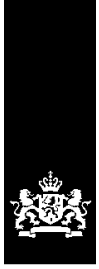


Ministerie van Financiën

iBB

Integrale Beveiligingsbeleid Belastingdienst

Inhoudsopgave

0.1 Voorwoord

De Belastingdienst draagt als onderdeel van het Ministerie van Financiën bij aan een financieel gezond Nederland, door eerlijk en zorgvuldig belasting te heffen en te innen en toeslagen uit te keren. Daarnaast draagt de Belastingdienst bij aan een financieel gezonde, concurrerende en veilige Europese Unie.
Burgers en bedrijven moeten op de overheid – en dus op de Belastingdienst – kunnen vertrouwen. Burgers zijn in veel opzichten afhankelijk van de overheid. Bovendien kunnen overheidsbesluiten diep ingrijpen in het leven van burgers. Daarom moet de overheid integer zijn. Dit komt tot uiting in de drie basiswaarden van de organisatie: geloofwaardig, verantwoordelijk en zorgvuldig.
Integrale beveiliging vult de basiswaarden in door te voldoen aan vigerende wet- en regelgeving en draagt direct bij aan de reputatie van de organisatie (en daarmee de reputatie van de Rijksoverheid) en zodoende ook aan het compliant gedrag van belastingplichtigen.
De sturing en organisatie van integrale beveiliging tot en met de implementatie van maatregelen zijn hiermee van essentieel belang voor de Belastingdienst.

Onder integrale beveiliging verstaan we: het selecteren, implementeren en periodiek evalueren van een samenhangend stelsel van beveiligingsmaatregelen van de organisatie, medewerkers, materieel, informatiesystemen, gebouwen en overige objecten op basis van risicomanagement[1].

In de brede context van onze maatschappelijke functie kijken we naar onze omgeving, politiek, bestuurlijk en technologisch, maar ook naar onszelf, bijvoorbeeld naar bewustwording, integriteit of digitale vaardigheid. Proportioneel, logisch en in samenhang. We gaan verder dan simpelweg risico's accepteren. We weten wat dat betekent voor ons en onze omgeving en onze keuzes zijn transparant, gedragen en uit te leggen. We laten zien wat we doen en kunnen uitleggen waarom. De maatschappij verwacht een adequate verantwoording van ons en zo werken we ook met elkaar.

We sluiten aan op rijksbrede kaders en hanteren een generiek beveiligingsniveau. Op basis van risicomanagement wordt beoordeeld of dit afdoende is, worden eventuele restrisico’s geaccepteerd of worden aanvullende maatregelen getroffen.

0.2 Leeswijzer

Dit beleidsdocument is de opvolger en vervanger van het Handboek Beveiliging Belastingdienst 2017 (HBB). Waar onderdelen uit het HBB 2017 nog niet zijn opgenomen of vervangen in dit document geldt het HBB vooralsnog als *good practice*. Het wordt in een aantal iteraties op onderdelen vervolmaakt en uitgebreid.

Voor 2019 geldt dit nog als beleidsdocument voor de Belastingdienst, vanaf 2020 wordt voorzien dat we samen met het Kerndepartement komen tot een Integrale Beveiligingsbeleid Financiën.

De bijlagen maken een integraal onderdeel uit van dit document. De bijlagen I en II vormen vooralsnog een fysiek apart document. De hoofdstukken 4 t/m 8 zijn onderwerp van het separate Plan van Aanpak Integrale Beveiliging en worden daarin uitgewerkt.

Dit beleidsdocument is bedoeld voor alle lijnmanagers en medewerkers in de organisatie, in- en externe dienstverleners zowel als het Kerndepartement, toezichthouders en andere departementen waarmee wij een functionele relatie hebben.

De inhoudelijke structuur van het document is ontleend aan de NEN-ISO High Level Structure (HLS). De HLS biedt eenzelfde structuur, met dezelfde kerneisen, aan normen die worden gesteld aan managementsystemen. Managementsystemen helpen te voldoen

[1] Conform het Beveiligingsvoorschrift Rijksdienst 2013 (BVR).

aan essentiële randvoorwaarden voor leiderschap, een goede inrichting van de organisatie en bedrijfsprocessen en competente en goed gemotiveerde medewerkers. Voor integrale beveiliging hanteren we daarom ook een integraal managementsysteem. In paragraaf 3.4 staat dit verder uitgewerkt.

Om het document leesbaar te houden en aan te laten sluiten bij de doelgroepen, volgen we niet de exacte hoofdstuknummering die door de HLS is voorgeschreven maar maken we een volgorde op inhoud.

iBB hoofdstuk	**Oorspronkelijk HLS hoofdstuk**
1 Onderwerp en toepassingsgebied	1
2 Leiderschap	5
3 Context van de organisatie	4
4 Planning	6
5 Ondersteuning	7
6 Uitvoering	8
7 Evaluatie van de prestaties	9
8 Verbetering	10
Bijlage IV Normatieve verwijzingen	2
Bijlage V Termen en definities	3

1 Onderwerp en toepassingsgebied

Integrale beveiliging beslaat een breed terrein en betreft organisatie, medewerkers, integriteit, materieel, informatiesystemen, gebouwen, calamiteitenmanagement, omgevingsvariabelen en overige objecten. Hierop is permanent kaderstellend beleid en toezicht nodig om het hoofd te kunnen bieden aan dreigingen als gevolg van opzettelijk en onopzettelijk menselijk handelen. Bestaande en nieuwe kwetsbaarheden hebben permanent invloed op het beleid en toezicht.

De reikwijdte van integrale beveiliging en de bijbehorende managementsystemen is de gehele bedrijfsvoering van de Belastingdienst, de materiële- en immateriële eigendommen, medewerkers, en alle personen die zich op locaties van de Belastingdienst bevinden. Daarbij vallen eveneens onder de reikwijdte activiteiten die zijn inbesteed of uitbesteed aan externe leveranciers, alsmede eigendommen van derden die ons ter beschikking staan.

Bij integrale beveiliging heeft iedere directie in concern-, pDG-staf en bedrijfsonderdeel een eigen rol binnen het eigen werkterrein, waarbij de Chief Security Officer Belastingdienst (CSO) de centrale regie voert op de integrale beveiliging namens de (p)DG.
De CSO wordt hierbij functioneel aangestuurd door de Beveiligingsambtenaar (BVA) van het Kerndepartement, conform het Beveiligingsvoorschrift Rijksdienst 2013 (BVR). De CSO is in BVR-termen de Beveiligingscoördinator, die evenals de BVA is aangewezen door de SG.

De verantwoordelijkheidsgebieden van integrale beveiliging zijn:
- *Bedrijfscontinuïteit*: het omgaan met risico's die de ongestoorde bedrijfsvoering van de Belastingdienst bedreigen;
- *Personele veiligheid en integriteit*: de veiligheid voor medewerkers en bezoekers en de invulling van de begrippen "goed ambtenaarschap" en "goed werkgeverschap" op het gebied van beveiliging - integriteit is een gezamenlijke verantwoordelijkheid van het individu en van de organisatie;
- *Fysieke beveiliging*: de veiligheid van gebouwen en terreinen;
- *Informatiebeveiliging*: de beschikbaarheid, vertrouwelijkheid en integriteit van alle vormen van informatie en verwerking daarvan (zowel handmatig als geautomatiseerd).

Privacybescherming, de beveiliging van de verwerking van persoonsgegevens, is een integraal onderdeel van deze beveiligingsaspecten.

