



Vernieuwen in samenwerking

Meerjaren Informatieplan Beleidsdepartement
Financiën 2026-2028

Versie 1.0

Datum: 21 november 2025

Colofon

Titel	Meerjaren Informatieplan Beleidsdepartement Financiën 2026-2028
-------	--

Inlichtingen	ConcernDirectie Informatisering en Openbaarmaking, CIO-office
--------------	---

Inhoud

0.	Samenvatting	4
1.	Inleiding	5
1.1	Digitale transformatie	5
1.2	Doel van het Informatieplan	6
2.	Gezamenlijke opgaven	7
2.1	Speerpunt: Betrouwbare (meta)data en toekomstbestendige AI	7
2.2	Speerpunt: Wendbaarheid IT-vernieuwing	8
2.3	Speerpunt: Risicomanagement	9
3.	Aandachtspunten Basis op orde	11
3.1	Voldoen aan wet- en regelgeving	11
3.2	Ondersteunende processen	12

0. Samenvatting

Informatievoorziening is een snel ontwikkelend beleidsterrein. Ook het Beleidsdepartement krijgt hiermee te maken. De roep om transparantie van informatie, het inspelen op nieuwe technologieën, de toenemende behoefte aan soevereiniteit van datagebruik en -opslag en de modernisering op het gebied van applicaties en technologische infrastructuur, maken dat de digitaliseringsopgaven omvangrijk zijn. Maatgevend in de digitale transformatie is de samenwerking met het primaire proces en het gezamenlijk stellen van prioriteiten.

In de articulatie van doelstellingen voor beleid en uitvoering is de rol van Informatievoorziening steeds dominanter. Het doel van dit Meerjarig informatieplan (MIP) is om vast te leggen wat de prioritaire doelstellingen zijn voor de informatievoorziening van het Beleidsdepartement. Er is met een vertegenwoordiging van de DG'n en het SG-cluster geïnventariseerd welke ontwikkelingen actueel zijn en de komende periode gaan worden en welke acties daarbij nodig zijn. Er zijn drie thema's bepaald die de komende jaren prioriteit hebben. Hierbij is gekeken naar de recent gepubliceerde Nederlandse Digitaliseringsstrategie¹ (NDS) en het departementale Meerjarig Informatieplan Financiën 2026-2028 (dMIP).

- Betrouwbare (meta) Data en toekomstbestendige AI.

Hier wordt gestreefd dat Dataverzameling, AI en archivering verder ingebed worden in processen binnen het Beleidsdepartement. Governance, compliance en ethiek worden geborgd in de voortbrenging, terwijl de uitvoering optimaal wordt ondersteund. De insteek is een steeds hoger volwassenheidsniveau van de voortbrenging, als basis voor verantwoorde besluitvorming en vernieuwing

- Wendbaarheid IT-vernieuwing.

De context van het beleidsdepartement maakt dat "de winkel nooit dicht kan". Continuïteit moet worden geborgd, terwijl vernieuwing van systemen plaatsvindt. Door te werken als "één organisatie" en in te zetten op collectieve oplossingen, uniforme standaarden, interoperabiliteit en bundeling van inkoopkracht, wordt de schaalbaarheid en weerbaarheid vergroot. Een goed geïmplementeerde sourcingstrategie kan hier een bijdrage aan leveren.

- Risicomanagement.

Vanuit Europa komt er veel nieuwe wetgeving op ons af. Denk aan de AI-Act en de NIS2. Veel van deze wetgeving heeft een risicogerichte insteek. Risicomanagement wordt meer ingebed in de processen. De schaarse capaciteit wordt ingezet waar de risico's het grootste zijn (zoals Te Beschermen Belangen, kritieke omgevingen of processen). Door risico-denken structureel onderdeel te maken van beleid, uitvoering en monitoring, worden risico's beheerst en kan er ook strategisch voordeel behaald worden. Het helpt de organisatie om adequaat te anticiperen op veranderingen, verstoringen te beperken en strategische doelen te blijven realiseren, ook in een dynamische context. Goed risicomanagement fungeert daarmee als hefboom voor duurzame besluitvorming en vergroot de slagkracht en weerbaarheid van de organisatie.

Deze thema's zullen worden uitgewerkt in roadmaps voor het Beleidsdepartement waarvan de monitoring van de voortgang in het IV-overleg Beleidsdepartement zal gaan plaatsvinden.

