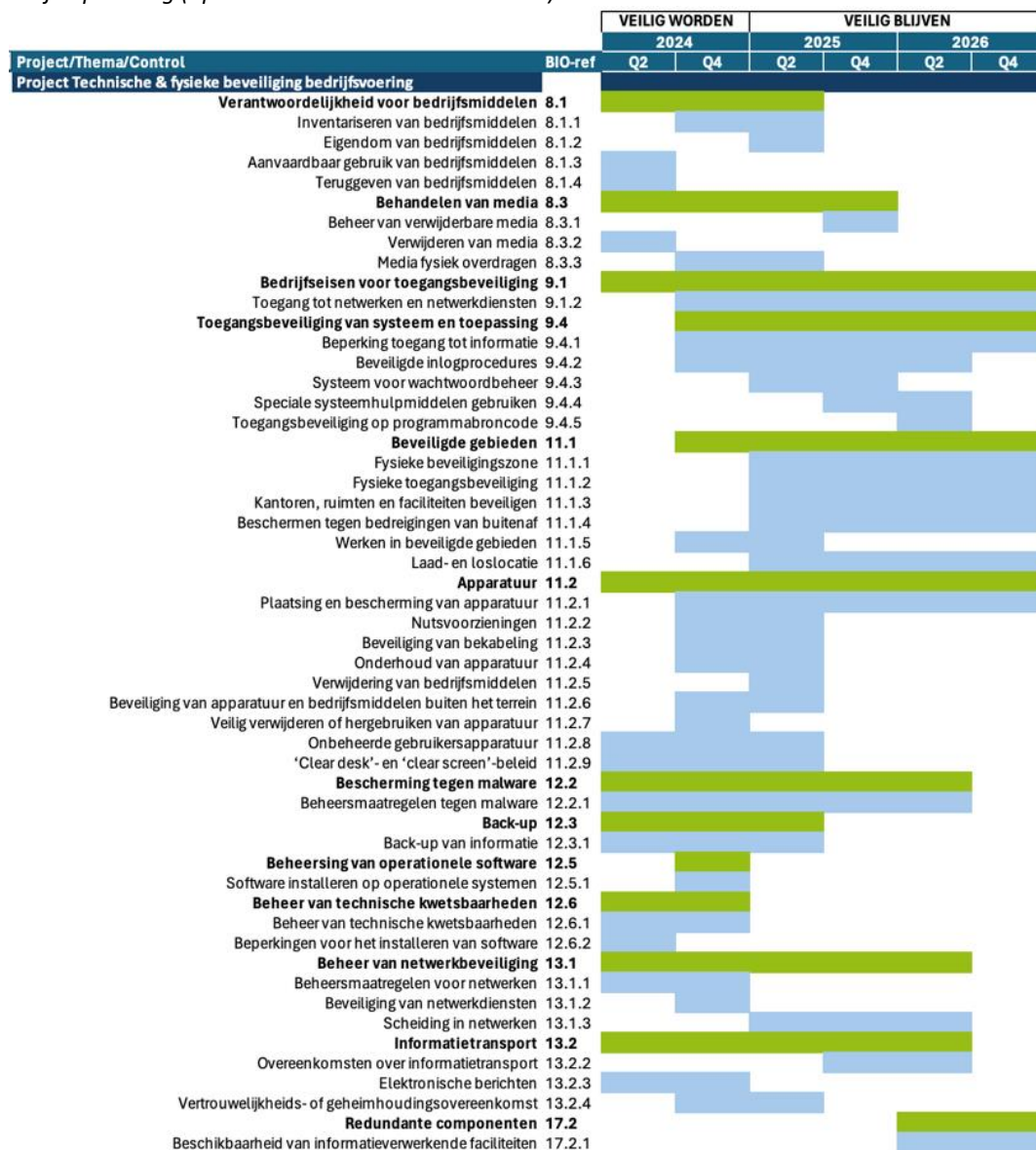
Project 3: Technische & fysieke beveiliging bedrijfsvoering

In dit project worden de hoofdstukken 8, 10, 11, 12, 13 en 17 van de BIO aangepakt. Deze hoofdstukken richten zich meer op de continuïteit & beheersing van de organisatie.

Projectdoelen (incl. BIO-verwijzing):

1. Bedrijfsmiddelen van de organisatie identificeren en passende verantwoordelijkheden ter bescherming definiëren. (8.1)
2. Onbevoegde openbaarmaking, wijziging, verwijdering of vernietiging van informatie die op media is opgeslagen voorkomen. (8.3)
3. Toegang tot informatie en informatie verwerkende faciliteiten beperken. (9.1)
4. Onbevoegde toegang tot systemen en toepassingen voorkomen. (9.4)
5. Onbevoegde fysieke toegang tot, schade aan en interferentie met informatie en informatie verwerkende faciliteiten van de organisatie voorkomen. (11.1)
6. Verlies, schade, diefstal of compromittering van bedrijfsmiddelen en onderbreking van de bedrijfsvoering van de organisatie voorkomen. (11.2)
7. Waarborgen dat informatie en informatie verwerkende faciliteiten beschermd zijn tegen malware. (12.2)
8. Beschermen tegen het verlies van gegevens. (12.3)
9. De integriteit van operationele systemen waarborgen. (12.5)
10. Benutting van technische kwetsbaarheden voorkomen. (12.6)
11. De bescherming van informatie in netwerken en de ondersteunende informatie verwerkende faciliteiten waarborgen. (13.1)
12. Handhaven van de beveiliging van informatie die wordt uitgewisseld binnen een organisatie en met een externe entiteit. (13.2)
13. Beschikbaarheid van informatie verwerkende faciliteiten bewerkstelligen. (17.2)

Projectplanning (op niveau BIO-thema's en controls)



Figuur 8 Hoofdlijnenplanning project Technische en fysieke beveiliging bedrijfsvoering (niveau thema en controls)

Projectdeliverables (incl. BIO-verwijzing):

Uit de controls en maatregelen zoals beschreven onder dit thema van de BIO volgen voor dit project op hoofdlijnen de volgende voorbeelden van projectproducten (deliverables), welke in de werkpakketten van het project nader zullen worden gespecificeerd:

Projectproduct/deliverable	BIO control
Verantwoordelijkheid bedrijfsmiddelen	8.1
Procedure voor behandelen media	8.3
Toegangsbeperkende maatregelen	9.1 (m.u.v. 9.1.1)
Afdwingen wachtwoordbeleid	9.4
Procedures fysieke beveiliging	11.1
Procedures/(beleid?) beveiliging apparatuur	11.2
Maatregelen toepassen/ kwetsbaarheden weg werken	12.2
Back-up maatregelen nemen en kwetsbaarheden wegwerken	12.3
Procedures ingericht om het op operationele systemen installeren van software te beheersen.	12.5