Noot: Op het moment van schrijven bestaan er nuanceverschillen in de scope van de verantwoordelijkheidsgebieden bij het Kerndepartement en de Belastingdienst. Zo omvat Business Continuity Management (BCM) bij de Belastingdienst calamiteitenmanagement in de vorm van crisismanagement. Bij het Kerndepartement wordt in eerste instantie uitgegaan van calamiteitenmanagement. (Personele) integriteit is bij de Belastingdienst verbonden met personele veiligheid, vanuit O&P perspectief. Het Kerndepartement kent een meer holistische benadering van integriteit. Deze verschillen zullen worden vereffend op weg naar een gemeenschappelijk beleid voor het gehele Ministerie van Financiën.

2 Leiderschap

2.1 Leiderschap en betrokkenheid

De operationalisering en implementatie van het beleid voor integrale beveiliging sluit aan op de strategie van de Belastingdienst. Alle aspecten van integrale beveiliging worden expliciet meegewogen bij koerswijzigingen en (grote) veranderingen zoals bijvoorbeeld ICT-trajecten. Dit wordt geborgd door de CSO op het niveau van het Directieteam Belastingdienst. Integrale beveiliging is verankerd op het hoogste bestuurlijke niveau in de CSO. De CSO agendeert minimaal twee keer per jaar het thema integrale beveiliging in het Directieteam Belastingdienst.
Daarnaast is integrale beveiliging zoveel mogelijk onderdeel van het reguliere (primaire) proces. Dat wil zeggen dat het niet apart georganiseerd zou moeten worden maar regulier onderdeel is van het (bedrijfsvoerings)beleid en de uitvoering.
De eisen vanuit integrale beveiliging worden via de managementsystemen geïntegreerd in de bedrijfsprocessen door de verantwoordelijke directie.

De middelen voor:
- het volgen van beveiligingsvoorschriften of het treffen van beveiligingsmaatregelen wordt gedragen door het uitvoerend organisatieonderdeel en wordt zichtbaar gemaakt in het jaarcontract;
- het inrichten en onderhouden van het managementsysteem wordt gedragen door de hiervoor aangewezen directie;
- het opvangen van de impact van nieuwe beveiligingseisen die met terugwerkende kracht moeten worden toegepast, worden op voorspraak van de CSO geprioriteerd in het Directieteam Belastingdienst. Hetzelfde geldt voor majeure wijzigingen in beveiligingsvoorzieningen.

De CSO en de managementsysteemverantwoordelijken zorgen er voor dat:
- Het belang en de betekenis van de managementsystemen gecommuniceerd is;
- Gestuurd wordt op compliance met de eisen van het managementsysteem en daarmee voldoen aan de onderliggende wet- en regelgeving;
- Vakinhoudelijke aanwijzingen worden gegeven ter bevordering van de eenheid van handelen, normering en waardering ten aanzien van de beveiliging in de organisatie in het verlengde van de functionele sturing op integrale beveiliging door de departementale Beveiligingsambtenaar (BVA);
- Alle directies bekend zijn met de na te leven beveiligingsvoorschriften;
- Van alle beveiligingsmaatregelen bekend is welke directie(s) deze leveren;
- Elke medewerker zich bewust is van de mogelijkheid om een bijdrage te leveren aan beveiliging door input te leveren aan het relevante managementsysteem;
- Dit document en de managementsystemen tijdig worden geactualiseerd ten gevolge van nieuwe risico’s, veranderingen in wet- en regelgeving of uitvoeringspraktijk.

2.2 Beleid

Het rijksbeleid wordt gevolgd, waarbij een sterke verbinding met het Kerndepartement bestaat. Het beleid voor integrale beveiliging volgt uit de vigerende wet- en regelgeving, rijksoverheidskaders, voor wat betreft informatiebeveiliging (eventueel) aanvullend het IB-beleid van het Ministerie van Financiën conform de “lemniscaat Rijk”.
De CSO is verantwoordelijk voor dit beleidsdocument, de bijlagen en de onderliggende managementsystemen. Deze worden vastgesteld in het Directieteam Belastingdienst. De onderhoudscyclus is minimaal 1 x per jaar. Bij het onderhoud worden veranderingen in wet- en regelgeving meegenomen. De impact hiervan wordt in opdracht van de CSO door een uitvoeringstoets bepaald. Publicatie is op het Belastingdienst Intranet.
Het besturingsmodel voor integrale beveiliging sluit aan bij de besturingsuitgangspunten binnen de topstructuur. De volgende functiescheiding voor integrale beveiliging komt hier uit voort.

Integrale beveiliging
De CSO is verantwoordelijk voor de integrale beveiligingsvisie en –strategie en de verbinding daarin tussen de verschillende beveiligingsaspecten. De CSO (laat) het concernbrede beveiligingsbeleid ontwikkelen en borgt de implementatie daarvan. Concreet zijn dat dit beleidsdocument, afgeleide documenten, het dreigingenbeeld en de beveiligingsarchitectuur van de Belastingdienst.
In dat kader zorgt hij in nauwe samenwerking met de BVA van het Kerndepartement voor de samenhang en relatie met het departementale en rijksbrede beveiligingsbeleid en de -kaders en bijbehorende beleidscycli. De CSO zoekt beleidsmatig de samenwerking en afstemming met onder andere de CIO, CDO en directeuren van respectievelijk C&F, CD O&P en SSO FD.
De CIO en CDO hebben een kaderstellende taak rondom IV en databeheersing; informatiebeveiliging vormt hier een onderdeel van. Beleidsvorming rondom de personele aspecten vindt plaats bij de concerndirectie O&P. Beleidsvoorbereiding over de fysieke aspecten gebeurt bij SSO FD.

Bedrijfscontinuïteit, Business Continuity Management (BCM)
BCM is een samenhangend geheel aan activiteiten dat erop is gericht de continuïteit van de organisatie te waarborgen, de reputatie te beschermen en de veiligheid van medewerkers en bezoekers te borgen. Crisismanagement is een onderdeel van BCM.
Het doel van BCM is het vergroten van de veerkracht waardoor de Belastingdienst te allen tijde, maar in het bijzonder tijdens calamiteiten en crises, een ongestoorde, betrouwbare dienstverlening naar burgers en bedrijven kan handhaven.

Fysieke beveiliging
De verantwoordelijkheid voor gebouwen en gebouwgebonden voorzieningen ligt bij het Rijksvastgoedbedrijf (RVB) als verhuurder/eigenaar rijkshuisvesting en opdrachtgever naar marktpartijen voor de bouwkundige en elektronische beveiligingsmaatregelen. SSO CFD, als concerndienstverlener (CDV), zorgt gezamenlijk met het RVB voor de fysieke beveiliging van de rijkskantoren waarbij de CDV de opdrachtgever is voor de organisatorische beveiliging van Rijkskantoren.
Het BZK/Directoraat-generaal Overheidsorganisatie houdt als systeemverantwoordelijke voor integrale beveiliging toezicht op het totale systeem van de Bedrijfsvoering Rijk, waaronder de fysieke beveiliging. Vanuit die hoedanigheid stelt hij kaders op, waaronder het Normenkader Beveiliging Rijkskantoren (NkBR), dat wordt vastgesteld op interdepartementaal niveau.