Daarnaast blijft veel aandacht uitgaan naar het op orde brengen en houden van de basis. De kapstok hiervoor is het te versterken IV-voortbrengingsproces waarin de basis verder versterkt op het gebied van Informatiebeveiliging, Privacy, Architectuur, Informatiehuishouding, Innovatie, Bedrijfs Continuïteits Management, Kwaliteitsmanagement en Portfoliomanagement. Ook wordt gewerkt aan het op orde brengen van de bronadministraties op basis waarvan rapportages meer geautomatiseerd gemaakt kunnen worden.

¹ Kamerstuk 26643nrK, Brief van de staatssecretaris van BZK ter aanbieding van de Nederlandse Digitaliseringsstrategie, 04-07-2025

1. Inleiding

1.1 Digitale transformatie

In de huidige geopolitieke situatie spelen wereldwijde spanningen, zoals veranderingen in handelsrelaties, energiezekerheid, en digitale dreigingen, een steeds prominenter rol. Daarnaast bevindt de digitalisering zich in een stroomversnelling en komend dagelijks nieuwe technologische ontwikkelingen beschikbaar. Dat roept de vraag op wat er wanneer kan, mag en wenselijk is en hoe de veiligheid voor onze medewerkers en stakeholders blijvend kan worden geborgd.

Op dit moment zijn er veel ontwikkelingen die het IV-vakgebied beïnvloeden. Digitalisering en innovatie, zoals de opkomst van artificial intelligence, blockchain, quantum computing, cryptovaluta en Central Bank Digital Currencies (CBDC), veranderen de manier waarop financiële markten wordt geopereerd vragen om aangepaste kaders, advisering en monitoring. Voor het Beleidsdepartement liggen speerpunten in het waarborgen van de stabiliteit en transparantie van de financiële sector, het moderniseren van wet- en regelgeving rondom digitale financiële producten en het stimuleren van duurzame financiering. Ook het versterken van cyberweerbaarheid in samenwerking met toezichthouders en marktpartijen is essentieel om de integriteit van financiële systemen te beschermen. Daarnaast zal het ministerie moeten blijven inzetten op internationale samenwerking in het kader van financiële regelgeving, om mondiale uitdagingen zoals belastingontwijking, witwassen en klimaatfinanciering effectief aan te pakken. In de komende jaren zal het departement een leidende rol moeten spelen in het vormgeven van een veerkrachtige, eerlijke en toekomstbestendige financiële sector in Nederland en Europa.

Dit vraagt om een adaptieve en veerkrachtige informatievoorziening die beleidsmakers ondersteunt in hun werkzaamheden voor een financieel gezond Nederland. Digitalisering speelt hierin een cruciale rol en zal worden ingezet om verdere efficiëntieslagen te maken in de werkzaamheden binnen het ministerie, bijvoorbeeld de beleidsvorming, financiële processen en het vergroten van de weerbaarheid. Het vermogen om snel op veranderingen in te spelen, vereist een toekomstbestendige IV-infrastructuur en een sterke focus op digitale veiligheidsmaatregelen vanuit een risicogerichte insteek, terwijl tegelijkertijd sprake moet zijn van een duurzaam ingerichte informatiehuishouding, transparantie en verantwoord datagebruik, om het maatschappelijk vertrouwen in het ministerie te borgen.

De recent uitgebrachte NDS vormt het kader voor het dMIP. In de NDS worden zes principes beschreven: Cloud, Data, AI, Burgers en ondernemers centraal, Versterken digitale weerbaarheid en autonomie van de overheid en Digitaal vakmanschap. Het dMIP geeft op hoofdlijnen aan hoe deze principes binnen processen van de Belastingdienst, Toeslagen, Douane en het beleidsdepartement worden vormgegeven, rekening houdend met de NDS. Er zijn binnen het dMIP vijf gemeenschappelijke uitdagingen geformuleerd waarop in de komende jaren een extra impuls of investering nodig is:

- Het verbeteren van de dienstverlening,
- Modernisering van het IT-landschap,
- Talent aantrekken en vasthouden,
- Voldoen aan wet- en regelgeving
- Het informatielandlandschap op orde.

Deze documenten zijn input voor het informatieplan van het Beleidsdepartement.

1.2 Doel van het Informatieplan

Jaarlijks wordt het MIP geactualiseerd in samenspraak met de DG'n van het Beleidsdepartement en het SG-cluster en betrokken dienstverleners. Hierbij worden jaarlijks speerpunten aangebracht. Het bundelt de prioritaire I-doelstellingen vanuit alle I- invalshoeken: ICT inclusief Life Cycle Management (LCM), Informatiehuishouding, Privacy, Informatiebeveiliging, Data en AI, IV-voortbrenging, Bedrijfs Continuïteit Management (BCM). Tot slot biedt het handvatten voor uitwerking, prioritering en monitoring van activiteiten.