Kwetsbaarhedenlog	12.6
Netwerk kwetsbaarheden weg werken, netwerkbeveiligen en netwerk scheiden	13.1
(Beleid?) voor informatie transport, overeenkomsten informatietransport /vertrouwelijk/geheime overeenkomst	13.2
Informatie verwerkende faciliteiten redundantie	17.2

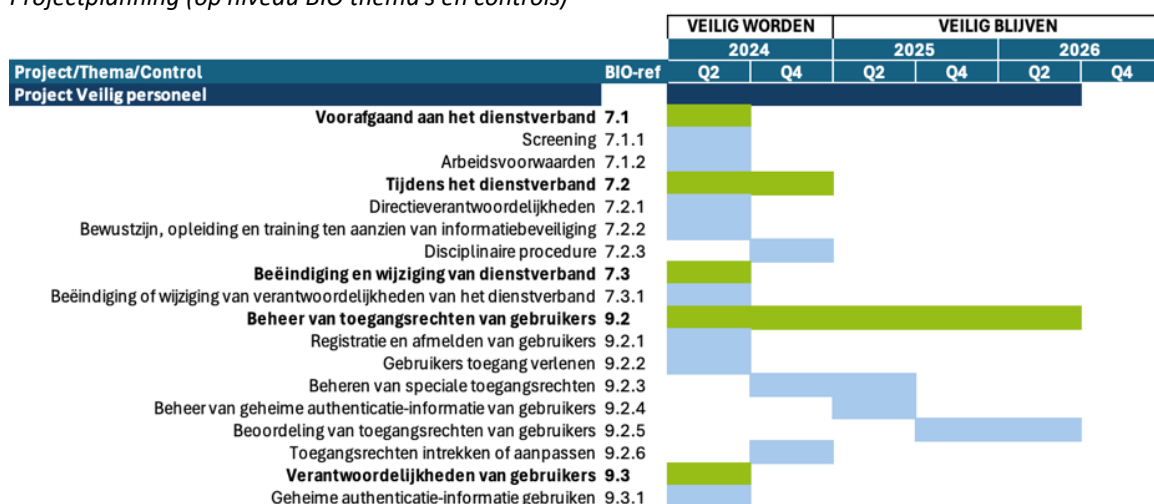
Project 4: Veilig personeel

In dit project worden met name hoofdstuk 7 en 9 van de BIO aangepakt. Deze hoofdstukken richten zich op het personeel en hun gegevens hiervan binnen de organisatie.

Projectdoelen (incl. BIO-verwijzing):

1. Waarborgen dat medewerkers en contractanten hun verantwoordelijkheden begrijpen en geschikt zijn voor de rollen waarvoor zij in aanmerking komen. (7.1)
2. Ervoor zorgen dat medewerkers en contractanten zich bewust zijn van hun verantwoordelijkheden op het gebied van informatiebeveiliging en deze nakomen. (7.2)
3. Het beschermen van de belangen van de organisatie als onderdeel van de wijzigings- of beëindigingsprocedure van het dienstverband. (7.3)
4. Toegang voor bevoegde gebruikers bewerkstelligen en onbevoegde toegang tot systemen en diensten voorkomen. (9.2)
5. Gebruikers verantwoordelijk maken voor het beschermen van hun authenticatie-informatie. (9.3)

Projectplanning (op niveau BIO thema's en controls)



Figuur 9 Hoofdpijnenplanning project Veilig personeel (niveau thema en controls)

Projectdeliverables (incl. BIO-verwijzing):

Uit de controls en maatregelen zoals beschreven onder dit thema van de BIO volgen voor dit project op hoofdlijnen de volgende voorbeelden van projectproducten (deliverables), welke in de werkpakketten van het project nader zullen worden gespecificeerd:

Projectproduct/deliverable	BIO control
Screeningbeleid, VOG	7.1
Bewustwording (awareness trainingen) Disciplinaire procedures	7.2
Procedure beëindiging dienstverband	7.3
Toegangsrechten	9.2
Authenticatie procedures Beschikbaar stellen van een wachtwoordenkluis.	9.3

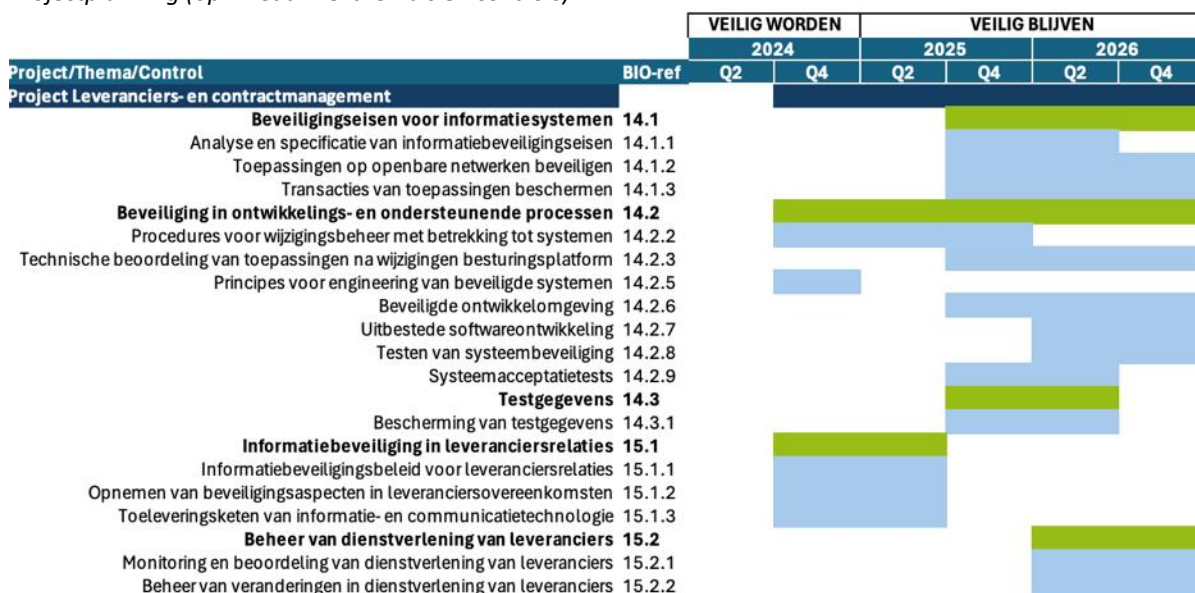
Project 5: Leveranciers- en contractmanagement (externe IB afhankelijkheid)

In dit project worden de hoofdstukken 14 en 15 van de BIO aangepakt. Deze hoofdstukken richten zich meer op dienstverlening door leveranciers voor de organisatie, en de eisen die de organisatie aan deze dienstverlening stelt.

