Good Practice

Informatiebeveiliging 2023

DeNederlandscheBank

EUROSYSTEEM

Inleiding

Deze Good Practice geeft de onder toezicht van DNB staande instellingen handvatten, beheersmaatregelen, waarmee zij kunnen voldoen aan de wettelijke bepalingen om de voortdurende beschikbaarheid, integriteit, vertrouwelijkheid en authenticiteit van de (geautomatiseerde) gegevensverwerking te waarborgen. In dit document wordt het waarborgen van de integriteit, voortdurende beschikbaarheid en de beveiliging van de geautomatiseerde gegevensverwerking, kort aangeduid met "informatiebeveiliging en cybersecurity".

Ter beheersing van risico's op het gebied van informatiebeveiliging en cybersecurity treffen instellingen – op grond van een risico-analyse –beheersmaatregelen. Deze beheersmaatregelen zijn passend bij de aard, omvang, complexiteit en evolutie van de risico's van de activiteiten van de instelling en de complexiteit van haar organisatiestructuur. De beheersmaatregelen zijn niet alleen gericht op technologische oplossingen (*Technology*), zij zijn ook gericht op menselijk handelen (*People*), inrichting van processen (*Processes*) en faciliteiten (*Facilities*).

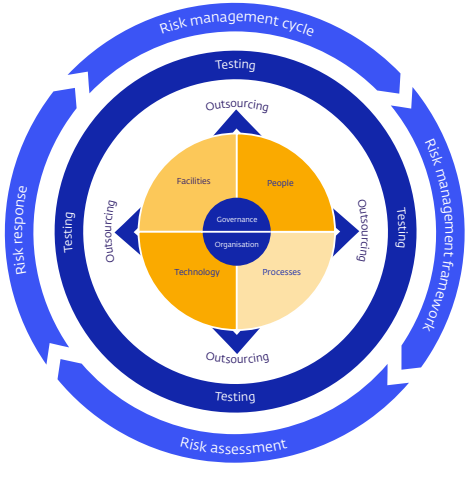
Instellingen evalueren periodiek en aantoonbaar in hoeverre de getroffen beheersmaatregelen in opzet, bestaan en werking effectief zijn om de voortdurend veranderende risico's op het gebied van informatiebeveiliging en cybersecurity het hoofd te bieden. Dit doen zij op basis van een risicoanalyse– als onderdeel van hun risicomanagementproces (*Risk Management Cycle*) en metrics die de daadwerkelijke impact van de maatregelen aantonen. Daar waar nodig worden beheersmaatregelen verbeterd of vervangen door betere beheersmaatregelen.
De instellingen richten hun bestuur (*Governance*) en organisatie (*Organisation)* in om de aansturing hiervan te bewerkstelligen. Instellingen zorgen daarbij onder andere in lijn met de nieuwe corporate governance code 2022, de *DNB Q&A Sleutelfuncties en adequate functiescheiding* en de *DNB Q&A Operationeel onafhankelijke en proportionele inrichting van sleutelfuncties* voor een passende scheiding en onafhankelijkheid van ICT-risicobeheer functies, controlefuncties en interne auditfuncties[1]. Verder heeft het bestuur aantoonbaar op hen toegesneden trainingen en opleidingen gevolgd om de belangrijkste ICT-risico's en beheers-maatregelen voor haar instelling te kunnen begrijpen en adresseren (*People*).

Tevens zorgen instellingen ervoor dat zij 'in control' zijn op het gebied van informatiebeveiliging bij uitbesteding (*Uitbesteding*).

Daarnaast testen (*Testing)* zij in hoeverre zij als instelling weerbaar zijn tegen cyberdreigingen. In deze Good Practice is een volwassen-heidsmodel opgenomen op grond waarvan DNB de beheersing van risico's op het gebied van informatiebeveiliging en cybersecurity toetst bij de onder haar toezicht staande instellingen.

Leeswijzer

Deze Good Practice is vormgegeven aan de hand van het volgende model dat bestaat uit corresponderende 'elementen'. ▶



1 Nederlandse+Corporate+Governance+Code+2022.pdf
https://www.dnb.nl/voor-de-sector/open-boek-toezicht/sectoren/pensioenfondsen/prudentieel-toezicht/governance/sleutelfuncties-en-adequate-functiescheiding/
https://www.dnb.nl/voor-de-sector/open-boek-toezicht/sectoren/verzekeraars/risicomanagement-en-governance-pilaar-2/operationeel-onafhankelijke-en-proportionele-inrichting-van-sleutelfuncties/

De Good Practice kan vanuit twee invalshoeken worden gelezen:

1. **Samengevat** voor bestuurders, raad van toezicht, raad van commissarissen, sleutelfunctiehouders en beleidsbepalers.
   Per element vindt u een korte samenvatting van de belangrijkste beheersmaatregelen met voorbeelden. De beheersmaatregelen zijn toegespitst op de instelling en op de rol van het bestuur bij het implementeren van en het toezien op die beheersmaatregelen.

2. **Gedetailleerd** op het niveau van de beheersmaatregelen voortkomend uit marktstandaarden[2] met bijbehorende Good Practices.
   Bij elk element kan via een link worden doorgeklikt naar de beheersmaatregelen. Voor de leesbaarheid is elke beheersmaatregel telkens onder één element uit het model opgenomen. Beheersmaatregelen kunnen bij verschillende elementen passen.

Onder het tabblad *Inhoud* kunt u op de verschillende elementen van het model klikken. Er zijn tabbladen toegevoegd voor de Q&A Informatiebeveiliging en voor het volwassenheidsmodel.

Aanleiding voor de update van de Good Practice Informatiebeveiliging (IB)

DNB onderzoekt structureel de kwaliteit van informatiebeveiliging en cybersecurity binnen de financiële sector.