2 Gezamenlijke opgaven

Het vertrekpunt voor verandering wordt enerzijds bepaald door de wettelijke en maatschappelijke taken van het beleidsdepartement en anderzijds door de steeds veranderende technologische mogelijkheden. De vertaling naar de behoefte aan IV en ondersteuning daarvan worden vastgelegd in doelstellingen van het beleidsdepartement: haar DG'n: Generale Thesaurie, Rijksbegroting, Fiscale Zaken, Herstel en het SG-cluster. Daarmee zijn de DG'n van Financiën maatgevend voor de IV-behoefte.

De vernieuwingen binnen het Beleidsdepartement komen vanuit decentrale behoeften tot stand. Daarnaast is er een centrale behoefte aan inzicht, verantwoording en transparantie. Gestroomlijnde processen helpen met het verhogen van de efficiëntie aan beide zijden. Een volgende stap in volwassenheid is om de samenhang tussen de verschillende dienstonderdelen te versterken, onder andere via het IV-overleg, de portfolioboard en de architectuurboard van het beleidsdepartement. De inrichting van Quality Assurance draagt bij aan het inzicht in en kwaliteit van de verschillende trajecten. Door in een vroegtijdig stadium te onderkennen wat de strategische uitdagingen zijn bij beleidsvorming en -uitvoering (en de mogelijke impact op de informatievoorziening en – technologie) kan meer integraal afgewogen worden welke inzet qua technologie, budget, capaciteit en competenties nodig is. Dit komt de voorspelbaarheid en de efficiëntie van IV-vernieuwing en innovatie ten goede.

Centraal in de informatievoorziening staat de voortbrenging. Dit proces loopt van visie en strategie naar behoeftestelling tot en met life cycle management en archivering. De voortbrenging (denk aan portfoliomanagement, architectuur, DPIA, Informatiehuishouding, cloudstrategie) wordt de komende jaren steeds verder uitgewerkt en beschreven. Daarmee wordt de basis verder op orde gebracht en compliantie in het ontwerp verwerkt.

Om bovenstaande ontwikkelingen en opgaven goed te kunnen borgen is het belangrijk om de informatievoorziening in gezamenlijkheid met de DG'n en de directies van het SG-cluster vorm te geven. Daarom wordt ingezet op een stabiele basis en daarnaast op drie speerpunten.

2.1 Speerpunt: Betrouwbare (meta)data en toekomstbestendige AI

Er ontstaan steeds meer mogelijkheden en behoeften om te werken met grote hoeveelheden data en nieuwe technologie. Veel van de processen om te komen tot de inzet van data of toepassingen van nieuwe technologie worden ad hoc uitgevoerd en volgen de kaders van de voortbrenging nog niet. Hierdoor is er minder grip op de kwaliteit van deze processen en is er niet altijd voldoende inzicht in de daaruit voortvloeiende risico's.

Dit leidt tot onvoldoende overzicht, dubbele datasets en tot inefficiënt gebruik van middelen. Datakwaliteit, data architectuur en het consequent toepassen van metadata moet steeds meer centraal staan voor een betere vindbaarheid en duurzame toegankelijkheid van onze informatie, alsmede voor het kunnen realiseren van betrouwbare rapportages.

Ook om AI duurzaam, verantwoord en effectief in te zetten, is het van essentieel belang om de basis op orde te brengen, zodat er aantoonbaar wordt gewerkt met de juiste kwaliteit van gegevens en een gedegen risicobeheer. Dit versterkt onze besluitvorming en de impact van ons beleid. In het licht van een duurzame informatiehuishouding, transparantie en openbaarmaking wordt Archiving by design ingericht. Een robuuste data architectuur vormt de ruggengraat voor datagedreven

werken. Dit helpt versnippering voorkomen en zorgt ervoor dat data betrouwbaar, toegankelijk en herbruikbaar is.