Projectdoelen (incl. BIO-verwijzing):

1. Waarborgen dat informatiebeveiliging integraal deel uitmaakt van informatiesystemen in de gehele levenscyclus. Hiertoe behoren ook de eisen voor informatiesystemen die diensten verlenen via openbare netwerken. (14.1)
2. Bewerkstelligen dat informatiebeveiliging wordt ontworpen en geïmplementeerd binnen de ontwikkelingslevenscyclus van informatiesystemen. (14.2)
3. Bescherming waarborgen van gegevens die voor het testen zijn gebruikt. (14.3)
4. De bescherming waarborgen van bedrijfsmiddelen van de organisatie die toegankelijk zijn voor leveranciers. (15.1)
5. Een overeengekomen niveau van informatiebeveiliging en dienstverlening in overeenstemming met de leveranciersovereenkomsten handhaven. (15.2)

Projectplanning (op niveau BIO-thema's en controls)



Figuur 10 Hoofddijnenplanning project Leveranciers en contractmanagement (niveau thema en controls)

Projectdeliverables (incl. BIO-verwijzing):

Uit de controls en maatregelen zoals beschreven onder dit thema van de BIO volgen voor dit project op hoofdlijnen de volgende voorbeelden van projectproducten (deliverables), welke in de werkpakketten van het project nader zullen worden gespecificeerd:

Projectproduct/deliverable	BIO control
Eisen voor informatiesystemen die diensten verlenen via openbare netwerken	14.1
Waarborging dat eisen worden toegepast	14.2
Bescherming testgegevens in beleid	14.3
IB-Beleid voor leverancier relaties	15.1
Monitoren van dienstverlening leveranciers	15.2

4.2 Inzet binnen programma en projecten

Binnen het programma is in ieder geval inzet nodig van een 'programma organisatie'. Deze bestaat uit zowel specifiek ingezette expertises en rollen, als rollen die vanuit bestaande functie en rol in lijnorganisatie worden

betrokken. Onder specifieke expertises en rollen in de programmaorganisatie worden verstaan: programmamanagement, programmaondersteuning, projectleiding, risicomanagement, stakeholder- en communicatiemanagement.

Expertises en rollen die vanuit lijnorganisatie worden voorzien betreffen rollen in de besturing, kwaliteitsbewaking, die zullen worden aan functionarissen waarvoor dergelijke rol weliswaar tijd en aandacht vergt, maar tevens binnen hun reguliere functie (denk aan opdrachtgever, CISO en concern control).

Binnen de projecten zal van diverse betrokkenen uit de lijnorganisatie tijd en aandacht (in verschillende mate) geclaimd moeten worden om de resultaten te realiseren. Wanneer deze capaciteit niet beschikbaar is binnen de organisatie kan per project externe inzet worden gebruikt.

Omdat specifieke organisatie kennis niet van buiten kan worden ingehuurd, zal op programmaniveau een zogenaamde 'backfill' constructie moeten worden ingezet. Hiermee is in de raming van het programmabudget rekening gehouden. Met een 'backfill' constructie kan een organisatie haar werkzaamheden door tijdelijke inzet op peil houden (zowel kwalitatief als kwantitatief) en toch interne capaciteit en expertise vrijmaken voor de realisatie van de producten en doelen.

5 Investerings en kosten

5.1 Uitwerking en onderbouwing 'out of pocket' kosten op programmaniveau

Deze paragraaf beschrijft de kosten die uit het programma voortvloeien. Deze kosten bestaan uit incidentele kosten (uitvoering programma, veilig worden) en structurele kosten (veilig blijven). Het betreft hier 'out of pocket kosten', waarmee de kosten worden bedoeld die extern worden gemaakt voor zaken waar de organisatie (nog) niet zelf in kan voorzien. Deze kosten kunnen bestaan uit inzet, diensten en/of producten. Voor het programma kunnen een aantal vaste kostenposten worden gedefinieerd en geraamd. Per component wordt aangegeven welke kostencomponenten te voorzien zijn, en in welk jaar binnen de looptijd van het programma. Een meer gedetailleerde uitwerking per component wordt als onderdeel van de projectopzet nader gespecificeerd.

Een deel van de veiligheidsmaatregelen zijn momenteel al onderdeel van de reguliere bedrijfsvoering (en begroting) dan wel sterk gerelateerd aan de bedrijfsvoering, en bijvoorbeeld ook toekomstige ontwikkelingen als de mogelijke verhuizing van het gemeentehuis. De afhankelijkheid tussen deze kosten moet vooral worden gezien in termen van desinvestering en synergie. Zo is de vraag in hoeverre moet worden geïnvesteerd in verbetering van fysieke beveiliging van de huidige locatie, terwijl synergie kan worden benut deze als vereiste aan de nieuwe locatie wordt meegenomen. Tegelijkertijd heeft een keuze om ontwikkelingen (zoals bv Cloud migratie) niet in te zetten mogelijk negatieve impact op het programmabudget, aangezien in dat geval de te continueren situatie "veilig moet worden gemaakt". Dit vereist andere inzet en middelen, waar dus ook andere kosten aan verbonden zullen zijn.

Als onderdeel van de roadmap worden de kosten daarom niet alleen per project nader gespecificeerd, maar is tevens een periodieke herijking van programmaplan en (financiële) businesscase in programboard/MT opgenomen.

Tabel 1: meerjarenraming kosten programma IB Sluis (alle bedragen *€1000)

Kosten component	Opmerking	U structureel	Begroet	2024	2025	2026	2027	2028
Programmamanagement/projectleiding	10 uur/week	Incidenteel	Nee	45	85	85	-	-
Projectleiding	10 uur/week	Incidenteel	Nee	30	60	-	-	-
Information Security Officer *	10 uur week	Incidenteel	Nee	30	60	-	-	-
Project Management Office (tijdelijke vervang	10 uur/week, 9 mnd	Incidenteel	Nee	30	10	-	-	-
Backfill Technical Information Sec. Officer **	Vrijspelen TISO-rol (4 dgn week	Incidenteel	Nee	35	70	70	-	-
Opleiding programma/projectmatig		Incidenteel	Nee	2	2	2	-	-
Business Continuity Management-traject	Inrichten en eerste oefening	Incidenteel	Nee	-	50	-	-	-
Opleiding		Incidenteel	Nee	10	10	10	-	-
ISMS-tooling inrichting		Incidenteel	Nee	10	-	-	-	-
Communicatie		Incidenteel	Nee	5	5	5	-	-
Cyberverzekering		Incidenteel	Nee	25	50	50	-	-
Kostencomponenten uit begroting organisatie onderdelen								
ISMS-tooling licentiekosten		Structureel	Ja		10	10	10	10
IB-organisatie *	1FTE (9) ISO rol/expertise	Structureel	Nee	-	90	90	90	90
Pentesten		Incidenteel	50%	15	30	-	-	-
Additionele auditkosten	Verhoogde handhaving	Structureel	Nee	10	10	10	10	10
Certificering ISO27001		Incidenteel	Nee	-		10	-	-
Wachtwoordkluis		Structureel	Nee	20	20	20	20	20
	Som programma componenten incidenteel:			222	402	222	-	-
	Onvoorzien programmbudget(10%):			22,2	40,2	22,2	-	-
	Programmakosten incidenteel totaal:			244,2	442,2	244,2	-	-
	identele ophoging Budget IB-organisatie BIO/NIS2:			15	30	10	-	-
	ucturele ophoging budget IB-organisatie BIO/NIS2:			30	130	130	130	130

* Naar het zich laat aanzien kan de invulling van een 'ISO-rol' binnen de gemeente FTE-neutraal worden gerealiseerd. Hiermee vallen de structurele kosten in de jaren 2026 e.v. €90.000 per jaar lager uit, namelijk op €40.000 per jaar. Deze FTE-neutrale invulling dient nog wel te worden geformaliseerd. Het proces hiervoor is binnen het programma opgestart en zal ter besluitvorming via de programma board worden voorgelegd aan het MT.