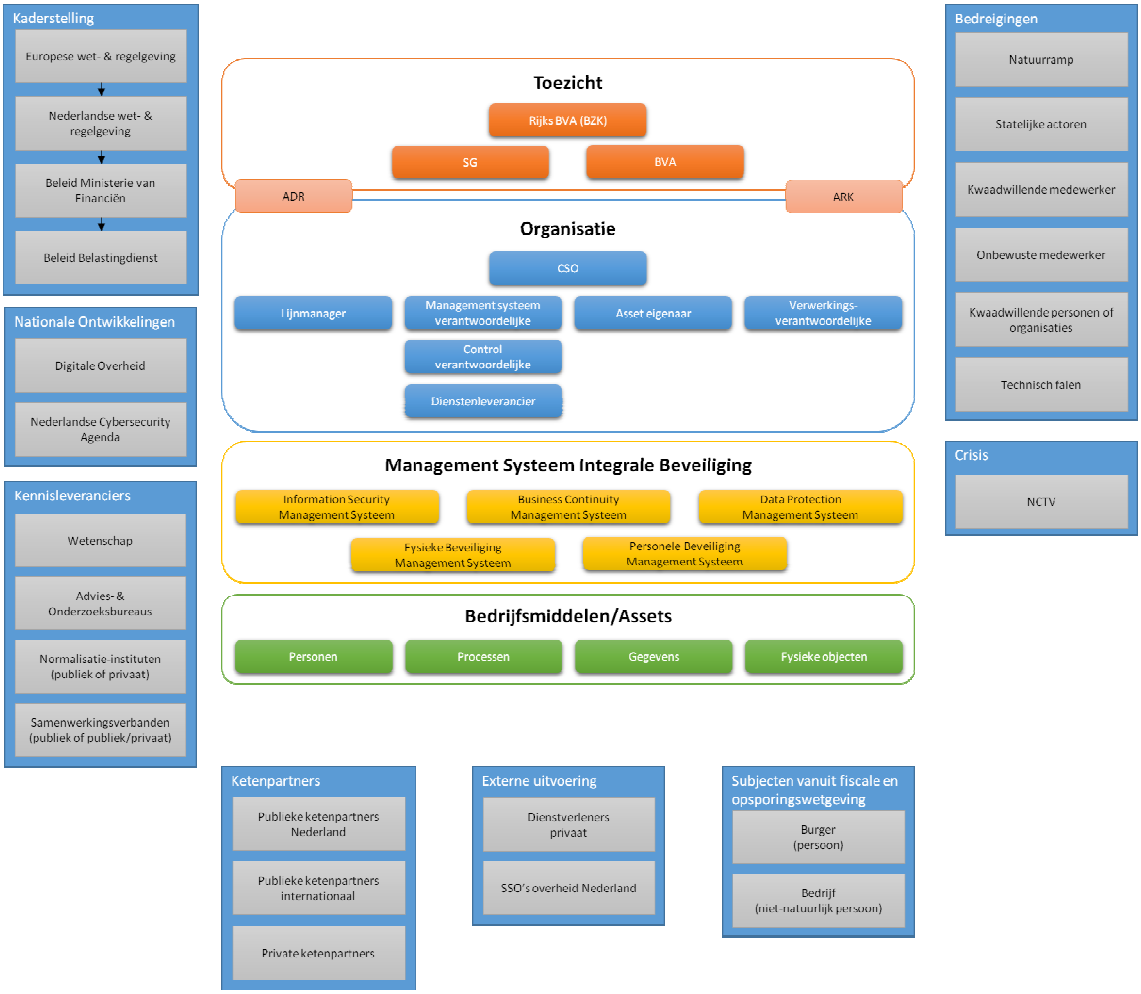
Informatiebeveiliging
Het beleid voor informatiebeveiliging volgt uit de vigerende wet- en regelgeving, rijksoverheidskaders en het IB-beleid van het Ministerie van Financiën. Eventueel expliciet te noemen belastingdienstspecifiek beleid wordt opgenomen in de volgende versie.

Personele veiligheid en integriteit
Naast de generieke wet- en regelgeving, volgt eventueel expliciet te noemen belastingdienstspecifiek beleid in de volgende versie.

3 Context van de organisatie

3.1 De organisatie en haar context

Een nadere uitwerking van deze paragraaf komt in de volgende versie.



3.2 Behoeften en verwachtingen van belanghebbenden

Een nadere uitwerking van deze paragraaf komt in de volgende versie.

3.2.1 Relevante wet- en regelgeving

Voor de managementsystemen is hieronder aangegeven welke wet- en regelgeving met name meegenomen moet worden. Onderstaande opgave is niet limitatief, dat wil zeggen mag c.q. moet door de verantwoordelijke worden aangevuld. Ook hoeft niet alle wetgeving van toepassing te zijn voor een directie (explain).
Mogelijk is in specifieke gevallen aanvullende wet- en regelgeving van toepassing. Deze wordt dan door de verantwoordelijk directeur geïntegreerd in het relevante management systeem en opgenomen in het jaarcontract en bijbehorende rapportage.

- Beveiligingsvoorschrift 2013 (BVR 2013), Stcrt. 2013, 15496
- Algemene Verordening Gegevensbescherming (AVG)
- BIO v1.0, d.w.z. ISO 27002 plus Rijksmaatregelen als invulling van de ISO 27001

- Voorschrift Informatiebeveiliging Rijksdienst (VIR2007), Stcrt. 2007, 122/11
- Voorschrift Informatiebeveiliging Rijksdienst - Bijzondere Informatie (VIRBI 2013)
- Wet structuur uitvoeringsorganisatie werk en inkomen (Wet SUWI)
- Wet basisregistratie personen (Wet BRP)
- Wet veiligheidsonderzoeken (WVO)
- Wet Politiegegevens
- Wet op de Inlichtingen en Veiligheidsdiensten
- Archiefwet
- NkBR (Normenkader Beveiliging Rijkskantoren) 2015
- Rijkstoegangsbeleid (ICBR)
- Algemene Rijksvoorwaarden bij IT-overeenkomsten (ARBIT 2016)
- Gedragsregeling voor de digitale werkomgeving (1 juli 2016; SGO besluit)
- 'Pas toe of leg uit'-lijst van het Forum Standaardisatie
- Programma van Eisen PKI Overheid
- AdES baseline profile standard
- Telecommunication Infrastructure Standard for Data Centers (TIA-942)
- Algemeen Rijksambtenarenreglement (ARAR)
- Gedragscode Integriteit Rijk
- PUB (Personele Uitvoeringsbepalingen Belastingdienst)

3.2.2 Principes voor integrale beveiliging

a) We maken beveiligingskeuzes op basis van risicomanagement.
Beleid(suitgangspunten):
- We hanteren een baselinebenadering tegen vastgestelde dreigingen[2];
- Prioritering bij het toekennen van middelen voor beveiliging vindt plaats op basis van classificatie en risico's.

b) We beschermen geclassificeerde bedrijfsmiddelen.
Beleid(suitgangspunten):
- De veiligheid van medewerkers, bezoekers en leveranciers binnen de eigen gebouwen en terreinen staat voorop.
- Toegang en autorisatie wordt verleend op basis van *need-to-know*, *need-to-do* en het principe van *least privilege*[3].
- Handelingen zijn onweerlegbaar herleidbaar tot de verantwoordelijkheid van een natuurlijk persoon.

c) We ontwikkelen veilige processen, administraties en fysieke objecten.
Beleid(suitgangspunten):
- Vanaf de ontwerpfase worden beveiligingseisen en maatregelen bepaald en geïmplementeerd.
- Bij wijzigingen in processen, administraties en fysieke objecten wordt de beveiliging opnieuw getoetst en waar nodig aangepast.
- We kunnen op elk moment tijdens de levenscyclus van (informatie)voorzieningen verantwoording afleggen over de wijze waarop de beveiliging is ingericht.

d) We verbeteren continu onze beveiliging.
Beleid:
- De effectiviteit van de beveiligingsmaatregelen wordt periodiek verantwoord en geëvalueerd.

[2] Zie ook paragraaf 3.2.3.3, Dreigingsprofiel.
[3] Least privilege: Alleen de autorisaties die iemand nodig heeft om zijn taak te kunnen vervullen, zullen worden toegekend (sic), conform VIRBI 2013.

3.2.3 Beleidsuitgangspunten

Strategisch en tactisch beleid voor integrale beveiliging is vastgesteld in rijksbrede kaders en wetgeving.