Ambitie:

Bouwen aan een datastelsel. Dit datastelsel moet gebaseerd zijn op drie pijlers: (meta)datakwaliteit, governance en ethiek. Om dit waar te maken wordt ingezet op de volgende vijf doelen:

1. Groeien naar een hoger volwassenheidsniveau door een structurele aanpak voor data- en AI-processen zodat deze integraal onderdeel van onze beleidsvorming en -uitvoering worden. Hierbij wordt een metadatacatalogus en datagovernancestructuur ingericht, afgestemd op bestaande IV-beheerprocessen, zodat de technische infrastructuur en de beleidsdata goed op elkaar aansluiten.
2. (Verder) verankeren van archivering by design als leidend principe bij architectuurkeuzes en bij het aanschaffen of ontwikkelen van nieuwe informatiesystemen. Hierdoor wordt vroegtijdig aandacht besteed aan informatiehuishouding, wordt archivering structureel geïntegreerd in onze processen en daarmee de digitale duurzaamheid van onze informatie en data en daarmee compliance versterkt met archiefwetgeving.
3. Inrichten van een metadatacatalogus om het Beleidsdepartement in staat te stellen om data vindbaar, toegankelijk en herbruikbaar te maken, en voorkomt onnodige duplicatie of verlies van data.
4. Inrichten van een eenduidige bronadministratie waarbij een "Single Source of Truth" wordt gedefinieerd. Door de bronadministratie te koppelen aan de metadatacatalogus ontstaan beter inzicht in waar data zich bevindt, onder welke voorwaarden deze wordt beheerd en hoe deze technisch is geborgd. De bronadministratie borgt het beheer van infrastructuur en applicaties, de metadatacatalogus en datagovernance processen borgen de kwaliteit, vindbaarheid en herleidbaarheid van data.
5. Vastleggen van dataprincipes en standaarden om vertrouwen en interoperabiliteit te creëren door heldere definities, kwaliteitseisen en afspraken over datagebruik.
6. Borgen van AI-compliance als onderdeel van de voortbrenging. Dit omvat risico-classificatie, algoritme-audits en het registreren van algoritmes in een algoritmeregister, zodat voldoen wordt aan de AI Act en andere relevante regelgeving.
7. Inzet op AI-geletterdheid en ethiek door het verzorgen van opleidingen, workshops en het oprichten van een directie overstijgend AI-kernteam onder leiding van een AI-regisseur, voor de borging van communicatie en beleid.

Toekomstperspectief:

Data, AI en archivering zijn meer structureel onderdeel van de processen binnen het Beleidsdepartement en voldoen aantoonbaar aan de randvoorwaarden op de gebieden data, AI, privacy, archivering en informatiebeveiliging. Governance, compliance en ethiek zijn centraal geborgd om de primaire processen optimaal te ondersteunen. Zo wordt gebouwd aan een steeds hoger volwassenheidsniveau, dat een stevige basis biedt voor verantwoorde besluitvorming en vernieuwing.

2.2 Speerpunt: Wendbaarheid IT-vernieuwing

In een tijdperk van snelle technologische ontwikkelingen en schaarse capaciteit en middelen is het belangrijk om zowel reguliere IT-behoefte als vernieuwingskansen in balans te brengen. Dit betekent niet alleen ruimte creëren voor innovatie op gebieden als machine learning, AI, cloudtoepassingen en quantum computing, maar ook aandacht besteden aan de dagelijkse continuïteit en het verbeteren van bestaande processen.

Het stimuleren van uniformiteit, interoperabiliteit, gebruik van standaarden en gebruik maken van (out)sourcing zijn hierbij ondersteunend. Daarbij worden op dit

moment keuzes gemaakt op verschillende niveaus. De aansluiting tussen de portfolioprioritering en – management binnen DG'n en de daarvoor benodigde algemene middelen van de portfolioboard moet worden verbeterd.

Ambitie:

De gezamenlijke realisatie van toekomstbestendige IT-oplossingen door:

- Een sourcingstrategie te implementeren die strategische en technische behoeften ondersteunt, waarbij de inzet van schaarse capaciteit en resources wordt geoptimaliseerd.
- De organisatie ruimte te geven om aan de slag te gaan met innovatieve experimenten, die snel kunnen worden uitgevoerd. Dit kan door het innovatieproces beter uit te werken en onder te brengen in de voortbrenging en daarnaast door het opleveren van een meerjarige innovatieplanning met budget. Of door het bieden van technische ondersteuning in de vorm van sandboxes en ontwikkelplatforms.
- Inzicht te bieden in de effectiviteit van middelen en capaciteiten, waarbij technologie, processen en mensen centraal staan.
- Regie te voeren op samenwerking binnen de verschillende IV-disciplines (bijvoorbeeld door bundeling van inkoopkracht en gebruik van collectieve oplossingen en bouwstenen) en het hanteren van het voortbrengingsproces.
- Ons lerend vermogen te verbeteren en daarmee bestaande structuren zoals het IT-voortbrengingsproces en het portfolio-overleg effectiever inzetten.