** Toelichting rollen Informatiebeveiliging:

CISO: De *Chief Information Security Officer* betreft een kaderstellende, toetsende en adviserende rol op strategisch niveau, met een rechtstreekse lijn naar MT en/of Bestuur;

ISO: De *Information Security Officer* betreft een operationele of tactische rol ten aanzien van beleid en procedures, binnen de IT- of beveiligingsafdeling. De ISO rapporteert hierover aan de CISO of een leidinggevende in de IT;

TISO: De *Technical Information Security Officer* is specifiek gericht op de technische aspecten van informatiebeveiliging binnen een organisatie. Deze wordt dan ook vaak gecombineerd met uitvoerende rollen binnen de IT-organisatie. Voor de TISO-werkzaamheden vereisen wel voldoende tijd, aandacht en het opbouwen en instand houden van specifieke expertise.

6 Programmabeheersing

6.1 Risicomanagement

Deze paragraaf beschrijft de geïdentificeerde risico's op programmaniveau. De paragraaf vormt daarmee tevens de basis voor het risicoregister wat gedurende de looptijd van het programma wordt opgesteld en gehanteerd.

Het risico- en issueregister dat voor risicomanagement wordt gebruik wordt programma breed ingevuld en zal in het centrale programmadosier worden geactualiseerd. Vanuit projectdefinitie en -beheersing zullen hieraan eventuele specifieke projectrisico's worden toegevoegd.

Vanuit dit centrale risicoregister worden vervolgens de belangrijkste programma- en projectrisico's gerapporteerd in de reguliere, periodieke programmarapportage aan de programmaboard. Optredende risico's zullen als issues worden beschouwd en -indien nodig- als zodanig aan de programmaboard worden geëscaleerd.

NB: deze risico's betreffen de realisatie van de doelstellingen van het programma en de onderliggende projecten en mogen niet worden verward met de generieke risico's (informatiebeveiliging en continuïteit) die voor de gemeentelijke organisatie worden beheerst.

6.2 Programmarisico's

#	Korte Risicon naam	Risicobeschrijving (oorzaak -> gebeurtenis -> gevolg)	Maatregel omschrijving	Weging (Kans x impact)
1	Capaciteit	Onvoldoende capaciteit beschikbaar om producten conform afgesproken kwaliteit en tijdigheid op te leveren, met gevolg voor doorlooptijd, kwaliteit en doelstelling.	Inzetraming baseren op projectproducten en werkpakketten; Inhoudelijke ondersteuning vanuit programma en projecten. Beschikbaar stellen van (centrale) resources, indien noodzakelijk op basis van inhuur. Gedeelte van programmabudget oormerken voor 'backfill' oplossingen.	HOOG
2	Verwachtingen en risicobereidheid i.r.t. haalbaarheid en kosten	Normen dienen situationeel te worden toegepast. Te hoge verwachtingen t.a.v. omvang of diepgang van implementatie, of een zeer lage risicobereidheid verkleinen de haalbaarheid het project en/of verhogen de kosten.	Vroegtijdig inventariseren en concretiseren van maatregelen in relatie tot normering, in kaart brengen impact en opties en gestructureerde besluitvorming door programmaboard o.b.v. ambitieniveau en risicobereidheid.	HOOG
3	Draagvlak	Impact en urgentie worden onderkend (tot zorg aan toe), maar voelt de organisatie ook eigenaarschap van het probleem of de inspanning?	Deelname afdelingen aan programmaboard, vanuit verantwoordelijkheid afdeling voor eigen proces, werkwijze en middelen. Meenemen in Communicatiestrategie en -plan.	MIDDEL
4	Inhoudelijke (keten) afhankelijkheden	Inhoudelijke afhankelijkheden van aanpalende initiatieven (programma Strategisch Informatiebeleid).	Afbakening scope en invulling BIO-maatregelen vanuit programmaboard (waarin ook opdrachtgever STIB).	MIDDEL
5	Voorspelbaarheid kosten	Gedetailleerde uitwerking t.a.v. concrete, situationele maatregelen pas te maken na verdere projectdefinities en besluitvorming, bv over afhankelijkheden.	Vroegtijdige projectdefinitie (detaillering scope, ambitieniveau en -planning inrichten door gedetailleerde GAP-inventarisatie, opgevolgd door besluitvorming door opdrachtgever & programmaboard; Nauwe afstemming over afhankelijkheden en besluiten bedrijfsvoering(strategie).	MIDDEL
6	Inhoudelijke discussie	Informatiebeveiliging en interpretatie van normeringen is en blijft voer voor discussie. Hoewel gedefinieerd bevat ook de BIO zaken die voor interpretatie vatbaar zijn. Dit geldt eveneens voor richtlijnen wat betreft volwassenheid of niveau's. Dit kan leiden tot inhoudelijke discussie over interpretatie en reikwijdte, met mogelijke gevolgen voor o.a. verwachtingen, doorlooptijd en scope.	- Opstellen heldere werkpakketten o.b.v. afgebakende scope/producten; Bewaking door programmamanager en projectleiders; - Structurele afstemming met QC van het programma - Tijdige interventie/escalatie in de vorm van besluitvorming door opdrachtgever en/of programmaboard.	HOOG

7	Aansluiting op bestaande ordeningen proces- en informatie	De mate waarin kan worden aangesloten op binnen de gemeente geldende ordeningen van processen, gegevensverzamelingen, eigenaarschap van informatie en informatiesystemen/applicaties is mede bepalend voor de kwaliteit van de resultaten, en de efficiënte van sommige activiteiten.	In gevallen waar (eenduidigheid in) bestaande ordening ontbreekt, dienen programma en projecten een keuze te maken voor de best passende ordening (bestaand of aan te brengen). Eventuele keuzes over in scope brengen hiervan worden indien nodig voorgelegd aan de programmaboard, inclusief beschrijving impact.	MIDDEL
---	---	---	---	--------

6.3 Kwaliteitsborging (Quality Control)

Invulling van de Quality Control wordt ingevuld door de 2^e en 3^e lijns verantwoordelijkheden binnen de bestaande organisatie (CISO, Concern controller, zie ook de toelichting in §3.2).