3.2.3.1 Classificatie en waardering van bedrijfsmiddelen

Elk bedrijfsmiddel heeft een verantwoordelijke (directeur van een organisatieonderdeel). De waarde van een bedrijfsmiddel wordt uitgedrukt in termen van Beschikbaarheid, Integriteit en Vertrouwelijkheid (BIV) op de niveaus laag-midden-hoog. Deze kwalitatieve waardebeoordeling komt in de plaats van de kwantitatieve (financiële) waarde die in andere sectoren gangbaar is en sluit aan op het classificatieschema dat gehanteerd wordt in de BIO. De regel is dat de hoogst toegekende waarde leidend is (geen middeling). Reputatie is voor de Belastingdienst een bedrijfsmiddel.

Er zijn meerdere stakeholders die gezamenlijk de waarde van een bedrijfsmiddel bepalen:

- Het Rijk: Te Beschermen Belangen (TBB), waaronder kritische bedrijfsprocessen;
- De Burger: Privacybelang;
- De Staat: Cruciaal Belang;
- Ministerie van Justitie en Veiligheid: Strafrechtelijk Belang;
- Daarnaast kan er nog sprake zijn van andere belangen, zoals het archiefbelang of een bedrijfsvoeringsbelang van de Belastingdienst zelf.

3.2.3.2 Risicomanagement

De Belastingdienst gaat uit van *aanvaardbaar risico* waarbij risico's geduid worden op basis van een gestandaardiseerde impact- en kansklasse. Er wordt aangesloten op het concernbrede proces voor risicomanagement, dat belegd is bij de concerndirectie C&F. Vanuit de context van integrale beveiliging gaat het om risico's die op operationeel niveau ontstaan maar op concernniveau impact (kunnen) hebben. Met het managementsysteem voor integrale beveiliging is de Belastingdienst in staat om risico's te identificeren, analyseren en mitigeren, op basis van bewuste keuzes en risicoacceptatie.

Periodiek wordt door alle directies een risicoanalyse[4] uitgevoerd op de integrale beveiligingsaspecten. Er zijn twee typen risicoanalyses:

Vanuit de bedrijfsmiddelverantwoordelijkheid:

- Up to date bedrijfsmiddelenlijst en bijbehorende classificatie: zijn er zaken bijgekomen of veranderd;
- Op basis van de rapportages uit de management systemen beoordelen of de bedrijfsmiddelen voldoende beschermd zijn (ook tegen calamiteiten). Mocht een rapportage ontbreken, kan er geen zekerheid gegeven worden of de bedrijfsmiddelen voldoende beschermd zijn, en moeten zo nodig aanvullende maatregelen genomen worden.

Vanuit de controlverantwoordelijkheid:

- Het stelsel van maatregelen dat invulling geeft aan een control moet blijvend sluitend zijn;
- Controls en maatregelen sluiten aan op het actuele dreigingsprofiel.

Ten einde een integraal beeld te krijgen uit de risicoanalyses, is onderlinge afstemming tussen de risicoverantwoordelijken noodzakelijk.
Om een sluitend stelsel van de organisatiebrede en departementale planning- en control cycli te doen ontstaan, rapporteert de CSO hierover functioneel aan zijn (p)DG en de concern- en pDG staf. De CSO informeert de BVA hierover.

[4] In de Referentiearchitectuur Integrale Beveiliging is bij de kaders voor architecten een handleiding opgenomen voor het maken van een risicoanalyse.

3.2.3.3 Dreigingsprofiel

De voor de Rijksoverheid geïdentificeerde dreigingen gelden ook voor de Belastingdienst, evenals het Cybersecuritybeeld Nederland van JenV/NCSC. Eventuele aanvullende specifieke dreigingen worden jaarlijks vastgesteld door de CSO. De Belastingdienst gaat uit van het volgende dreigingsprofiel:

- Personen (derden en eigen medewerkers, al dan niet opzettelijk), die verantwoordelijk zijn voor fouten, datalekken, diefstal, fraude, staking, sabotage, omkoping, afluisteren, verbale of fysieke agressie;
- Technisch falen, veroorzaakt door bijvoorbeeld brand, water- en weersoverlast, virussen, apparatuur- en softwarestoringen;
- Criminele organisaties, beroepscriminelen en buitenlandse actoren/inlichtingen.

Specifieke aandacht wordt besteed aan digitale spionage, digitale identiteitsfraude, verstoring van online dienstverlening en datalekken zoals (al dan niet bewuste) publicatie van vertrouwelijke informatie.
De omgang met extreme bedreigingen zoals gewapende conflicten, daden van terreur, atoomkernreacties en aardbevingen valt in het gebied van crisismanagement en bedrijfscontinuïteit.
De processen van de Belastingdienst worden niet gerekend tot de vitale infrastructuur van Nederland[5].

3.2.3.4 Generiek beveiligingsniveau

De Belastingdienst hanteert een generiek beveiligingsniveau dat voor informatiebeveiliging overeenkomt met BBN2 van de BIO (BIV is gelijk aan midden-midden-midden[6] voor gegevens én processen). Dit niveau is gericht op de beveiliging van verwerking van persoons- en financieel economische gegevens (departementaal vertrouwelijk volgens het VIRBI), inclusief het aspect privacy. De maatregelen voor fysieke beveiliging en voor personele veiligheid en integriteit sluiten hierop aan, dat wil zeggen, ondersteunen het generieke beveiligingsniveau.
Dit betekent dat alle bedrijfsmiddelen beschermd worden op het niveau van BBN2, ook als er minder bescherming nodig is. Een uitzondering hierop kan alleen gemaakt worden indien de verwerking buiten de Belastingdienst plaatsvindt, en door middel van een risicoanalyse is aangetoond dat een lager beveiligingsniveau aanvaardbaar is.

Aanvullende maatregelen bovenop het generieke worden genomen op basis van een risicoanalyse. Een risicoanalyse is verplicht in de volgende gevallen:

- BIV hoger dan midden-midden-midden voor gegeven of proces;
- Dreiging komt niet voor in het dreigingsprofiel;
- Bekende onvolkomenheden in de implementatie van het generieke beveiligingsniveau.

De verantwoordelijkheid voor risicoanalyse, mitigatie en acceptatie ligt bij de directie die het risico draagt. Van interne en externe leveranciers (dienstverleners) wordt geëist dat actief op beveiligingsrisico's wordt gestuurd en worden gerapporteerd aan de risicodragende directie.

3.2.3.5 Gegevens en processen met een verhoogde classificatie

Voor bedrijfsmiddelen die op een hoger niveau geclassificeerd zijn dan het generiek beveiligingsniveau, moeten in de regel aanvullende beschermingsmaatregelen genomen worden. Welke bedrijfsmiddelen hiervoor in aanmerking komen, wordt bepaald door de bedrijfsmiddelverantwoordelijke.
Informatie wordt overeenkomstig het niveau departementaal vertrouwelijk volgens het VIRBI beschermd. Er wordt in de regel geen bijzondere informatie gegenereerd op het niveau van staatsgeheim-confidentieel of hoger, met uitzondering van bepaalde informatie bij de FIOD. Met betrekking tot die gegevens worden op basis van ketenafspraken met andere inspectiediensten afzonderlijke maatregelen getroffen ter

[5] Weerbare vitale infrastructuur, JenV/NCTV, december 2017.
[6] Beschikbaarheid, Integriteit (data), Vertrouwelijkheid wordt uitgedrukt in niveaus laag-midden-hoog.

voldoening aan het VIRBI.
Voor de bepaling van de rubricering gebruiken we de richtlijnen van de Rijksoverheid. Voor zover de Belastingdienst verder bijzondere informatie op het niveau van staatsgeheim-confidentieel of hoger onder zich heeft, bestaat deze uit als zodanig geclassificeerde bijzondere informatie, welke is aangeleverd door andere (handhavings)partners en is het VIRBI van toepassing.