Toekomstperspectief:

Wendbaarheid vraagt om een goede balans tussen het ondersteunen van dagelijkse processen ("going concern") en het benutten van technologische kansen en een efficiënte inzet van de beschikbare mensen en middelen. Door duidelijke kaders en processen te bieden, worden innovatieve oplossingen sneller beschikbaar voor alle onderdelen van de organisatie. Door te werken als "één organisatie" en waar mogelijk in te zetten op collectieve oplossingen, uniforme standaarden en bundeling van inkoopkracht, wordt onze strategische autonomie, schaalbaarheid en weerbaarheid versterkt. Dit zorgt ervoor dat de organisatie niet alleen voorbereid is op de toekomst, maar zich ook continu aan kan passen aan veranderingen in een steeds complexere digitale omgeving.

2.3 Speerpunt: Risicomanagement

De snelheid waarmee technologische innovaties en nieuwe wet- en regelgeving elkaar opvolgen, stelt hoge eisen aan de wendbaarheid en flexibiliteit van onze organisatie. Het veranderende dreigingsbeeld vraagt investering in onze de weerbaarheid en versterkte inzet op digitale risico-en bedrijfsvoering continuïteit management (BCM) en Informatiebeveiliging. Veel nieuwe wet- en regelgeving kent een risico-gebaseerde insteek. Dit vraagt om een risico-gebaseerde sturing en het mitigeren van risico's met behulp van uniforme werkwijzen, ondersteunt door Quality Assurance (QA). Door onzekerheden vroegtijdig te signaleren en de bijbehorende kansen en bedreigingen in kaart te brengen, ontstaat er ruimte voor snellere en beter onderbouwde besluiten en passende beheersmaatregelen. IT-risico's (bijvoorbeeld cybersecurityrisico's, inbreuk op privacy, incidenten met IT-infrastructuur, etc.) dienen integraal deel uit te maken van de risicoanalyses en het interne beheersingssysteem van het Beleidsdepartement. Tegelijk biedt IT kansen en mogelijkheden om risico's met geautomatiseerde beheersmaatregelen te beheersen. Dit vraagt ook om het maken van bewuste keuzes: risico's kunnen niet volledig worden uitgesloten, maar moeten binnen acceptabele grenzen beheerst worden — balanceren betekent hier expliciete risico-acceptatie waar nodig. Risicomanagement dient in de volle breedte van het Beleidsdepartement te worden ingebed.

Ambitie:

Risicomanagement wordt praktisch ingebed in alle processen en is een managementverantwoordelijkheid en maakt deel uit van onze cultuur. Het is een vanzelfsprekend onderdeel van regulier werk, ondersteund door duidelijke kaders, passende tooling en continue verbetering. Het wordt ingebed door:

1) Basis verder op orde brengen:

- Heldere en toegankelijke kaders & IV-governance zoals Informatiebeheer en Informatiehuishouding, Informatiebeveiliging, Business Continuity Management, Privacy, Data, algoritme & Artificial Intelligence gebruik.
- Versterken en inrichten van een centraal portfoliomanagementproces binnen de voortbrenging.
- Het verder centraliseren inzicht in het projectenportfolio van het Beleidsdepartement en waar mogelijk het centraliseren van -budgetten voor de realisatie van portfolioprojecten.
- Verder inrichten rollen en verantwoordelijkheden zoals proceseigenaarschap, applicatie/systeem-eigenaarschap en data-eigenaarschap.

2) Fundament aanbrengen voor risicomanagement:

- Kaders opstellen en implementeren van risicomanagement, inclusief een Plan, Do, Check, Act-cyclus ten behoeve van risicogebaseerde sturing en 1e en 2e lijnsverantwoordelijkheid. Zo mogelijk wordt aangesloten op het Key Control Dashboard (KCD);
- Betere verankering en prioritering van IV-risico's en - beheersmaatregelen waarbij rapportages vanuit gedefinieerde bronsystemen worden gegenereerd.
- Betere samenwerking en een integrale risicomanagementaanpak op het IV-vakgebied met FEZ;
- Versterken risico-bewuste cultuur: trainingen risico-bewustzijn in bestaande leertrajecten, awareness sessies, onboarding en onaangekondigde phishing simulaties of cyberoefeningen.
- Monitoren van de risicomaatregelen door de inrichting van Quality assurance management.