In eerste instantie zal de kwaliteitsborging op programmaniveau plaatsvinden vanuit deelname aan de programmaboard, de reguliere programmarapportage en periodieke afstemming met de programmamanager en PMO. Vanuit de scope van de kwaliteitsborging volgt dat de QC zich eveneens richt op de vanuit het programma uitgezette organisatie activiteiten en resultaten. Dit in lijn met de reguliere rol en positie van CISO en CC.

Op projectniveau zal de QC-rol tevens worden ingezet op het gebied van advies en kaderstelling in de kwalitatieve (acceptatie) criteria voor projectproducten. De invulling hiervan wordt in de projectdefinitie fase nader afgestemd tussen programma en QC.

6.4 Stuur en communicatiemiddelen

Als belangrijkste stuur- en communicatiemiddelen voor het programma en de onderliggende projecten gelden dit Programmaplan en de onderliggende projectplannen. Deze zullen gedurende de looptijd van het programma periodiek worden herijkt. Voor het programma is het streven dit jaarlijks te doen, en op zijn minst bij de overgang van Fase 1 naar fase 2. Voor de projectplannen is het streven halfjaarlijks te herijken en bij te stellen waar nodig.

De periodieke voortgangsrapportage wordt maandelijks opgeleverd en gebruikt om tussentijds te sturen op de realisatie van de beoogde doelen en producten, binnen de kaders, planning en toleranties die zijn benoemd in de programma- en projectplannen. De voortgangsrapportage behelst zowel de procesmatige voortgang van de geplande activiteiten als inhoudelijke voortgang als gevolg van de resultaten hiervan. Voor de procesmatige voortgang vormen dit programmaplan (fases, mijlpalen) en de onderliggende projectplannen (deliverable planning) de basis. Voor de inhoudelijke voortgang zal worden aangesloten op twee producten die in de voorbereiding op dit plan zijn opgezet, te weten de BIO-rapportage en het Kwetsbaarhedenlog. Om deze beoogde rol te kunnen vervullen dienen beiden rapportages gedurende de fase projectdefinitie nog wel nader te worden ingevuld. Bijlage 8.1 bevat een illustratie van beide rapportages.

7 Stakeholdermanagement en communicatie

Stakeholdermanagement betreft het proces waarmee alle belanghebbenden bij het programma en de onderliggende projecten betrokken worden en blijven. Van het systematisch identificeren van belanghebbenden; het analyseren van hun behoeften en verwachtingen tot het plannen en uitvoeren van verschillende taken om met hen in contact te komen en te blijven. Gezien de omvang van de organisatie en de relaties met aanpalende programma's ligt het voor de hand deze functie in te vullen vanuit de lijnorganisatie en te combineren binnen de bestaande lijnfunctie die ook de interne communicatie verzorgt.

Het systematisch identificeren van belanghebbenden, analyseren van behoeften en verwachtingen en plannen van communicatie zal in de praktijk een samenwerking zijn tussen de stakeholdermanager, de programmamanager en de projectleiders, waarbij de stakeholdermanager coördinerend optreedt en adviseert.

5B. Tactisch IB-beleid <<kunnen meer beleidstukken bij komen>>			
Omschrijving Opstellen ontbrekende tactische beleidsdocumenten		Eigenaar	
		Prioriteit	Hoog - Midden - Laag
		Inspanning	Hoog - Midden - Laag
Acties	BIO-ref	Verantwoordelijk	Planning
Tactisch beleid <i>Logging</i>	12.4.1		
Tactisch beleid <i>Personeelsbeveiliging</i>	7.1.1 7.1.2 7.2.1 7.2.2	Afhankelijkheid Awareness project	
Validatie tactisch beleid <i>fysieke beveiliging</i>	11.1.1		
Tactisch beleid <i>patchmanagement</i>	12.6.1		
Validatie tactisch beleid <i>logische toegang</i>	9.1.1		
tactisch beleid IB voor leveranciers	15.1.1		
Tactisch beleid <i>gebruik cryptografie</i> (zie WP 18C)	18.1.5		
Precondities en/of afhankelijkheden			
-			

BIO H.6 Organiseren van informatiebeveiliging

6A. Externe relaties			
Omschrijving Er dient een actueel en beheerd overzicht te zijn van externe relaties met wie contact wordt onderhouden t.a.v. informatiebeveiliging		Eigenaar	
		Prioriteit	Hoog - Midden - Laag
		Inspanning	Hoog - Midden - Laag
Acties	BIO-ref	Verantwoordelijk	Planning
Bijwerken overzicht	6.1.3		
Borgen jaarlijkse actualisatie			
Precondities en/of afhankelijkheden			
-			

6B. Informatiebeveiliging in projecten en bij vernieuwingen			
Omschrijving Informatiebeveiliging behoort aan de orde te komen in projectbeheer, ongeacht het soort project. Principes 'by design' zijn reeds onderdeel van PSA's, maar werkwijze is niet vastgelegd		Eigenaar	
		Prioriteit	Hoog - Midden - Laag
		Inspanning	Hoog - Midden - Laag
Acties	BIO-ref	Verantwoordelijk	Planning
Validatie werkwijze PSA's	6.1.5		
Toetsing design principes	14.1.1		
Vastleggen proces borging by design (van projectstart tot PvE tot beheerinrichting en beoordeling bij oplevering)	15.1.1		
Precondities en/of afhankelijkheden			
-			

BIO H.7 Veilig personeel

7A. Beveiligingsbewustzijn			
Omschrijving Naar een hoger niveau tillen van awareness sessies, inclusief toetsmoment, waarbij resultaten worden geborgd in verbeterplannen		Eigenaar	
		Prioriteit	Hoog - Midden - Laag
		Inspanning	Hoog - Midden - Laag
Acties	BIO-ref	Verantwoordelijk	Planning
Het op de hoogte houden van de werknemers van het beleid, en het veilig werken	7.2.2.2 9.3.1 16.1.3 17.1.3.2		
Borgen resultaten in verbeterplan			
Opstellen IB-opleidingsplan (risicogebaseerd)	7.2.2.3		
Precondities en/of afhankelijkheden			
-			

7B. Borging informatiebeveiliging bij uitdiensttreding			
Omschrijving Na uitdiensttreding zijn nog steeds eisen t.a.v. informatiebeveiliging van kracht voor de vertrekkende medewerker. Dit dient onder de aandacht gebracht te worden		Eigenaar	
		Prioriteit	Hoog - Midden - Laag
		Inspanning	Hoog - Midden - Laag
Acties	BIO-ref	Verantwoordelijk	Planning
Borging IB in het exitgesprek	7.3.1		
Precondities en/of afhankelijkheden			
-			
Relatie met BIO 8.1.4 (mogelijk te combineren)			