Bijzondere groepen personen en bedrijven
Bij de Belastingdienst zijn bijzondere groepen personen of bedrijven aan te wijzen, die op het aspect vertrouwelijkheid niet voldoende hebben aan het generieke beveiligingsniveau. Tevens kan uit een risicoanalyse naar voren komen dat dat ook voor hier niet benoemde groepen geldt. Voor deze groepen moeten aanvullende maatregelen getroffen worden. In de praktijk worden er meestal extra maatregelen genomen om de gegevens logisch en soms fysiek af te schermen. Het is van belang de maatregelen zo veel mogelijk organisatiebreed en uniform uit te werken. Bekende groepen zijn:

- *Very important persons* (Vips);
- Ambtenaren;
- Beursgenoteerde ondernemingen;
- Gegevens die onder Wet Politie Gegevens vallen.
- Sleutels, certificaten, tokens en wachtwoorden

Vips zijn personen met specifieke te beschermen functies (Koninklijk Huis, bewindspersonen etc.). Deze classificatie wordt gebruikt om de toegang tot (fiscale) gegevens van bepaalde personen aan een beperkt aantal daartoe aangewezen functionarissen toe te wijzen. Aanwijzing gebeurt door CD FJZ, hiervoor is geen aparte risicoanalyse nodig.

Kritische bedrijfsprocessen
Kritische bedrijfsprocessen zijn benoemd op basis van de aan de Belastingdienst opgedragen wettelijke uitvoeringstaken, maar ook bijvoorbeeld op basis van impact en risico's op reputatieschade, maatschappelijke onrust of politieke invloed uit binnen- of buitenland:

- Alle uitbetalingsprocessen naar burgers en bedrijven;
- Communicatiemiddelen naar burgers, bedrijven en eigen personeel;
- De stopfunctie van Douane;
- Fysiek toezicht Douane;
- Vervoer Douane;
- Toeslagen.

Voor elk bedrijfsproces van de Belastingdienst is vastgesteld wat de maximaal toelaatbare uitvalsduur (MTU) en het maximaal (toelaatbare) data verlies (MDV) is. Op basis hiervan moet bepaald zijn welke activiteiten als kritisch aangemerkt worden.

3.2.3.6 Vertrouwensfuncties

De Wet veiligheidsonderzoeken bepaalt dat functies die de mogelijkheid bieden de nationale veiligheid te schaden, door de verantwoordelijke minister worden aangewezen als vertrouwensfuncties. Deze vakminister is verantwoordelijk voor het juist doorlopen van het afwegingsproces en wijst met een besluit[7] vertrouwensfuncties aan.
Een vertrouwensfunctie wordt als zodanig aangewezen als er sprake is van tenminste één van de volgende vier criteria.

- Op basis van wetgeving is de functie aangewezen;
- De functie geeft structureel toegang tot kwetsbare en/of staatsgeheime informatie en/of kernbelangen die bij compromittering schade aan de nationale veiligheid veroorzaken (informatie);
- De functie geeft directe, ongecontroleerde toegang tot mogelijke doelwitten of middelen die een aanslag of spionage faciliteren, waarbij in alle gevallen schade aan de nationale veiligheid ontstaat (toegang);

[7] Conform de Algemene wet bestuursrecht.

- De functie is een sleutelpositie in een organisatie die de democratische rechtsorde bewaakt en is daarmee een nationale voorbeeldfunctie (boegbeeld).

Voor de aanwijzing van vertrouwensfuncties wordt de leidraad van BZK/AIVD gehanteerd. Het management van een bedrijfsonderdeel geeft binnen de kaders van de leidraad aan of en zo ja welke functies er binnen het eigen bedrijfsonderdeel als vertrouwensfuncties dienen te worden aangewezen. Het niveau (screening) van de vertrouwensfunctie volgt uit de leidraad.

3.2.3.7 Kritische en risicovolle functies

Kritische en risicovolle functies zijn functies die invloed kunnen hebben op de bedrijfscontinuïteit of de integriteit van de Belastingdienst. We definiëren deze als volgt:

- Kritische functies zijn functies waarbij de voortgang van een kritisch bedrijfsproces ernstig in gevaar komt bij uitval van medewerkers;
- Risicovolle (of kwetsbare) functies zijn functies die risico's op integriteitsinbreuken met zich mee brengen, door bijvoorbeeld het werken met gevoelige informatie, het kunnen beschikken over geld en de omgang met zakelijke relaties.

Elk bedrijfsonderdeel van de Belastingdienst kan geconfronteerd worden met integriteitsinbreuken en/of stagnatie van de bedrijfscontinuïteit. Deze kunnen voortkomen uit het in onvoldoende mate nemen van maatregelen tegen de risico's die zich voor kunnen doen bij het uitoefenen van kritische, risicovolle en/of vertrouwensfuncties.
De kritische en risicovolle functies, de risico's daarvan en de maatregelen die zijn getroffen worden daarom door de leidinggevende in kaart gebracht, geregistreerd en door het management vastgesteld.
Het vaststellen van deze functies door het management helpt de organisatie zicht te houden op de risico's die worden gelopen en vergroot het bewustzijn en het draagvlak voor de te nemen maatregelen.

3.3 Het toepassingsgebied van de managementsystemen

De reikwijdte van de managementsystemen uit paragraaf 3.4 is de gehele organisatie en bedrijfsvoering van de Belastingdienst, de materiële- en immateriële eigendommen en alle personen die zich op locaties van de Belastingdienst bevinden en de omgevingsvariabelen die hierop van invloed zijn.
Daarnaast vallen activiteiten die door de Belastingdienst zijn inbesteed of uitbesteed aan externe leveranciers, alsmede eigendommen van derden die ter beschikking staan van de Belastingdienst onder de reikwijdte ervan.

3.4 Managementsysteem voor integrale beveiliging

De Belastingdienst hanteert één managementsysteem voor integrale beveiliging, dat is samengesteld (geaggregeerd) uit de managementsystemen van de respectievelijke aspectgebieden.

Een managementsysteem is een geheel van samenhangende of elkaar beïnvloedende elementen van een organisatie om een beleid en doelstellingen vast te stellen, alsmede de processen om die doelstellingen te bereiken. Een managementsysteem omvat de volgende componenten:

- beleid;
- individuen met bepaalde verantwoordelijkheden;
- managementprocessen gerelateerd aan:
  1) beleidsvorming;
  2) bewustzijn en competentieontwikkeling;
  3) planning;
  4) implementatie;
  5) uitvoering;
  6) prestatiebeoordeling;
  7) (directie)beoordeling van het managementsysteem;
  8) verbetering;

- gedocumenteerde informatie.

Opmerkingen:
- Een managementsysteem kan betrekking hebben op een of meer disciplines.
- Tot de elementen van het systeem behoren de organisatiestructuur, rollen en verantwoordelijkheden, planning en uitvoering.
- Het toepassingsgebied van een managementsysteem kan de gehele organisatie omvatten, specifieke en geïdentificeerde functies van de organisatie, specifieke en geïdentificeerde onderdelen van de organisatie, of één of meer functies in een groep van organisaties.

De Belastingdienst kent de volgende managementsystemen:

3.4.1 BCMS

De Belastingdienst heeft een Business Continuity Management Systeem (BCMS). Dit omvat de organisatiestructuur, beleid, planningsactiviteiten, verantwoordelijkheden, procedures, processen en middelen. Het BCMS is conform de NEN-ISO 22301:2014. Deze internationale norm past het Plan-Do-Check-Act (PDCA) model toe als het gaat om het plannen, vaststellen, implementeren, uitvoeren, controleren, beoordelen, onderhouden en continu verbeteren van het BCMS.
Alle bedrijfsonderdelen van de Belastingdienst beschikken over een BCMS volgens de ISO/NEN22301. De output van deze BCMS-en zijn input voor het overkoepelende BCMS dat de PDCA-cycli van de gehele Belastingdienst monitort en op zijn beurt onderdeel uit maakt van het managementsysteem voor integrale beveiliging.