Toekomstperspectief:

Door risico-denken integraal onderdeel te maken van beleid, uitvoering en evaluatie, ontstaat een organisatie die risico's niet alleen beheerst, maar er ook strategisch voordeel uit weet te halen. Het helpt de organisatie om adequaat te anticiperen op veranderingen, verstoringen te beperken en strategische doelen te blijven realiseren, ook in een dynamische context. Goed risicomanagement fungeert daarmee als hefboom voor duurzame besluitvorming en vergroot de slagkracht van de organisatie.

3. Aandachtspunten basis op orde

Het is een uitdaging voor het Beleidsdepartement om het informatiebeheer, lees het datafundament en de informatiehuishouding, wendbaar te houden, het IT-landschap te moderniseren en risico's beheersbaar te houden. De mate waarin zij deze ambities weet te realiseren wordt voor een belangrijk deel bepaald door de mate waarin mens, proces en technologie congruent samenvallen. Essentieel is dat de organisatie voldoende gefaciliteerd wordt om de digitale transformatie te kunnen vormgeven.

Om te zorgen dat medewerkers sterke schakels zijn in het beheersen van risico's, is in 2025 gestart met het meerjarig programma: 'Digitaal Vakmanschap'. In dit programma ligt de focus op langdurige gedragsverandering op het gebied van veilig en effectief werken met (vertrouwelijke) informatie en nieuwe technologieën. Onderdeel van dit programma is de e-learning digitaal vakmanschap. Alle relevante onderwerpen binnen het I-domein komen aan bod, van informatiebeveiliging tot privacy en van informatiehuishouding tot generatieve AI. Alle bestaande en nieuwe medewerkers zijn verplicht om de e-learning te doorlopen. Naast het programma 'Digitaal Vakmanschap' voert CDIO de regie over een integraal plan voor informatiebewustzijn dat de komende jaren moet zorgen voor gestructureerde, doelgerichte communicatie over verantwoord omgaan met gegevens.

Processen definiëren hoe er wordt gewerkt. Het IV-voortbrengingsproces speelt een cruciale rol in het realiseren van kwalitatieve, veilige en betrouwbare digitale oplossingen en dienstverlening. Dit proces is het kader voor de ontwikkeling, implementatie en levering van IV-oplossingen, met inachtneming van organisatiedoelen, wettelijke vereisten en normen en standaarden. Technologie maakt het mogelijk. De digitale infrastructuur is op onderdelen verouderd en zijn systemen complex in opzet. Het Beleidsdepartement kiest ervoor de digitale infrastructuur in beheersbare stappen wendbaar en toekomstbestendig te maken en continue betrouwbaar en veilig te houden.

3.1 Voldoen aan wet- en regelgeving

- Informatiebeveiliging (IB)

Cybercrime, verstoringen en digitale spionage zijn grote bedreigingen voor de digitale veiligheid van Financiën. Geopolitieke ontwikkelingen hebben daarop evidente invloed. De opkomst van quantumcomputing brengt ingrijpende veranderingen en dreigingen met zich mee binnen het domein van informatiebeveiliging, waardoor klassieke cryptografische algoritmes serieus onder druk komen te staan. In lijn met zowel de Europese richtlijnen als de aanbevelingen van het Programma Quantumveilige Cryptografie NL en het PQC-Migratiehandboek (2024) van de AIVD, TNO en CWI1, is het nodig de dreiging van quantumcomputers voor de huidige cryptografie te mitigeren door migratie van huidige kritische cryptografie en moet worden toegewerkt worden naar crypto-wendbaarheid (crypto-agility).

De ambitie van Financiën is een gestructureerde informatiebeveiliging (IB) volgens het Cyberbeveiligingswet (CbW) (de Baseline Informatiebeveiliging Overheid (BIO2) en NIS2 zijn onderdeel van het Cbw). Er wordt gestreefd steeds een hoger volwassenheidsniveau te bereiken. Daartoe is er een IB Roadmap met als thema's: de focus op feitelijke en operationele beveiliging (1), zorgen voor een volwassen organisatorische context waardoor securitymaatregelen duurzaam geborgd kunnen worden (2) en de medewerkers helpen zich aan te passen aan de snel veranderende (cyber)omstandigheden (3). Als ondersteuning maakt Financiën gebruik van solide cyber security technologie en houdt hierbij actief in de gaten welke (technische) ontwikkelingen er rijksbreed en in de markt gaande zijn op dit gebied (4). Onderdeel van de roadmap vormt de periodieke herijking van de thema's aan en verwerking, vastlegging en implementatie van de nieuwe beleidskaders zoals NIS2. Ingezet wordt

op het verder professionaliseren van de diensten van het Security Operations Center (SOC), de samenwerking met het SOC binnen het ministerie van Financiën en het in control brengen van Identity & Access Management (IAM).