BIO H.8 Beheer van bedrijfsmiddelen

8A. Inventarisatie en eigenaarschap bedrijfsmiddelen			
Omschrijving Er dient een inventaris te zijn en te worden onderhouden van bedrijfsmiddelen (informatie en informatieverwerkende faciliteiten)		Eigenaar	
		Prioriteit	Hoog - Midden - Laag
		Inspanning	Hoog - Midden - Laag
Acties	BIO-ref	Verantwoordelijk	Planning
Opstellen format inventarisatie	8.1.1		
Vullen format met bekende gegevens			
Uitbreiden proces voor borging aanvulling gegevens met IB-gegevens			
Eigenaren vaststellen	8.1.2		
Eigenaren vastleggen in inventarisatie			
Precondities en/of afhankelijkheden			
-			

8B. Teruggeven van bedrijfsmiddelen			
Omschrijving Er dient een procedure te zijn voor het teruggeven van bedrijfsmiddelen bij beëindiging van het dienstverband		Eigenaar	
		Prioriteit	Hoog - Midden - Laag
		Inspanning	Hoog - Midden - Laag
Acties	BIO-ref	Verantwoordelijk	Planning
Opstellen procedure inname bedrijfsmiddelen (manager verantwoordelijk)	8.1.4		
Bekend stellen procedure			
Borging uitvoering procedure			
Precondities en/of afhankelijkheden - Link naar exitgesprek BIO 7.3.1			

8C. Classificatie van informatie			
Omschrijving Informatie behoort te worden geclassificeerd m.b.t. wettelijke eisen, waarde, belang en gevoeligheid voor onbevoegde bekendmaking of wijziging. Dit vereist het maken van procedures en		Eigenaar	
		Prioriteit	Hoog - Midden - Laag
		Inspanning	Hoog - Midden - Laag
Acties	BIO-ref	Verantwoordelijk	Planning
Classificeren van informatie in de organisatie met betrekking op wettelijke eisen, waarde, belang en gevoeligheid voor onbevoegde bekendmaking of wijziging	8.2.1		
informatie labels behoort een passende reeks procedures te worden ontwikkeld en geïmplementeerd in overeenstemming met het informatieclassificatieschema dat is vastgesteld door de organisatie	8.2.3		
Maken van procedures voor het behandelen van bedrijfsmiddelen en implementeren in overeenstemming met de informatieclassificatie die is vastgesteld	8.2.3		
Verantwoording BBN-niveau VVNR			
maatregelsets aanscherpen en bekendstellen			
Precondities en/of afhankelijkheden -			

8D. Behandelen van media			
Omschrijving Er dient een procedure te zijn voor het handelen van media		Eigenaar	
		Prioriteit	Hoog - Midden - Laag
		Inspanning	Hoog - Midden - Laag
Acties	BIO-ref	Verantwoordelijk	Planning
Opstellen procedure beheer, gebruik, overdragen en verwijderen van media	8.3.1		
	8.3.2		
Bekend stellen procedure	8.3.3		
Borging uitvoering procedure			
Precondities en/of afhankelijkheden -			

BIO H.9 Toegangsbeveiliging

9A. Toegangsverlening			
Omschrijving Toegang tot netwerken en netwerkdiensten: gebruikers dienen hier alleen toegang te krijgen waarvoor ze specifiek bevoegd zijn. En periodieke controle op verantwoordelijkheid, verlening en intrekking van toegang		Eigenaar	
		Prioriteit	Hoog - Midden - Laag
		Inspanning	Hoog - Midden - Laag
Acties	BIO-ref	Verantwoordelijk	Planning
Opstellen procedure	9.1.2		
toegangsverlening en controle	9.2.1		
autorisaties ,uitvoering & beleid	9.2.2		
logische toegang	9.2.3		
Bekend stellen procedure	9.2.5		
Zo nodig aanpassen uitvoering proces	9.2.6		
autorisatie	9.4.1		
Opstellen procedure	9.4.1.2		
toegangsverlening en controle inclusief speciale systeemhulpmiddelen en controle speciale bevoegdheden per kwartaal	9.4.4		
Borging uitvoering procedure			
Onderbouwing autorisatiematrices t.b.v. zichtbare risicoafweging			
functiescheiding			
Borgen lijst van bevoegde aanvragers (gemandateerde managers)			
Precondities en/of afhankelijkheden -			

9B. Authenticatie			
Omschrijving Beheer van geheime authenticatie-informatie van gebruikers dient te worden beheerst via een formeel beheersproces		Eigenaar	
		Prioriteit	Hoog - Midden - Laag
		Inspanning	Hoog - Midden - Laag
Acties	BIO-ref	Verantwoordelijk	Planning
Proces van toewijzing authenticatie-informatie opstellen	9.2.4 9.3.1		
Proces bekend stellen			
Precondities en/of afhankelijkheden			
-			

9C. Wachtwoordvereisten (hoog risico)			
Omschrijving Hoog risico systemen dienen ingericht te zijn conform het beleid logische toegang met betrekking tot het inlogmechanisme		Eigenaar	
		Prioriteit	Hoog - Midden - Laag
		Inspanning	Hoog - Midden - Laag
Acties	BIO-ref	Verantwoordelijk	Planning
Aanscherpen wachtwoordeisen en afdwingen in hoog risico applicaties	9.4.2 9.4.3		
Borging inrichting hoog risico applicaties op eisen t.a.v. inlogmechanisme in beleid logische toegang			
Borging inrichting (hoog risico) op eisen t.a.v. inlogmechanisme in beleid logische toegang			
Precondities en/of afhankelijkheden			
-			

9D. Wachtwoordvereisten (midden en laag risico)			
Omschrijving Midden en laag risico systemen dienen ingericht te zijn conform het beleid logische toegang met betrekking tot het inlogmechanisme		Eigenaar	
		Prioriteit	Hoog - Midden - Laag
		Inspanning	Hoog - Midden - Laag
Acties	BIO-ref	Verantwoordelijk	Planning
Aanscherpen wachtwoordeisen en afdwingen in midden en laag risico applicaties	9.4.2 9.4.3		
Borging inrichting midden en laag risico applicaties op eisen t.a.v. inlogmechanisme in beleid logische toegang			
Borging inrichting (midden en laag risico) op eisen t.a.v. inlogmechanisme in beleid logische toegang			
Precondities en/of afhankelijkheden			
-			

9E. Beperking toegang tot informatie			
Omschrijving Er dienen maatregelen genomen te zijn die het fysiek en/of logisch isoleren van informatie met specifiek belang waarborgen		Eigenaar	
		Prioriteit	Hoog - Midden - Laag
		Inspanning	Hoog - Midden - Laag
Acties	BIO-ref	Verantwoordelijk	Planning
Onderzoek huidige werkwijze dataopslag en toegang) t.b.v. uitwerken werkpakket	9.4.1.1		
Opstellen beleid data-opslag			
Bekend stellen vastgesteld beleid			
Toetsen of autorisatiematrix hierop zijn ingericht			
Zo nodig aanpassen autorisatiematrix en inrichting			
Precondities en/of afhankelijkheden -			