De afgelopen decennia ziet DNB in de financiële sector en daarbuiten een toename van potentieel zeer schadelijke en geprofessionaliseerde cyberdreigingen. Verder ziet DNB een financiële sector die als gevolg van verschillende vormen van uitbesteding en samenwerkingsverbanden meer in ketens opereert, met de daarbij behorende kansen en risico's voor informatiebeveiliging en cybersecurity.

Het belang van kennis en aandacht op het gebied van informatiebeveiliging en cyberrisico's wordt aan veel bestuurstafels onderschreven. Bestuurlijke verankering van dit onderwerp en het op orde brengen en houden van kennis bij bestuurders en intern toezicht behoeft nadrukkelijke aandacht.

Sinds de publicatie van de Good Practice Informatiebeveiliging 2019/2020 zijn door de European Supervisory Authorities waaronder EIOPA twee relevante Guidelines op het gebied van informatiebeveiliging uitgebracht over ICT security en uitbesteding[3].

Daarnaast heeft de Europese commissie recent de geconsolideerde versie van *Proposal for a regulation on digital operational resilience for the financial sector and amending Regulations (DORA)*[4] vastgesteld die per 17 januari 2025 van toepassing is.

In haar toezichtonderzoeken en het TIBER[5] programma is DNB de afgelopen jaren veel goede voorbeelden van beheersmaatregelen tegengekomen die risico's kunnen mitigeren.

Verder zijn vanuit de diverse financiele sectoren verschillende goede voorbeelden en verbeteringen van de Good Practice Informatiebeveiliging aangedragen. Dit was aanleiding om de 'Good Practice Informatiebeveiliging 2019/2020' te actualiseren. Met deze actualisatie draagt DNB uit dat informatiebeveiliging en cybersecurity permanente aandacht behoeft. Deze aandacht ziet op strategisch en bestuurlijk niveau om de verbetering van de effectiviteit van de beheersmaatregelen, die past bij een voortdurend veranderend dreigingsbeeld waarmee instellingen worden geconfronteerd, te blijven waarborgen. ▶

2 Voor de beheersmaatregelen in deze Good Practice en bijbehorende Q&A zijn relevante Internationale Standaarden aangehaald waaronder EIOPA Richtsnoeren betreffende beveiliging en governance van informatie- en communicatietechnologie en EIOPA Richtsnoeren voor uitbesteding aan aanbieders van clouddiensten, Proposal for a regulation on digital operational resilience for the financial sector and amending Regulations (DORA), Cobit (Control Objectives for Information and related Technology) van ISACA, ISO27000, het NIST Cybersecurity Framework SP 800-207, Zero Trust Architecture | CSRC (nist.gov) en The 18 CIS Critical Security Controls (cisecurity.org).
3 EIOPA Richtsnoeren betreffende beveiliging en governance van informatie- en communicatietechnologie en EIOPA Richtsnoeren voor uitbesteding aan aanbieders van clouddiensten
4 Zie, EUR-Lex - 52020PC0595 - EN - EUR-Lex (europa.eu)
5 Threat Intelligence Based Ethical Red-teaming TIBER: samen tegen cybercrime (dnb.nl)

Wat is er gewijzigd ten opzichte van de Good Practice Informatiebeveiliging 2019/2020?

De Good Practice Informatiebeveiliging 2023 sluit zoveel mogelijk aan op de indeling van de 'Good Practice Informatiebeveiliging 2019/2020' [6].

De voornoemde guidelines van EIOPA zijn verwerkt in de beheersmaatregelen (controls) in de Good Practice Informatie-beveiliging 2023. De voorbeelden bij de controls zijn geactualiseerd. Hierbij zijn marktstandaarden vanuit de Zero Trust Architecture (NIST[7]) en de CIS Critical Security Controls[8] betrokken, en heeft DNB praktijkvoorbeelden opgehaald uit het toezicht.

Daarnaast zijn in deze update de ontwikkelingen rondom DORA[9] betrokken; belangrijke aspecten en uitgangspunten van DORA zijn verwerkt. Echter, de Regulatory technical standards (RTS)[10] van DORA waren tijdens het actualiseren van deze Good Practice Informatiebeveiliging 2023 nog niet allen op gedetailleerd niveau uitgewerkt en derhalve nog niet verwerkt. De GP moet daarom worden gezien als aanvulling op de ontwikkeling rond DORA en niet als (volledige) vervanging van DORA.

De belangrijkste wijzigingen zijn:

- een verdere verdieping cq aanscherping van de beschrijvingen ten opzichte van de Good Practice informatiebeveiliging 2019/2020.
- aandacht voor een risico-gebaseerde invulling per control. Hierdoor kunnen de instellingen steeds verdergaand maatwerk toepassen ten aanzien van de inrichting en implementatie van hun specifieke informatiebeveiligingsmaatregelen.
- aandacht voor het uitvoeren van een business impact analyse, om daarmee de blootstelling van de instelling aan ernstige bedrijfsonderbrekingen en de potentiële gevolgen ervan te kunnen beoordelen.
- aandacht voor een digitale operationele weerbaarheid strategie op korte, middellange en lange termijn die uiteenzet hoe het Risk Management Framework wordt uitgevoerd.
- de rol van het bestuur van de instellingen is uitgeschreven in een groot deel van de controls.
- aandacht voor het aantoonbaar volgen van op hen toegesneden trainingen en opleidingen door het bestuur, raad van toezicht, raad van commissarissen en sleutelfunctiehouders om de belangrijkste ICT-risico's en beheersmaatregelen voor hun instelling te kunnen begrijpen en adresseren.
- aandacht voor het inrichten van een informatiebeveiligings-functie door de instellingen.
- extra voorbeelden voor het versterken van de samenwerking tussen instellingen en andere betrokken partijen.
- aandacht voor risico's die kunnen voortkomen uit 'Quantum Computing' en de mogelijke beheersing daarvan.
- verduidelijking van de volwassenheidsniveaus.