- Privacy

Privacy is een onderwerp wat vaak aandacht vraagt in het politieke en maatschappelijke debat. Toch is het verwerken van gegevens over medewerkers en personen ook onontkoombaar voor het goed uitvoeren van de taken van het

ministerie van Financiën. Essentieel is daarom dat we weloverwogen besluiten nemen over het gebruik van gegevens over personen, en dat we aan kunnen tonen dat de juiste belangenafweging is gedaan en risico mitigerende maatregelen zijn genomen.

Om dit te faciliteren is een departementaal privacy beleid opgesteld met een governance structuur daarnaast zijn voor het beleidsdepartement overlegstructuren en werkprocessen ingericht met als insteek het zo gemakkelijk mogelijk te maken voor de organisatie om te voldoen aan de verplichtingen uit de privacywetgeving, en hen hierin optimaal te begeleiden.

- Bedrijfs Continuity Management (BCM)

Bedrijfscontinuïteitsmanagement richt zich op het identificeren van dreigingen en kwetsbaarheden om het Beleidsdepartement voor te bereiden op mogelijke verstoringen van haar kritische bedrijfsprocessen. In de huidige tijd is BCM belangrijker dan ooit. Gezien de kritische processen en maatschappelijke belangen van ons ministerie, de toename van (nieuwe) dreigingen en technologische ontwikkelingen is het blijven toetsen, testen en verbeteren van de (digitale) weerbaarheid essentieel. Om de volwassenheid van de organisatie te vergroten wordt ingezet op het creëren van organisatie breed bewustzijn en wordt BCM verankerd in de relevante processen van het Beleidsdepartement. Daarnaast wordt ingezet op het oprichten van een BCM-systeem, het opstellen van Opleiden, Trainen Oefenen (OTO)-plan en het actualiseren van alle BCM-plannen van het Beleidsdepartement in het kader van de militaire weerbaarheid.

- Informatiehuishouding (IHH)

De samenleving, de politiek en ambtenaren verwachten dat overheidsinformatie vindbaar, betrouwbaar en duurzaam toegankelijk is. Dit vraagt om het structureel (en compliant met de Archiefwet en Woo) op orde brengen van de IHH van het beleidsdepartement van Financiën, een ontwikkeling die reeds in gang gezet is (en onder andere invulling krijgt door de '(Beleids)dossiers op Orde-trajecten en meer aandacht voor bewustwording) en ook de komende jaren nog een aanzienlijke inspanning zal vragen.

Daarnaast is er een transitie gaande naar een meer integrale IHH op basis van digitale processen en informatie, waarbinnen ook consequent gebruik van (meta)data en de toepassing by design-principes bijdragen aan duurzame toegankelijkheid van onze informatie. Deze transitie is urgent vanuit compliantie met de Archiefwet en raakt onder andere (werk)processen, bewustwording en de inzet van nieuwe technologieën en worden geborgd in voortbrengingsproces. Tot slot bereidt het beleidsdepartement zich voor op de implementatie van de nieuwe Archiefwet, welke verscherpte eisen voor digitaal archiefbeheer en een verkorte overbrengingstermijn met zich meebrengt.

3.2 Ondersteunende processen

- Portfoliomanagement

Voor het beleidsdepartement vormt het Rijksbrede kwaliteitshandboek Portfoliomanagement de basis om het portfolioproces in te richten als onderdeel van de voortbrenging. In dit proces zorgen beleidsdirecties ervoor dat de projectinitiatieven tijdig worden aangemeld. Dit geeft zicht op het benodigde budget en inzet van capaciteit en de daaruit af te leiden behoefte aan IV en ondersteunende IT. Na aanmelding volgt uitwerking en realisatie van het idee naar dienstverlening. Borging vindt onder meer plaats via instrumenten als de Project Start Architectuur, DPIA, cloudtoets en quickscans IB. Indien noodzakelijk wordt

het portfolio periodiek bijgesteld. Bijvoorbeeld om ruimte te maken voor nieuwe initiatieven of om vanuit schaarse middelen te herverdelen. In komende jaren wordt dit proces sterk verbeterd: decentrale registers worden aangesloten op het centrale portfolioproces ten behoeve van inzicht en overzicht conform gelijke definities en voorwaarden. Dat betekent uiteindelijk dat alle (majeure) IT-activiteiten van het Beleidsdepartement integraal geprioriteerd kunnen worden en worden opgenomen in de PDCA-cyclus.