BIO H.10 Cryprografie

10A. Cryptografie			
Omschrijving Een beleid van cryptografische beheersmaatregelen waaronder het sleutel beheer ook valt		Eigenaar	
		Prioriteit	Hoog - Midden - Laag
		Inspanning	Hoog - Midden - Laag
Acties	BIO-ref	Verantwoordelijk	Planning
Opstellen beleid over het gebruik van cryptografie waar aandacht aan de eisen van de BIO worden gegeven	10.1		
Bekend stellen procedure			
Borging uitvoering procedure			
Precondities en/of afhankelijkheden -			

BIO H.11 Fysieke beveiliging van de omgeving

11A. beveiligde gebieden			
Omschrijving Een beleid en uitvoering van de fysieke beveiligen van de werk locaties zoals kantoren, server ruimte, etc.		Eigenaar	
		Prioriteit	Hoog - Midden - Laag
		Inspanning	Hoog - Midden - Laag
Acties	BIO-ref	Verantwoordelijk	Planning
Opstellen beleid over hoe de fysieke toegang is ingesteld tot de locaties van de organisatie	11.1		
Bekend stellen procedure			
Borging uitvoering procedure		Implementatie beleid heeft relatie met evt plannen behuizing (risico desinvestering).	
Precondities en/of afhankelijkheden -			

Er is geen vastgestelde autorisatie matrix op maar op afdelingen & clusters

11B. beveiligde apparatuur (fysiek)

Omschrijving Een beleid en uitvoering van de fysieke beveiligen van de apparatuur van de organisatie		Eigenaar	
		Prioriteit	Hoog - Midden - Laag
		Inspanning	Hoog - Midden - Laag
Acties	BIO-ref	Verantwoordelijk	Planning
Opstellen beleid over hoe de apparatuur fysiek veilig gebruikt moet worden en de regels hierom heen	11.2	Afhankelijkheid project MEBV (Str. IB)	
Bekend stellen procedure		Afhankelijkheid Awareness project	
Borging uitvoering procedure			
Precondities en/of afhankelijkheden			
-			

BIO H.12 beveiliging bedrijfsvoering

12A. bedieningsprocedures en verantwoordelijkheden

Omschrijving Gedocumenteerde procedure over de bedieningsprocedure en onderliggende acties		Eigenaar	
		Prioriteit	Hoog - Midden - Laag
		Inspanning	Hoog - Midden - Laag
Acties	BIO-ref	Verantwoordelijk	Planning
Opstellen van procedures voor het bedieningsprocedure en dit bekend stellen aan gebruikers	12.1.1		
Het uitvoeren van wijzigingsbeheer en capaciteitsbeheer binnen de organisatie	12.1.2 12.1.3		
Borging uitvoering procedure			
Precondities en/of afhankelijkheden			
-			

12B. bescherming tegen malware

Omschrijving Ter bescherming tegen malware behoren beheersmaatregelen voor detectie, preventie en herstel te worden geïmplementeerd, in combinatie met een passend bewustzijn van gebruikers.		Eigenaar	
		Prioriteit	Hoog - Midden - Laag
		Inspanning	Hoog - Midden - Laag
Acties	BIO-ref	Verantwoordelijk	Planning
Gebruikers zijn voorgelicht over de risico's ten aanzien van surfgedrag en het klikken op onbekende linken.	12.2.1.1		
Software en bijbehorende herstelsoftware die malware opspoor zijn geïnstalleerd en worden regelmatig geüpdate.	12.2.1.2		
Computers en media worden als voorzorgsmaatregel routinematig gescand. De uitgevoerde scan behoort te omvatten: (a) alle bestanden die via netwerken of via elke vorm van opslagmedium zijn ontvangen, vóór	12.2.1.3		

gebruik op malware scannen; (b) bijlagen en downloads vóór gebruik.			
De malware scan wordt op verschillende omgevingen uitgevoerd, bijv. op mailservers, desktopcomputers en bij de toegang tot het netwerk van de organisatie.	12.2.1.4		
Gebruikers zijn voorgelicht over de risico's ten aanzien van surfgedrag en het klikken op onbekende linken.	12.2.1.5		
Precondities en/of afhankelijkheden			
-			

12C. back-up			
Omschrijving Beschermen tegen het verlies van gegevens.		Eigenaar	
		Prioriteit	Hoog - Midden - Laag
		Inspanning	Hoog - Midden - Laag
Acties	BIO-ref	Verantwoordelijk	Planning
Er is een back-up beleid waarin de eisen voor het bewaren en beschermen zijn gedefinieerd en vastgesteld.	12.3.1.1		
Op basis van een expliciete risicoafweging is bepaald wat het maximaal toegestane dataverlies is en wat de maximale hersteltijd is na een incident.	12.3.1.2		
In het back-up beleid staan minimaal de volgende eisen: (a) dataverlies bedraagt maximaal 28 uur; (b) hersteltijd in geval van incidenten is maximaal 16 werkuren (2 dagen van 8 uur) in 85% van de gevallen.	12.3.1.3		
Het back-up proces voorziet in opslag van de back-up op een locatie, waarbij een incident op de ene locatie niet kan leiden tot schade op de andere.	12.3.1.4		
De restore procedure wordt minimaal jaarlijks getest of na een grote wijziging om de betrouwbaarheid te waarborgen als ze in noodgevallen uitgevoerd moet worden.	12.3.1.5		
Precondities en/of afhankelijkheden			
-			

12D. Vastlegging en monitoren			
Omschrijving Logbestanden van gebeurtenissen die gebruikersactiviteiten, uitzonderingen en informatiebeveiligingsgebeurtenissen registreren, behoren te worden gemaakt, bewaard en regelmatig te worden beoordeeld.		Eigenaar	
		Prioriteit	Hoog - Midden - Laag
		Inspanning	Hoog - Midden - Laag
Acties	BIO-ref	Verantwoordelijk	Planning
Logregels definiëren welke informatie en systemen	12.4		

SOC / SIEM middels detectie voorzieningen hebben			
Beleid met de regels en te nemen acties voor het rapporteren			
Beschermen van informatie in logbestanden			
Logbestanden van beheerders en operators			
Kloksynchronisatie			
Precondities en/of afhankelijkheden			
-			

BIO H.13 communicatie beveiliging

13A. beheer van netwerkbeveiliging			
Omschrijving De bescherming van informatie in netwerken en de ondersteunende informatie verwerkende faciliteiten waarborgen.		Eigenaar	
		Prioriteit	Hoog - Midden - Laag
		Inspanning	Hoog - Midden - Laag
Acties	BIO-ref	Verantwoordelijk	Planning
Uitvoeren beheers/beveiligingsmaatregelen rondom het netwerk	13.1.1 13.1.2 13.1.3		
Precondities en/of afhankelijkheden			
-			

13b. Informatietransport			
Omschrijving Handhaven van de beveiliging van informatie die wordt uitgewisseld binnen een organisatie en met een externe entiteit.		Eigenaar	
		Prioriteit	Hoog - Midden - Laag
		Inspanning	Hoog - Midden - Laag
Acties	BIO-ref	Verantwoordelijk	Planning
Opstellen beleid en procedures voor informatietransport. En dit in uitvoering krijgen voor overeenkomsten en elektronische berichten	13.1.1 13.1.2 13.1.3	Afhankelijkheid project MEBV (Str. IB)	
Precondities en/of afhankelijkheden			
-			