Een holistische benadering

De Good Practice Informatiebeveiliging bevat een stelsel aan beheersmaatregelen voor instellingen om te komen tot een operational resilience framework waarin het stelsel van beheersmaatregelen een integrale benadering ten aanzien van de inrichting en implementatie van hun specifieke informatie-beveiligingsmaatregelen is. In de Good Practice Informatie-beveiliging hangen de verschillende beheersmaatregelen met elkaar samen en versterken elkaar. Risico's kunnen door verschillende beheersmaatregelen worden gemitigeerd en een beheersmaatregel kan verschillende risico's afdekken. De Good Practice Informatiebeveiliging ziet er op toe dat daarbij de bestuurders, de raden van toezicht, raden van commissarissen, de eerste, tweede en derde lijn, de ketenpartners en de dienst-verleners, aan wie activiteiten zijn uitbesteed, samenwerken. ▶

6 Voor de herkenbaarheid zijn de beheersmaatregelen op dezelfde wijze genummerd.
7 SP 800-207, Zero Trust Architecture | CSRC (nist.gov)
8 The 18 CIS Critical Security Controls (cisecurity.org)
9 Digital Operational Resilience Act. EU vereisten die erop zijn gericht om ICT weerbaar te maken tegen ernstige operationele verstoringen en cyberaanvallen.
10 Digital finance: Council adopts Digital Operational Resilience Act - Consilium (europa.eu)

Diverse vormen van assurance vanuit externe (ICT-)Auditors kunnen ten aanzien van de Good Practice Informatiebeveiliging waarborgen geven aan bestuurders, raden van toezicht en raden van commissarissen[11].

Voor verdere verduidelijking is een begrippenlijst toegevoegd.

Reikwijdte

Deze Good Practice laat zien – zonder ernaar te streven compleet te zijn – wat DNB verstaat onder een juiste invulling van de regelgeving op het op een integere en beheerste wijze inrichten van informatiebeveiliging en cybersecurity. Het is aan de instellingen zelf om een beheersingsraamwerk te implementeren dat past bij de aard, risicoprofiel, omvang en complexiteit van de instelling. Deze Good Practice sluit niet uit dat voor een instelling een afwijkende, mogelijk strengere toepassing van de onderliggende regels geboden is, dan wel dat onderdelen van de Good Practice niet relevant zijn voor een betreffende instelling. ■

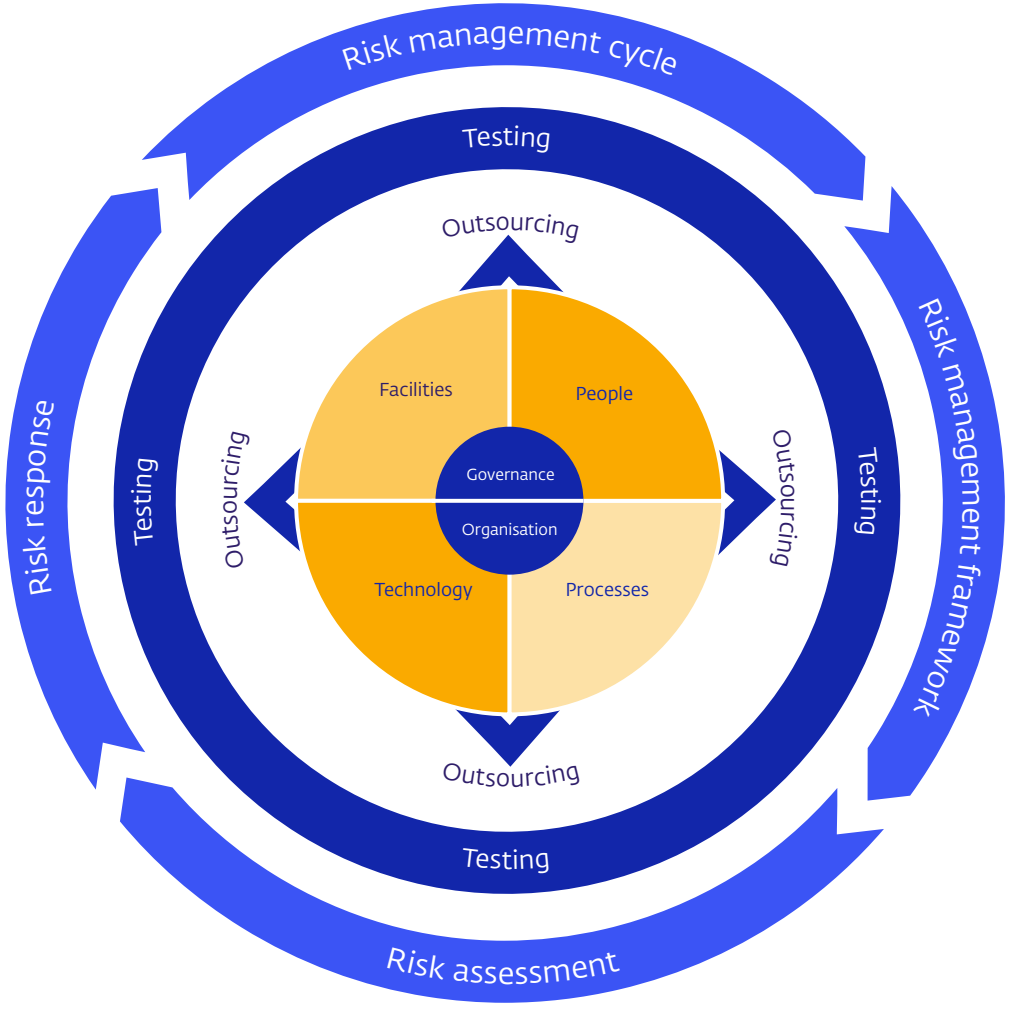
Disclaimer

Voor deze Good Practice geldt dat dit niet-verplichtende aanbevelingen zijn. Met behulp van deze Good Practice draagt DNB haar opvattingen uit over de geconstateerde of verwachte gedragingen in de beleidspraktijk, die naar ons oordeel een goede toepassing inhouden voor informatiebeveiliging en cybersecurity.