Doelstellingen van het BCMS
- Het vastleggen van het BCM beleid en de BCM-PDCA cyclus;
- Nadere invulling geven aan de normen uit de BIO en ISO 22301 en 22313;
- Het vaststellen van een crisisorganisatiestructuur waardoor de Belastingdienst in staat is om zich voor te bereiden op een crisis, deze waar mogelijk te voorkomen en in geval van een crisis de gevolgen te beheersen;
- Ervoor zorgdragen dat er voorzieningen zijn getroffen om de continuïteit van de kritische activiteiten te waarborgen in lijn met de vastgestelde continuïteitsstrategie(en);
- Het opstellen van plannen om te kunnen reageren op calamiteiten en crises;
- Als Belastingdienst in staat zijn om, ongeacht de omstandigheden, te voldoen aan verplichtingen die voortvloeien uit wet- en regelgeving;
- Het inzichtelijk hebben van de belangen, eisen en afhankelijkheden van andere organisaties, leveranciers en overige belanghebbenden;
- De medewerkers een passend opleidingsniveau bieden voor de rol die zij binnen de BCM-proces innemen;
- Het BCM bewustzijn binnen de Belastingdienst verhogen;
- Het zeker stellen dat de Belastingdienst de getroffen BCM maatregelen regelmatig herziet, beoordeelt, test en oefent;
- Het continu verbeteren van het BCM proces conform de ISO 22301.

3.4.2 PBMS

Het Personele Beveiligings Management Systeem (PBMS) is ten behoeve van personele veiligheid en integriteit.

3.4.3 DPMS

Het Data Protection Management Systeem (DPMS) is ten behoeve van privacy, de bescherming van (persoons)gegevensverwerking.

3.4.4 FBMS

Het Fysieke Beveiligings Management Systeem (FBMS) is ten behoeve van fysieke beveiliging.

3.4.5 ISMS

Een Information Security Management System (ISMS) heeft *aanvullend* componenten als:
- Informatiebeveiligingsrisicobeoordeling;
- Informatiebeveiligingsrisicobehandeling, waaronder bepaling en implementatie van beheersmaatregelen (controls).

3.4.6 Organisatorische toewijzing

De CSO is verantwoordelijk voor de inrichting en het functioneren van het management-systeem voor integrale beveiliging en de aansluiting hiervan op het managementsysteem van de BVA van het Kerndepartement.
Het managementsysteem bestaat uit de volgende onderdelen met verantwoordelijke directie:
- BCMS –CD IV&D
- PBMS – CD O&P
- DPMS – CD IV&D
- FBMS – SSO CFD
- ISMS – CD IV&D

Deze directies zijn verantwoordelijk voor de inrichting en het functioneren van het managementsysteem, inclusief de toewijzing van controls uit het betreffende managementsysteem aan controlverantwoordelijken.

Het managementsysteem moet geschikt zijn om:
- Effectiviteit van maatregelen in relatie tot controls te beoordelen (algemene compliancy met wet- en regelgeving). Dit geldt voor zowel het uitvoeren als het leveren van maatregelen;
- Risico's voor specifieke bedrijfsmiddelen (als eigendom van directeuren) te beoordelen. De directeur moet kunnen beoordelen of aan alle controls van alle management systemen voldaan is, zodat hij zijn verantwoordelijkheid kan nemen;
- Inzicht te verschaffen op diverse niveaus (centraal en binnen organisatieonderdelen). De regie voor de organisatie hiervan ligt bij de managementsysteemverantwoordelijke.

(Nieuwe) risico's die uit de managementsystemen volgen, worden beschreven en vastgelegd in een risicoregister en gekoppeld aan een risico-eigenaar.

Voor het DPMS, FBMS en het PBMS bestaan er geen specifieke normen die eisen stellen aan het managementsysteem. Deze eisen moeten door de managementsysteemeigenaar in een systeem gevat worden, waarbij de ISO High Level Structure gevolgd dient te worden.

4 Planning

Zie apart Plan van Aanpak Integrale Beveiliging.

4.1 Maatregelen om risico's aan te pakken en kansen te benutten

Bij het plannen voor het integrale beveiligingsmanagementsysteem moet de organisatie de in 3.1 genoemde onderwerpen en de in 3.2 genoemde eisen overwegen, en de risico's en kansen vaststellen die moeten worden aangepakt om:

- te bewerkstelligen dat het integrale beveiligingsmanagementsysteem zijn beoogde resulta(a)t(en) behaalt;
- ongewenste effecten te voorkomen of te verminderen;
- continue verbetering te bereiken.

De organisatie moet:

- maatregelen plannen om deze risico's en kansen aan te pakken;
- plannen op welke manier:
  a) de maatregelen in haar integrale beveiligingsmanagementsysteemprocessen worden geïntegreerd en geïmplementeerd;
  b) de doeltreffendheid van deze maatregelen moet worden geëvalueerd.

4.2 Integrale beveiligingsdoelstellingen en de planning om ze te bereiken

De organisatie moet voor relevante functies en op relevante niveaus integrale beveiligingsdoelstellingen vaststellen.
De integrale beveiligingsdoelstellingen moeten:

a) consistent zijn met het integrale beveiligingsbeleid en daarmee de vigerende wet- en regelgeving;
b) meetbaar zijn (indien praktisch uitvoerbaar);
c) rekening houden met van toepassing zijnde eisen;
d) worden gemonitord;
e) worden gecommuniceerd;
f) indien van toepassing, worden geactualiseerd.

De organisatie moet gedocumenteerde informatie over de integrale beveiligingsmanagementsystemen en -doelstellingen bewaren. Bij het opstellen van planningen voor het bereiken van de integrale beveiligingsdoelstellingen moet de organisatie vaststellen:

- wat er zal worden gedaan;
- welke middelen er nodig zijn;
- wie er verantwoordelijk is;
- wanneer het zal zijn voltooid;
- hoe de resultaten zullen worden geëvalueerd.

5 Ondersteuning

Zie apart Plan van Aanpak Integrale Beveiliging.

5.1 Middelen

De organisatie moet de middelen vaststellen en beschikbaar stellen die nodig zijn voor het inrichten, implementeren, onderhouden en continu verbeteren van het integrale beveiligingsmanagementsysteem.

5.2 Competentie

De organisatie moet:
- de noodzakelijke competentie vaststellen van de perso(o)n(en) die onder haar gezag werkzaamheden verricht(en) die de integrale beveiligingsprestaties van de organisatie beïnvloeden;
- bewerkstelligen dat deze personen competent zijn op basis van de juiste scholing, opleiding of ervaring;
- waar van toepassing, maatregelen nemen om de benodigde competentie te verwerven, en de doeltreffendheid van de genomen maatregelen evalueren;
- geschikte gedocumenteerde informatie als bewijsmateriaal van competentie bewaren.

Opmerking: Geschikte maatregelen kunnen bijvoorbeeld zijn: het voorzien in training van, het begeleiden van, of het in een andere functie benoemen van mensen die al in dienst zijn; of het inhuren of contracteren van competente personen.

5.3 Bewustzijn

Personen die werkzaamheden verrichten onder het gezag van de organisatie, moeten zich bewust zijn van:
- het integrale beveiligingsbeleid;
- hun bijdrage aan de doeltreffendheid van het integrale beveiligingsmanagementsysteem, met inbegrip van de voordelen van verbeterde integrale beveiligingsprestaties;
- de gevolgen van het niet voldoen aan de eisen van het integrale beveiligingsmanagementsysteem.