BIO H.14 Acquisitie, ontwikkeling en onderhoud van informatiesystemen

14A. Beveiligingseisen (zie ook 6B / 6.1.5)			
Omschrijving Bij nieuwe informatiesystemen op bestaande informatiesystemen moeten beveiligingseisen worden vastgesteld op basis van een risicoafweging (zie 6B voor nieuwe informatiesystemen)		Eigenaar	
		Prioriteit	Hoog - Midden - Laag
		Inspanning	Hoog - Midden - Laag
Acties	BIO-ref	Verantwoordelijk	Planning
Beleid risicoanalyse opstellen / aanscherpen	6.1.5 14.1.1		
Procedure risicoanalyse opstellen	14.1.2		

Vastgesteld beleid en procedure bekend stellen	14.1.3		
Borgen stellen van beveiligingseisen openbare netwerken		Relatie met project MEBV (Str. IB)	
Precondities en/of afhankelijkheden			
-			

14B. Wijzigingenbeheer			
Omschrijving Bij wijzigingen op bestaande informatiesystemen moeten beveiligingseisen worden vastgesteld op basis van een risicoafweging.		Eigenaar	
		Prioriteit	Hoog - Midden - Laag
		Inspanning	Hoog - Midden - Laag
Acties	BIO-ref	Verantwoordelijk	Planning
Vastleggen proces wijzigingenbeheer (inclusief beoordelen beveiligingseisen en regie op uitbestede ontwikkeling)	14.1.1 14.1.2 14.2.2		
Zo nodig aanpassen inrichting proces wijzigingenbeheer	14.2.3 14.2.5		
Precondities en/of afhankelijkheden			
-			

BIO H.15 Leveranciersrelaties

15A. Borging informatiebeveiligingsrapportage bij leveranciers			
Omschrijving Met leveranciers behoren de informatiebeveiligingseisen om risico's te verlagen te worden overeengekomen en gedocumenteerd		Eigenaar	
		Prioriteit	Hoog - Midden - Laag
		Inspanning	Hoog - Midden - Laag
Acties	BIO-ref	Verantwoordelijk	Planning
Borging vooraf dat nieuwe leveranciers een beveiligingseisen, risico afwegingen (ook bij offerteaanvragen)	15.1 15.2		
Opnemen beveiligingseisen in leveranciersovereenkomsten			
Beheren van dienstverlening leveranciers (monitoring, beoordelingen)			
Precondities en/of afhankelijkheden			
-			

15B. Verwerkersovereenkomsten			
Omschrijving Met leveranciers (en via hen subleveranciers) behoren verwerkersovereenkomsten gesloten te zijn		Eigenaar	
		Prioriteit	Hoog - Midden - Laag
		Inspanning	Hoog - Midden - Laag
Acties	BIO-ref	Verantwoordelijk	Planning
Borging van afsluiten ontbrekende of te wijzigen verwerkersovereenkomsten	15.1.1.3		
Precondities en/of afhankelijkheden			
-			

BIO H.16 Beheer van informatiebeveiligingsincidenten

16A. Aanscherpen IB-incidentenproces			
Omschrijving Beveiligingsincidenten dienen adequaat gemeld te worden volgens een formeel proces		Eigenaar	
		Prioriteit	Hoog - Midden - Laag
		Inspanning	Hoog - Midden - Laag
Acties	BIO-ref	Verantwoordelijk	Planning
Validatie actualiteit en compliancy incidentenprocedure (o.a. rapportage aan management)	16.1.1 16.1.2 16.1.3		
Borging vaststelling en analyse tijdsduur tussen optreden – constateren – melden- leren	16.1.5 16.1.6 16.1.7		
Precondities en/of afhankelijkheden -			

BIO H.17 Informatiebeveiligingsaspecten van bedrijfscontinuïteitsbeheer

17A. Informatiebeveiligingscontinuïteit			
Omschrijving Een organisatie dient te beschikken over continuïteitswaarborg van informatiebeveiliging in ongunstige situaties		Eigenaar	
		Prioriteit	Hoog - Midden - Laag
		Inspanning	Hoog - Midden - Laag
Acties	BIO-ref	Verantwoordelijk	Planning
Toetsen hernieuwd continuïteitsplan op BIO-compliancy	17.1.1 17.1.2		
Zo nodig aanscherpen continuïteitsplan op BIO-compliancy	17.1.3 17.2.1		
Borging periodieke toetsing continuïteitsplan			
Precondities en/of afhankelijkheden -			

BIO. H18 Naleving

18A. Wet- en regelgeving			
Omschrijving Overzicht relevante wet- en regelgeving en intellectueel eigendom. Borging van de AVG-compliance		Eigenaar	
		Prioriteit	Hoog - Midden - Laag
		Inspanning	Hoog - Midden - Laag
Acties	BIO-ref	Verantwoordelijk	Planning
Borging actueel overzicht relevante wet- en regelgeving, inclusief intellectueel eigendom	18.1.1 18.1.2		
Borging AVG-compliance	18.1.4	Afhankelijkheid Privacy en Strategisch Informatiebeleid	
Precondities en/of afhankelijkheden -			

18B. Bewaartermijnen			
Omschrijving Bewaartermijnen dienen vastgelegd te zijn		Eigenaar	
		Prioriteit	Hoog - Midden - Laag
		Inspanning	Hoog - Midden - Laag
Acties	BIO-ref	Verantwoordelijk	Planning
Controle huidige proces en vastlegging op BIO-compliance	18.1.3		
Zo nodig aanpassen huidig proces en vastlegging			
Precondities en/of afhankelijkheden			
-			

18C. Crypto			
Omschrijving Voorschriften gebruik cryptografische toepassingen		Eigenaar	
		Prioriteit	Hoog - Midden - Laag
		Inspanning	Hoog - Midden - Laag
Acties	BIO-ref	Verantwoordelijk	Planning
Opstellen voorschriften gebruik van cryptografische toepassingen	18.1.5		
Vaststellen en bekend stellen voorschriften			
Precondities beleid Cryptografie			
Precondities en/of afhankelijkheden -			

18D. ISMS			
Omschrijving Het ISMS, informatiebeveiliging als proces volgens het plan-do-check-act principe, dient vastgelegd te zijn, inclusief onafhankelijke beoordeling, auditplan en directiebeoordeling.		Eigenaar	
		Prioriteit	Hoog - Midden - Laag
		Inspanning	Hoog - Midden - Laag
Acties	BIO-ref	Verantwoordelijk	Planning
ISMS-document, audit plan	18.2.1		
Proces voor periodieke rapportage, geënt op directiebeoordeling	18.2.2		
Precondities en/of afhankelijkheden			
-			