Met deze Good Practice beoogt DNB te bereiken dat de onder toezicht staande instellingen het daarin gestelde, de eigen omstandigheden in aanmerking nemende, in hun afweging betrekken, zonder dat zij verplicht zijn dat te doen. DNB Good Practices zijn indicatief van aard en sluiten daarmee niet uit dat voor instellingen een afwijkende, al dan niet strengere toepassing van de onderliggende regels geboden is.

11 Voorbeelden daarvan zijn COS 3000 SOC2 rapportage alsmede een recent uitgebrachte standaard van NOREA over het ICT verslag en de ICT-Audit verklaring https://www.norea.nl/nieuws/nieuw-de-it-auditverklaring en Microsoft Word - NOREA Reporting on Management of ICT - v0.11 MASTER.docx

DNB Good Practice Informatiebeveiliging 2023



Q&A Informatiebeveiliging

Open Boek Toezicht

DNB onderzoekt structureel de kwaliteit van informatiebeveiliging en cybersecurity binnen de financiële sector. Dit doet zij onder meer op basis van periodieke *self assessments* van de onder haar toezicht staande instellingen. Als handvat voor het invullen van deze *self assessments* gaf DNB tot 2019 in de 'Q&A Toetsingskader Informatiebeveiliging voor DNB onderzoek' aan waar zij op let bij haar onderzoeken. In 2019 is de Q&A vervangen door de 'Q&A Informatiebeveiliging' en de 'Good Practice Informatiebeveiliging'. DNB heeft de Q&A en de Good Practice Informatiebeveiliging per eind 2023 geactualiseerd (zie onder 'Downloads' op Open Boek Toezicht).

Vraag:

Hoe voldoen pensioenfondsen, premiepensioeninstellingen en verzekeraars (hierna "instellingen") onder het toezicht van DNB aan de wettelijke eisen ten aanzien van de voortdurende beschikbaarheid, integriteit, vertrouwelijkheid, authenticiteit, verantwoording, onweerlegbaarheid en betrouwbaarheid van de geautomatiseerde gegevensverwerking?

Antwoord:

Op grond van art. 3.17 Wet Financieel Toezicht, juncto artikel 20 Besluit prudentiële regels en artikel 143 Pensioenwet en artikel 18 Besluit FTK beschikken instellingen onder toezicht van DNB over adequate procedures en maatregelen ter beheersing van ICT-risico's. Onder beheersing van ICT-risico's valt het waarborgen van de integriteit, voortdurende beschikbaarheid en de beveiliging van de geautomatiseerde gegevensverwerking. Adequaat betekent in dit verband dat de procedures en beheersmaatregelen zijn gebaseerd op de aard, omvang en complexiteit van de risico's van de activiteiten van de instelling en de complexiteit van haar organisatiestructuur. Dit omvat tevens procedures en beheersmaatregelen van die onderdelen van de geautomatiseerde gegevensverwerking die zijn (onder)uitbesteed. In dit document worden het waarborgen van de integriteit, voortdurende beschikbaarheid en de beveiliging van geautomatiseerde gegevens, kort aangeduid met 'informatiebeveiliging en cybersecurity'.

Om aan deze bepalingen te kunnen voldoen hebben instellingen op grond van een risicoanalyse beheersmaatregelen getroffen op het gebied van informatiebeveiliging en cybersecurity. Deze beheersmaatregelen zijn niet alleen gericht op technologische oplossingen (*Technology*), zij zijn ook gericht op menselijk handelen (*People*), inrichting van processen (*Processes*) en faciliteiten (*Facilities*).

Instellingen evalueren periodiek en aantoonbaar in hoeverre de getroffen beheersmaatregelen in opzet, bestaan en werking effectief zijn om de voortdurend veranderende risico's op het gebied van informatiebeveiliging en cybersecurity het hoofd te bieden. Dit doen zij op basis van een risicoanalyse– als onderdeel van hun risicomanagementproces (*Risk Management Cycle*). Daar waar nodig worden beheersmaatregelen verbeterd of vervangen door andere beheersmaatregelen. De instellingen richten hun bestuur (*Governance*) en organisatie (*Organisation*) in om de aansturing hiervan te bewerkstelligen. Instellingen zorgen daarbij onder andere in lijn met de nieuwe corporate governance code 2022, de *DNB Q&A Sleutelfuncties en adequate functiescheiding* en de *DNB Q&A Operationeel onafhankelijke en proportionele inrichting van sleutelfuncties* voor een passende scheiding en onafhankelijkheid van ICT-risicobeheer functies, controlefuncties en interne auditfuncties. Verder heeft het bestuur aantoonbaar op hen toegesneden trainingen en opleidingen gevolgd om de belangrijkste ICT-risico's en beheersmaatregelen voor haar instelling te kunnen begrijpen (*People*). ▶

Tevens zorgen instellingen ervoor dat zij 'in control' zijn op het gebied van informatiebeveiliging bij uitbesteding (*Outsourcing*). Daarnaast testen (*Testing*) zij in hoeverre zij als instelling weerbaar zijn tegen cyberdreigingen.

In de bij deze Q&A behorende Good Practice Informatiebeveiliging biedt DNB handvatten waarmee instellingen een praktische invulling kunnen geven aan de beheersmaatregelen op het gebied van *Governance*, *Organisation*, *People*, *Processes*, *Technology*, *Facilities*, *Outsourcing*, *Testing* en de *Risk Management Cycle*. In dat document worden verschillende Good Practices (aanbevelingen voor beheersmaatregelen) gegeven die naar het oordeel van DNB goede invulling geven aan voornoemde vereisten uit art 3.17 Wet Financieel Toezicht, juncto artikel 20 Besluit prudentiële regels en artikel 143 Pensioenwet en artikel 18 Besluit FTK. ■

Deze Q&A is eind 2023 geactualiseerd. Het antwoord is uitgebreid met passages over (onder)uitbesteding, governance & sleutelfuncties, trainingen & opleidingen en een definitie van informatiebeveiliging & cybersecurity.