5.4 Communicatie

De organisatie moet de behoefte vaststellen aan interne en externe communicatie die relevant is voor het integrale beveiligingsmanagementsysteem, waaronder:
- waarover te communiceren;
- wanneer te communiceren;
- met wie te communiceren;
- hoe te communiceren.

5.5 Gedocumenteerde informatie

5.5.1 Algemeen

Het integrale beveiligingsmanagementsysteem van de organisatie moet onder andere bevatten:
a) de gedocumenteerde informatie die de internationale norm vereist;
b) de gedocumenteerde informatie die de organisatie nodig acht voor de doeltreffendheid van hetintegrale beveiligingsmanagementsysteem.

Opmerking: De uitgebreidheid van gedocumenteerde informatie voor een integrale beveiligingsmanagementsysteem kan van organisatie tot organisatie verschillen vanwege:

- de omvang van de organisatie en het type van haar activiteiten, processen, producten en diensten;
- de complexiteit van de processen en hun interacties;
- de competentie van de mensen.

5.5.2 Creëren en actualiseren

Bij het creëren en actualiseren van gedocumenteerde informatie moet de organisatiezorgen voor een passend(e):

- identificatie en beschrijving (bijv. een titel, datum, auteur of referentienummer);
- format (bijv. taal, softwareversie, afbeeldingen) en media (bijv. papier, elektronisch);
- beoordeling en goedkeuring van geschiktheid en adequaatheid.

5.5.3 Beheer van gedocumenteerde informatie

Gedocumenteerde informatie zoals het integrale beveiligingsmanagementsysteem en de internationale norm vereisen, moet worden beheerd om te bewerkstelligen dat:
a) de informatie beschikbaar is en geschikt is voor gebruik, waar en wanneer het nodig is;
b) de informatie adequaat is beveiligd (bijv. tegen verlies van vertrouwelijkheid, oneigenlijk gebruik en aantasting).
Voor het beheren van gedocumenteerde informatie moet de organisatie, voor zover van toepassing, invulling geven aan de volgende activiteiten:

- distributie, toegang, het terugvinden alsmede het gebruik;
- opslag en behoud, waaronder behoud van leesbaarheid;
- beheersing van wijzigingen (bijv. versiebeheer);
- bewaring en vernietiging.

Gedocumenteerde informatie van externe oorsprong die de organisatie nodig acht voor de planning en uitvoering van het integrale beveiligingsmanagementsysteem, moet worden geïdentificeerd voor zover van toepassing en beheerd.

Opmerking: Toegang kan betekenen een besluit tot toestemming om de gedocumenteerde informatie alleen in te zien, of tot toestemming en bevoegdheid om de gedocumenteerde informatie in te zien en te wijzigen.

6 Uitvoering

Zie apart Plan van Aanpak Integrale Beveiliging.

6.1 Operationele planning en uitvoering

Om te voldoen aan de eisen, en om de in 4.1 vastgestelde maatregelen te implementeren, moet de organisatie de benodigde processen plannen, implementeren en beheersen, door:

- criteria voor de processen vast te stellen;
- procesbeheersing te implementeren in overeenstemming met de criteria;
- gedocumenteerde informatie bij te houden in de omvang die nodig is om het vertrouwen te hebben dat de processen volgens planning zijn uitgevoerd.

De organisatie moet geplande wijzigingen beheersen en de consequenties van onbedoelde wijzigingen beoordelen, en zo nodig maatregelen treffen om nadelige effecten tegen te gaan. De organisatie moet bewerkstelligen dat uitbestede processen worden beheerst.

7 Evaluatie van de prestaties

Zie apart Plan van Aanpak Integrale Beveiliging.

7.1 Monitoren, meten, analyseren en evalueren

De organisatie moet vaststellen:
- wat moet worden gemonitord en gemeten;
- welke methoden worden gebruikt voor het, voor zover van toepassing, monitoren, meten, analyseren en evalueren, om geldige resultaten te bewerkstelligen;
- wanneer moet worden gemonitord en gemeten;
- wanneer de resultaten van het monitoren en meten moeten worden geanalyseerd en geëvalueerd.

De organisatie moet geschikte gedocumenteerde informatie bewaren als bewijsmateriaal van de resultaten.
De organisatie moet de integrale beveiligingsprestaties en de doeltreffendheid van het integrale beveiligingsmanagementsysteem evalueren.

7.2 Interne audit

De organisatie moet met geplande tussenpozen interne audits uitvoeren om informatie te verkrijgen of het integrale beveiligingsmanagementsysteem overeenkomt met de eigen eisen van de organisatie voor haar integrale beveiligingsmanagementsysteem, de eisen van wet- en regelgeving en doeltreffend is geïmplementeerd en onderhouden.

De organisatie moet:
a) (een) auditprogramma('s) plannen, vaststellen, implementeren en onderhouden, met inbegrip van de frequentie, methoden, verantwoordelijkheden, planningseisen en rapportage. Het auditprogramma moet rekening houden met het belang van de betrokken processen en de resultaten van voorgaande audits;
b) de auditcriteria voor en de reikwijdte van elke audit definiëren;
c) auditoren selecteren en audits uitvoeren zodanig dat de objectiviteit en de onpartijdigheid van het auditproces worden bewerkstelligd;
d) bewerkstelligen dat de resultaten van de audits worden gerapporteerd aan het relevante management;
e) gedocumenteerde informatie bewaren als bewijsmateriaal van de implementatie van het auditprogramma en de auditresultaten.

7.3 Directiebeoordeling

De directie moet met geplande tussenpozen het integrale beveiligingsmanagementsysteem van de organisatie beoordelen, om de continue geschiktheid, adequaatheid en doeltreffendheid te bewerkstelligen.
Bij de directiebeoordeling moet onder andere in overweging worden genomen:
a) de status van acties als gevolg van voorgaande directiebeoordelingen;
b) wijzigingen in externe en interne onderwerpen die relevant zijn voor het integrale beveiligingsmanagementsysteem;
c) informatie over de integrale beveiligingsprestaties, met inbegrip van trends in:
- afwijkingen en corrigerende maatregelen;
- resultaten van monitoren en meten;
- auditresultaten;
- kansen voor continue verbetering.

De resultaten van de directiebeoordeling moeten beslissingen omvatten met betrekking tot kansen voor continue verbetering en de noodzaak voor wijzigingen in het integrale beveiligingsmanagementsysteem.
De organisatie moet gedocumenteerde informatie bewaren als bewijsmateriaal van de resultaten van de directiebeoordeling.

8 Verbetering

Zie apart Plan van Aanpak Integrale Beveiliging.

8.1 Afwijkingen en corrigerende maatregelen

Wanneer zich een afwijking voordoet, moet de organisatie:
a) op de afwijking reageren, en indien van toepassing:
- maatregelen treffen om de afwijking te beheersen en te corrigeren;
- de consequenties aanpakken;

b) de noodzaak evalueren om maatregelen te treffen om de oorzaken van de afwijking weg te nemen, zodat de afwijking zich niet herhaalt of zich elders voordoet, door:
- de afwijking te beoordelen;
- de oorzaken van de afwijking vast te stellen;
- vast te stellen of zich gelijksoortige afwijkingen voordoen of zouden kunnen voordoen;

c) de benodigde maatregelen implementeren;
d) de doeltreffendheid van getroffen corrigerende maatregelen beoordelen;
e) zo nodig, wijzigingen aanbrengen in het integrale beveiligingsmanagementsysteem.

Corrigerende maatregelen moeten passend zijn voor de effecten van de opgetreden afwijkingen.

De organisatie moet gedocumenteerde informatie bewaren als bewijsmateriaal van:
- de aard van de afwijkingen en de vervolgens genomen maatregelen;
- de resultaten van corrigerende maatregelen.