- Life Cycle Management (LCM)

Om te komen tot een wendbare IV-ondersteuning is het wezenlijk van belang dat onderhoud van het IT-landschap up to date is en blijft. De producten en diensten binnen het productportfolio bestaan uit meerdere componenten (applicaties en infrastructuur), elk met verschillende levenscycli. Ter voorkoming van veroudering van het IT-landschap is binnen het departement een ontwikkelpad Lifecycle Management opgesteld. Hierin wordt de samenhang tussen lifecycle management, enterprise architectuur en portfoliomanagement aangegeven. Het accent zal komen te liggen op preventief en toestand-gerelateerd onderhoud. Hierdoor kunnen tijdig keuzes gemaakt worden inzake investeringen en aanbestedingen en voorkomt het verrassingen en langdurige vernieuwingsprojecten met risico's in de continuïteit. Lifecycle Management wordt de komende periode geïntensiveerd in nauwe samenwerking met DG'n. Zo wordt van alle applicaties gezien of ze up to date zijn en zonodig vinden upgrades danwel vervangingen plaats. Daarna zal de infrastructuur en technologie worden geanalyseerd en deze zomogelijk gemoderniseerd. De komende jaren zal er fasegewijs aandacht nodig blijven voor LCM en zal het uiteindelijk een on-going activiteit zijn middels regulier onderhoud.

- Architectuur

Binnen het beleidsdepartement wordt onder architectuur gewerkt. Het doel van architectuur is het realiseren van strategische doelstellingen van het beleidsdepartement door richting te geven aan de ontwikkeling van het IV-landschap en de samenhang tussen de onderdelen daarbinnen te borgen. In de architectuur speelt de architectuurbibliotheek een belangrijke rol. Deze biedt een centrale plek waar architectuurmodellen gestructureerd en in samenhang worden vastgelegd. De ambitie vanuit architectuur is om de komende tijd de informatie in de architectuurbibliotheek verder te verrijken en te ontsluiten, waardoor deze waardevolle informatie breed beschikbaar komt als onderdeel van de bronadministratie. Daarnaast worden stappen gezet om vanuit architectuur een bijdrage te leveren aan een meerjarig projecten- en innovatieportfolio

- Innovatie

Het technologielandschap waar de (financiële) wereld mee te maken heeft, en mee te maken zal krijgen, verandert snel, ook door versmelting van technologieën. Zaken als cloud, API's en Business Intelligence tooling hebben hun intrede gedaan. Verder investeren in data-analytics, predictive analytics, Robotic Process Automation, Artificial Intelligence/machine learning en process mining zijn van belang voor Financiën om haar rol in het financiële ecosysteem te kunnen blijven spelen.

- Werkomgeving

Een moderne werkomgeving ter ondersteuning van (inter-) departementaal samenwerken en optimale ondersteuning van de informatiehuishouding is onmisbaar. Hiervoor participeert het ministerie in het programma Beter Samenwerken (BSW) wat tot doel heeft de ontwikkeling van een nieuwe digitale werkomgeving volgens het principe van Archive by Design, als opvolger van het huidige Document Management Systeem (DMS). Tegelijkertijd wordt er volop hybride gewerkt en dat moet veilig en betrouwbaar en zo veel mogelijk op maat gemaakt kunnen worden door medewerkers (self-service). Om dit goed te ondersteunen wordt nauw samengewerkt met SSC-ICT die de werkplekdiensten leveren, optimaliseren en veilig houden. Ook wordt gewerkt aan Digitale Werkplek Rijk (DWR) 2.0. Ook de projecten in het licht van Programma Meerjarenplan Openbaarheid en Informatiehuishouding (PMOI) dienen hierin geïntegreerd te

worden, denk aan Archive by Design en Single Source of Truth. Tot slot wordt om inzet van SaaS-applicaties, webapplicaties en cloudbased applicaties gevraagd. En dat heeft effect op het IT-landschap, de samenwerking met externe leveranciers, de informatiebeveiliging, exit strategieën privacy en afspraken rondom hooggekwalificeerde data en systemen.