Relevante wet- en regelgeving

- Wet op het financieel toezicht (Wft)
  - Artikel 1:1; definities
  - Artikel 3:17 eerste lid; beheerste en integere bedrijfsvoering
  - Artikel 3:17 tweede lid; het beheersen van bedrijfsprocessen en bedrijfsrisico's
- Besluit prudentiële regels (Bpr)
  - Artikel 17; onder financiële instelling wordt verstaan ene betaalonderneming, clearingonderneming, entiteit voor risico-acceptatie, kredietonderneming, premie-pensioenonderneming, verzekeraar of bijkantoor
  - Artikel 20, tweede lid; beschikken over procedures en maatregelen om de integriteit, voortdurende beschikbaarheid en beveiliging van geautomatiseerde gegevens te waarborgen
- Pensioenwet
  - Artikel 143, eerste lid; waarborgen beheerste en integere bedrijfsvoering
- Wet verplichte beroepspensioenregeling
  - Artikel 138, eerste lid; waarborgen beheerste en integere bedrijfsvoering*
- Besluit Financieel Toetsingskader Pensioenfondsen
  - Artikel 18; beheerste bedrijfsvoering
- EIOPA
  - EIOPA Richtsnoeren betreffende beveiliging en governance van informatie- en communicatietechnologie
  - EIOPA Richtsnoeren voor uitbesteding aan aanbieders van clouddiensten
  - Regulation on Digital Operational Resilience
- Good practice uitbesteding verzekeraars, uitgave van de Nederlandsche Bank N.V. van augustus 2018
- Guidance uitbesteding door pensioenfondsen, uitgave van de Nederlandsche Bank N.V. van juni 2014

* DNB is van oordeel dat de overeenkomstige toepasselijkheid voor deze (beroeps pensioenfondsen van de algemene norm inzake een zodanige organisatie-inrichting dat deze een beheerste en integere bedrijfsvoering waarborgt, met zich brengt dat ook deze instellingen voor zover van toepassing – dat wil zeggen proportioneel toegepast - dienen te beschikken over procedures en maatregelen om de integriteit, voortdurende beschikbaarheid en beveiliging van geautomatiseerde gegevens te waarborgen.

Begrippenlijst

Term	Definitie
Aanbieder van clouddiensten Cloud service provider	Een dienstverlener die verantwoordelijk is voor het uitvoeren van clouddiensten op grond van een uitbestedingsovereenkomst.
Applicatie	Een hardware- / softwaresysteem dat is geïmplementeerd om aan een bepaalde reeks eisen te voldoen. De term applicatie wordt over het algemeen gebruikt om te verwijzen naar een onderdeel van software dat kan worden uitgevoerd. De termen applicatie en softwareapplicatie worden vaak als synoniemen gebruikt.
Beschikbaarheid	De eigenschap van toegankelijkheid en (tijdige) beschikbaarheid voor gebruik op verzoek voor een bevoegde entiteit.
Bestuur	Het beleidsbepalend of bestuurlijk orgaan van de instelling.
Beveiligingsincident	Een losse gebeurtenis of een reeks met elkaar verbonden gebeurtenissen die niet is gepland en die een nadelig effect heeft of waarschijnlijk zal hebben op de voortdurende beschikbaarheid, integriteit, vertrouwelijkheid en authenticiteit van ICT systemen en diensten.
Beveiligingsmaatregel	Een beveiligingsmaatregel of tegenmaatregel die is ontworpen om de voortdurende beschikbaarheid, integriteit, vertrouwelijkheid en authenticiteit van informatie te beschermen en om te voldoen aan een reeks gedefinieerde beveiligingsvereisten.
Business Continuity Plan (BCP)	Gedocumenteerde informatie die een instelling begeleidt om te reageren op een verstoring en de levering van producten en diensten te voort te zetten, te herstellen en te hervatten in overeenstemming met haar doelstellingen voor bedrijfscontinuïteit.
Clouddienst	Diensten geleverd met behulp van cloudcomputing, dat wil zeggen een model om via het netwerk overal eenvoudig op verzoek toegang te verlenen tot een gedeelde pool van configureerbare ICT-middelen (bijvoorbeeld netwerken, servers, opslagmedia, applicaties en diensten) die met een minimale beheerinspanning of tussenkomst van dienstverleners snel kunnen worden op- en afgeschaald.

Term	Definitie
Cyber aanval	Een aanval, via cyberspace, die zich richt op het gebruik van cyber-space door een instelling met het doel een computeromgeving / -infrastructuur te verstoren, buiten werking te stellen, te vernietigen of kwaadwillig te controleren; of het aantasten van de gegevens of het stelen van informatie.
Cyberdreiging	Elke vorm van kwaadaardige activiteit die probeert informatie-systeembronnen of de informatie zelf te verzamelen, te verstoren, te degraderen of te vernietigen.
Cybersecurity	Voorkomen van schade aan, bescherming van en herstel van computers, elektronische communicatiesystemen, elektronische communicatiediensten, draadloze communicatie en elektronische communicatie, inclusief informatie die daarin is opgenomen, om de voortdurende beschikbaarheid, integriteit, vertrouwelijkheid, authenticiteit en onweerlegbaarheid ervan te waarborgen.
Datalek	Toegang tot of vernietiging, wijziging of vrijkomen van (vertrouwelijke) gegevens bij een instelling, zonder dat dit de bedoeling is van deze instelling.
Dienstverlener	Een derde partij die een proces, dienst of activiteit, of onderdelen daarvan, verricht op grond van een uitbestedingsovereenkomst.
End User Computing	De mogelijkheid voor eindgebruikers om zelf hun eigen informatie-systemen te ontwerpen, te implementeren en daarmee data van de instelling in te zien of te bewerken.
ICT asset	Een ICT-asset omvat hardware, softwaresystemen of informatie en waarden van een organisatie.