8.2 Continue verbetering

De organisatie moet continu de geschiktheid, adequaatheid en doeltreffendheid van het integrale beveiligingsmanagementsysteem verbeteren.

Bijlage I Stelsel van Integrale Beveiliging

Zie separate bijlage.

Bijlage II Taken, bevoegdheden en verantwoordelijkheden

Zie separate bijlage.

Bijlage III Gebruikte afkortingen

ADR	Auditdienst Rijk
AIVD	Algemene Inlichtingen- en Veiligheidsdienst
BCM	Business continuity management, bedrijfscontinuïteitsbeheer
BHV	Bedrijfshulpverlening
BIA	Business Impact Analysis
BIO	Baseline Informatiebeveiliging Overheid
BVA	Beveiligingsambtenaar
BVR	Beveiligingsvoorschrift Rijksdienst
BZK	Ministerie van Binnenlandse Zaken en Koninkrijksrelaties
CDV	Concerndienstverlener
CIO	Chief Information Officer
CSO	Chief Security Officer
FG	Functionaris voor de Gegevensbescherming
JenV	Ministerie van Justitie en Veiligheid
NkBR	Normenkader Beveiliging Rijkskantoren
NCSC	Nationaal Cyber Security Centrum
PDCA	Plan - do - check – act
PIA	Privacy Impact Assessment
TBO	Tactisch Beveiligingsoverleg
VIR	Voorschrift Informatiebeveiliging Rijksdienst
VIRBI	VIR Bijzondere Informatie

Bijlage IV Normatieve verwijzingen

De volgende documenten, waarnaar als geheel of voor een onderdeel, in dit document normatief is verwezen, zijn onmisbaar voor de toepassing ervan. Bij gedateerde verwijzingen is alleen de aangehaalde uitgave van toepassing. Bij ongedateerde verwijzingen is de laatste uitgave van het document (met inbegrip van eventuele wijzigings- en correctiebladen waarnaar is verwezen) van toepassing.

- Baseline informatiebeveiliging Overheid (BIO) 2019, vervangt Baseline Informatiebeveiliging Rijksdienst (BIR) 2017[8]
- NEN-ISO/IEC 27001:2013 Informatietechnologie - Beveiligingstechnieken - Managementsystemen voor informatiebeveiliging - Eisen
- NEN-ISO/IEC 27002:2013 Informatietechnologie - Beveiligingstechnieken - Praktijkrichtlijn met beheersmaatregelen op het gebied van informatiebeveiliging
- NEN-EN-ISO 22301:2012 Maatschappelijke veiligheid – Managementsystemen voor bedrijfscontinuïteit (business continuity management systems) – Eisen
- NEN-EN-ISO 22313:2014 Maatschappelijke veiligheid – Managementsystemen voor bedrijfscontinuïteit (business continuity management systems) – Richtlijnen
- ISO/IEC 27017:2015 Information technology – Security techniques – Code of practice for information security controls based on ISO/IEC 27002 for cloud services
- ISO/IEC 27018:2014 Information technology – Security techniques – Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors
- ISO 31000:2018, Risk management – Guidelines
- Normenkader Beveiliging Rijkskantoren (NkBR) 2015

[8] De BIO is verplicht vanaf 2020, met 2019 als overgangsjaar.

Bijlage V Termen en definities

Begrip	Beschrijving	Bron
Afwijking	Het niet voldoen aan een eis.	ISO HLS paragraaf 3.19.
Audit	Systematisch, onafhankelijk en gedocumenteerd proces voor het verkrijgen van auditbewijsmateriaal en het objectief beoordelen daarvan om vast te stellen in welke mate aan de auditcriteria is voldaan.	ISO HLS paragraaf 3.17.
Belanghebbende	Persoon of organisatie die een besluit of activiteit kan beïnvloeden, door een besluit of activiteit kan worden beïnvloed, of zichzelf beschouwt als beïnvloed door een besluit of activiteit.	ISO HLS paragraaf 3.2.
Beleid	Bedoelingen en richting van een organisatie zoals formeel door de directie kenbaar gemaakt.	ISO HLS paragraaf 3.7.
Competentie	Vermogen om kennis en vaardigheden toe te passen om beoogde resultaten te bereiken.	ISO HLS paragraaf 3.10.
Conformiteit	Het voldoen aan een eis.	ISO HLS paragraaf 3.18.
Continue verbetering	Zich herhalende activiteit om prestaties te verbeteren.	ISO HLS paragraaf 3.21.
Corrigerende maatregel	Maatregel om de oorzaak van een afwijking weg te nemen en om herhaling te voorkomen.	ISO HLS paragraaf 3.20.
Directie	Persoon of groep van personen die een organisatie op het hoogste niveau bestuurt en beheert.	ISO HLS paragraaf 3.5.
Doelstelling	Te behalen resultaat.	ISO HLS paragraaf 3.8.
Doeltreffendheid	Mate waarin geplande activiteiten worden gerealiseerd en geplande resultaten worden behaald.	ISO HLS paragraaf 3.6.
Eis	Behoefte of verwachting die kenbaar is gemaakt, vanzelfsprekend is of dwingend is voorgeschreven.	ISO HLS paragraaf 3.3.
Gedocumenteerde informatie	Informatie die een organisatie moet beheren en onderhouden en het medium waarop deze informatie is vastgelegd.	ISO HLS paragraaf 3.11.
Informatiebeveiliging	Het proces van vaststellen van de vereiste betrouwbaarheid van informatiesystemen in termen van vertrouwelijkheid, beschikbaarheid en integriteit alsmede het treffen, onderhouden en controleren van een samenhangend pakket van bijbehorende maatregelen.	VIR.
Informatiesysteem	Een samenhangend geheel van gegevensverzamelingen, en de daarbij behorende personen, procedures, processen en programmatuur alsmede de voor het informatiesysteem getroffen voorzieningen voor opslag, verwerking en communicatie	VIR.
Integrale beveiliging	Het selecteren, implementeren en periodiek evalueren van een samenhangend stelsel van beveiligingsmaatregelen van de organisatie, medewerkers, materieel, informatiesystemen, gebouwen en overige objecten op basis van risicomanagement.	BVR.

Managementsysteem	Geheel van samenhangende of elkaar beïnvloedende elementen van een organisatie om een beleid en doelstellingen vast te stellen, alsmede de processen om die doelstellingen te bereiken.	ISO HLS paragraaf 3.4.
Meting	Proces om een waarde vast te stellen.	ISO HLS paragraaf 3.16.
Monitoren	Vaststellen van de status van een systeem, een proces of een activiteit.	ISO HLS paragraaf 3.15.
Organisatie	Persoon of groep van personen die zijn eigen functies heeft met verantwoordelijkheden, bevoegdheden en relaties om zijn doelstellingen te bereiken.	ISO HLS paragraaf 3.1.
Prestatie	Meetbaar resultaat.	ISO HLS paragraaf 3.13.
Proces	Geheel van samenhangende of elkaar beïnvloedende activiteiten dat input omzet in output.	ISO HLS paragraaf 3.12.
Risico	Effect van onzekerheid.	ISO HLS paragraaf 3.9.
Risicomanagement	Inzichtelijk en systematisch inventariseren, beoordelen en – door het treffen van maatregelen – beheersbaar maken van risico's en kansen, die het bereiken van de doelstellingen van de organisatie bedreigen dan wel bevorderen, op een zodanige wijze dat verantwoording kan worden afgelegd over de gemaakte keuzes.	BVR.
Stakeholder	Belanghebbende.	ISO HLS paragraaf 3.2.
Uitbesteden	Treffen van een overeenkomst waarbij een externe organisatie een deel van een functie of proces van de organisatie verricht.	ISO HLS paragraaf 3.14.