Term	Definitie
ICT-concentratierisico	Een blootstelling aan individuele of aan meerdere onderling verbonden cruciale derde aanbieders van ICT-diensten, waardoor een bepaalde mate van afhankelijkheid ten aanzien van deze aanbieders ontstaat, zodat de onbeschikbaarheid, het falen of een ander soort tekortkoming van deze laatste het vermogen van een financiële entiteit, en uiteindelijk van het financiële stelsel van de Unie in zijn geheel, om cruciale functies te vervullen of om andere soorten nadelige effecten, waaronder grote verliezen, op te vangen, in gevaar kan brengen.
ICT-infrastructuur	Alle ICT-voorzieningen (hardware, middleware en software waaronder applicaties, database, operating system, netwerk, interface etc) die nodig zijn binnen een organisatie, als ondersteuning van de verschillende bedrijfsprocessen.
Informatiebeveiliging	Processen gericht op het behoud van de voortdurende beschikbaar-heid, integriteit, vertrouwelijkheid en authenticiteit van informatie en/of informatiesystemen. Tevens kan het gaan om andere eigenschappen, zoals verantwoording, onweerlegbaarheid en betrouwbaarheid.
Integriteit	De eigenschap van nauwkeurigheid, volledigheid en tijdigheid.
Kritiek of belangrijk systeem / proces	Indien de betreffende functie, activiteit of systeem van essentieel belang is voor de bedrijfsvoering van de instelling in de zin dat de instelling zonder deze functie, activiteit of ICT systeem niet in staat zou zijn om haar diensten aan haar klanten (polishouders, deelnemers) te verlenen.
Kroonjuwelen analyse	Een proces voor het identificeren van die ICT-assets die het meest cruciaal zijn voor het vervullen van de missie van een organisatie danwel die assets die door een criminele actor als waardevol wordt gezien, zoals specifieke Data, Applicaties, Assets en Services (DAAS).
Kwetsbaarheid	Een zwakte, gevoeligheid of tekortkoming in een actief systeem, proces of controle die door een dreiging kan worden misbruikt.
Legacy ICT-systeem	Een ICT-systeem dat het einde van zijn levenscyclus (end-of-life) heeft bereikt en niet geschikt is voor upgrades of fixes, om technologische of commerciële redenen, of niet langer ondersteund wordt door de leverancier of door een externe ICT dienstverlener, maar die nog steeds in gebruik is en de functies van de financiële entiteit ondersteunt.
Metrics	Meetinstrumenten die op basis van informatie verzameld vanuit de bedrijfsinfrastructuur en -processen kan aantonen of de beveiligings-maatregelen naar wens functioneren en het risico zoals verwacht mitigeren.
Ransomware	Schadelijke software die de databestanden van de instelling versleutelt, met als doel om deze later te ontsleutelen in ruil voor losgeld. Ransomware kan ook de beschikbaarheid of toegang tot ICT-systemen beperken door systeembestanden te versleutelen die essentieel zijn voor de goede werking van het systeem.
Recovery Point Objective (RPO)	Herstelpuntdoelstelling. RPO is het streven om te voldoen aan de afgesproken maximaal toelaatbare hoeveelheid dataverlies na een disruptie door de afdeling ICT en/of een dienstverlener. RPO is verwant aan RTO, beide zijn tijdsintervallen.
Recovery Time Objective (RTO)	*Hersteltijddoelstelling* en is het streven om te voldoen aan de afgesproken hersteltijd na een disruptie (bijv. een technische storing of cyberaanval) door de afdeling ICT en/of een ICT dienstverlener.
Systeem / ICT systeem	Set van applicaties, services, ICT-assets of andere informatiebehandelingscomponenten, waaronder de besturingsomgeving.
Uitbesteding	Een overeenkomst van - om het even welke vorm - tussen een instelling en een al dan niet onder toezicht staande dienstverlener op grond waarvan deze dienstverlener hetzij rechtstreeks, hetzij door middel van onder-uitbesteding een proces, een dienst of een activiteit uitvoert die anders door de instelling zelf zou worden uitgevoerd.
Uncompromisable backup	Een back-up van uw gegevens die op geen enkele manier kan worden gewijzigd of verwijderd, zelfs niet door systeembeheerders of door de gebruikers, applicaties of systemen die de gegevens hebben gemaakt.
Vertrouwelijkheid	De eigenschap dat informatie niet beschikbaar wordt gesteld aan of verstrekt aan niet geautoriseerde personen, entiteiten, processen of systemen.

Aandachtspunten voor alle controls

Risico gebaseerd

Een adequate beheersing van informatiebeveiliging betekent optimale effectiviteit van de controls/beheersmaatregelen die een instelling toepast. Deze effectiviteit wordt onder andere bereikt door een goed zicht op het eigen interne en externe dreigings-beeld. Met een analyse van de risico's die in het dreigingsbeeld zijn geïdentificeerd[1], bepaalt de instelling periodiek *haar risico acceptatie* en welke beheersmaatregelen op welke wijze effectief voor haar zijn. Voor het monitoren van bronnen van dreigingsinformatie door de instelling zijn verantwoordelijkheden intern aangewezen en bestaan er procedures hoe dreigingsinformatie wordt ontvangen en intern wordt gedeeld ter afhandeling. De instelling identificeert ook periodiek welke dienstverleners relevant zijn om te betrekken bij de monitoring en het uitwisselen van dreigings-informatie en heeft daarvoor afspraken gemaakt met deze partijen. Deze risico-gebaseerde aanpak per control/beheers-maatregel biedt de instelling de mogelijkheid om steeds verder-gaand maatwerk ten aanzien van haar informatiebeveiliging toe te passen alsmede een proportionele benadering te hanteren. Hierbij heeft de inzet op kwaliteit van beheersmaatregelen de voorkeur boven kwantiteit van beheersmaatregelen. Inzicht in de belangrijkste middelen (*key assets*), de belangrijkste controls (*key controls*) en daar waar relevant het opzetten van metrics die zekerheid kunnen bieden aan het toezicht dat de belangrijkste beheersmaatregelen wel degelijk het verwachte effect hebben op de risicobeperking zijn daarbij essentieel.

Three lines Model

Financiële instellingen zorgen voor een passende scheiding en onafhankelijkheid van ICT-risicobeheer functies, controlefuncties en interne auditfuncties, volgens de regels van het 'three lines model' of een vergelijkbaar intern risicobeheersings- en controle-model[2]. Bij elke control is het van belang de taakverdeling en verantwoordelijkheid tussen de three lines te definiëren: *Hoe zijn per control de taken en verantwoordelijkheden tussen de eerste de tweede en derde lijn verdeeld?*
Waarbij voor de de derde lijn geldt dat zij onafhankelijk is gepositioneerd, rapporteert en zelf haar audit programma risk based bepaalt.

Kennis en competenties en Assurance

Het belang van kennis en aandacht op het gebied van infor-matiebeveiliging en cyberrisico's wordt aan veel bestuurstafels onderschreven. Bestuurlijke verankering van het hele stelsel aan controls en het op orde brengen en houden van kennis bij bestuurders en intern toezicht behoeft nadrukkelijke aandacht. Het bestuur, raad van toezicht, raad van commissarissen en sleutelfunctiehouders hebben aantoonbaar op hen toegesneden trainingen en opleidingen gevolgd om de belangrijkste ICT-risico's en beheersmaatregelen voor hun instelling te kunnen begrijpen en adresseren.

Vormen van assurance vanuit externe ICT-Auditors ten aanzien van de afzonderlijke controls en hun context in het hele stelsel van informatiebeveiligingsmaatregelen kunnen ook bij uitbestede activiteiten ten aanzien van de Good Practice Informatie-beveiliging waarborgen geven aan bestuurders, raden van toezicht en raden van commissarissen. Voorbeelden daarvan zijn Richtlijn 3000 rapportages, een SOC 2 rapportage alsmede een recent uitgebrachte standaard van NOREA over het IT verslag en de ICT-Audit verklaring[3]. ▶

1 Risico = waarschijnlijkheid X impact, waarschijnlijkheid = dreiging X kans.
2 Zie ook: Operationeel onafhankelijke en proportionele inrichting van sleutelfuncties (dnb.nl) en Sleutelfuncties en adequate functiescheiding (dnb.nl)
3 https://www.norea.nl/nieuws/nieuw-de-it-auditverklaring en Microsoft Word - NOREA Reporting on Management of ICT - v0.11 MASTER.docx

Uitbesteding

De instelling is eindverantwoordelijk voor de beheersing van de informatiebeveiliging en cybersecurity risico" van al haar uitbestede activiteiten en functies in de uitbestedingsketen. Dit betekent dat het noodzakelijk is dat de instelling aantoonbaar de effectieve werking en de uitvoering van alle 58 controls monitort en controleert inclusief waar deze deels of geheel plaatsvinden bij dienstverleners c.q. in de uitbestedingsketen.

Voor alle 58 controls geldt

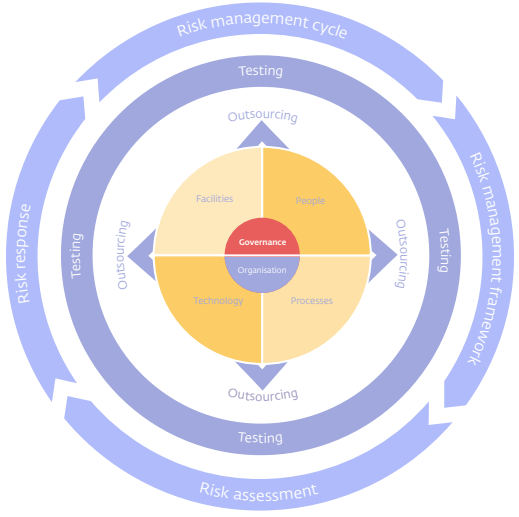
Bij het toepassen van alle 58 controls zoals die in deze Good Practice Informatiebeveiliging zijn beschreven, adresseren de instellingen expliciet de volgende aandachtspunten.
Bij **elke** control:

- Wordt de effectiviteit van de control periodiek geoptimaliseerd aan de hand van de risicoanalyse die uit het interne en externe dreigingsbeeld naar voren is gekomen en metrics die de werking van de controls aantonen. Daarbij is ook betrokken de ervaring die is opgedaan met de betreffende control en de plaats die de control inneemt in de hele set van informatie-beveiliging controls.
- Worden taken en verantwoordelijkheden en de formele rapportagelijnen van de 1e, 2e, en 3e lijnfunctie van de in de control genoemde onderdelen van de Good Practices belegd. Dit wordt ook gedaan in het geval van uitbestede activiteiten.
- Maakt de instelling met dienstverleners, aan wie activiteiten zijn uitbesteed, afspraken over een duidelijke verdeling van taken en verantwoordelijkheden. Bij iedere control maakt de instelling risicogebaseerd afspraken met de dienstverleners over de performance en het niveau van de interne beheersing. Deze afspraken werken ook door naar eventuele onderaan-nemers verderop in de keten.
- Monitort en controleert de instelling aantoonbaar de naleving van de gemaakte afspraken met en door haar dienstverleners met de juiste scope en diepgang. Dit doet zij aan de hand van rapportages of dashboards over de naleving van de Service Level afspraken en het niveau van de interne beheersing, inclusief de effectieve werking conform de gestelde volwassen-heidsniveaus (zoals assurance en audit rapportages).
- De instelling stelt bij het ontvangen van assurance rapportages en/of audit rapportages vast dat deze qua diepgang, scope en assurance niveau (zoals Type I versus Type II; ISO certificering vs ISAE/SOC) aansluit bij die maatregelen uit de 58 benoemde controls, waarvan een deel of de gehele uitvoering bij de dienstverlener plaatsvindt. Indien deze rapportages niet de scope van de betreffende maatregelen afdekken, heeft dat mogelijk gevolgen voor de mate waarin de instelling aantoonbaar de effectieve werking (van minimaal 6 maanden) van één of meer controls in de keten kan aantonen, met als gevolg dat het volwassenheidsniveau niet kan worden onderbouwd.
- Stuurt de instelling bij wanneer haar risicotoleranties door de uitbesteding worden overschreden, bijvoorbeeld wanneer er afwijkingen zichtbaar zijn in de rapportages of dashboards (zie *Risk Management cycle*) of wanneer het dreigingslandschap daartoe noodzaakt.

Bij het uitvoeren van self-assessments en het aanleveren van evidence voor het bepalen van de volwassenheidsniveaus neemt de instelling per control mee hoe zij uitvoering heeft gegeven aan de aandachtspunten met betrekking tot de onderwerpen 'Risicogebaseerd' en het 'Three lines model' of een vergelijkbaar intern risicobeheersings- en controlemodel.

Ten aanzien van de aandachtspunten voor uitbesteding kan gekozen worden om per control de impact van de uitbesteding vast te stellen. Op basis daarvan kunnen de beheersmaatregelen van de dienstverlener mee worden gewogen in de bepaling van het volwassenheidsniveau van de control. Verder is het goed gebruik om in een separaat document voor de belangrijkste dienstverleners aan te tonen welke volwassenheidsniveaus zijn bepaald ten aanzien van de controls waarop de uitbestede activiteiten impact hebben. ■

Governance



In dit onderdeel treft u een korte samenvatting aan van de beheersmaatregelen voortkomend uit markt-standaarden die bij het element Governance horen met bijbehorende Good Practices. Aan het einde van dit onderdeel staan 'links' waarop kan worden door-geklikt naar de beheersmaatregelen.

DNB verstaat onder dit element

Governance gaat over het op basis van een risicoanalyse geven van strategische, tactische en operationele sturing aan informatie-beveiliging en cybersecurity in overeenstemming met de strategie van de instelling, de doelen uit de ICT-strategie, haar risicobereid-heid en wet- en regelgeving. Hierbij wordt rekening gehouden met de aard, omvang en complexiteit van de instelling.

Goede voorbeelden van Governance beheersmaatregelen voor de instelling

Bij het element *Governance* maakt een instelling op basis van een actuele risicoanalyse en dreigingsbeeld een digitale operationele weerbaarheid strategie op korte, middellange en lange termijn.
In lijn met de digitale operationele weerbaarheid strategie, wordt verder periodiek het informatiebeveiligingsbeleid vastgesteld, uitgevoerd en gemonitord inclusief het daaruit volgend informatiebeveiligingsplan.
Het beleid omvat een omschrijving van de belangrijkste taken, verantwoordelijkheden en formele rapportagelijnen inzake informatiebeveiligingsbeheer. Het beleid zet de vereisten voor budget, personeel, processen en technologie met betrekking tot informatiebeveiliging uiteen, waarbij medewerkers op alle niveaus verantwoordelijkheid dragen om de informatiebeveiliging van de instelling te waarborgen.

De instelling heeft in het beleid nadrukkelijk aandacht gegeven aan de weerbaarheid tegen cyberdreigingen. Het beleid is geoperationaliseerd in zowel preventieve, detecterende, corrigerende als repressieve beheersmaatregelen. Daarbij monitort de instelling relevante ontwikkelingen op het gebied van informatiebeveiliging en cybersecurity waaronder ook de ontwikkelingen op het gebied van Quantum technologie, AI, blockchain en technologische kennis. De instelling let erop dat bedrijfsprocessen en ICT-systemen zijn opgezet volgens een door de instelling vastgestelde informatiearchitectuur. Deze Security Architectuur maakt inzichtelijk hoe de ICT-systemen en dataverzamelingen ondersteunend zijn aan de strategie van de instelling en haar processen. Daarbij zijn alle relevante ICT- en beveiligingsrisico's waaraan de instelling is blootgesteld, geïdentificeerd en gemeten. De geïdentificeerde bedrijfsprocessen en -activiteiten, bedrijfsfuncties, rollen en assets (zoals informatie- en ICT-assets) worden daarna ingedeeld op hoe kritiek ze zijn.

De instelling maakt daarbij gebruik van een classificatieschema[4] op basis waarvan relevante beheersmaatregelen zijn getroffen voor bijvoorbeeld toegang, versleuteling, opslag en retentie van gegevens. ▶

4 ICT-systemen en data zijn op een basis van een risicoanalyse ingedeeld in categorieën die de mate van voortdurende beschikbaarheid, integriteit en vertrouwelijkheid (BIV) aangeeft.

De instelling werkt volgens geaccepteerde (technische) standaarden op het gebied van informatiebeveiliging en cybersecurity.

Rol van het bestuur bij de implementatie van deze beheersmaatregelen

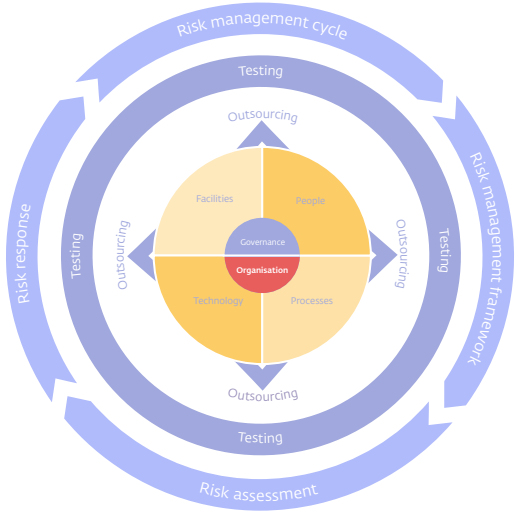
Het bestuur van de instelling is eindverantwoordelijk voor een adequate governance en ziet erop toe dat alle elementen van informatiebeveiliging en cybersecurity zijn beheerst. U kunt hierbij bijvoorbeeld denken aan de volgende aspecten:

- Op basis van een risicoanalyse en dreigingsbeeld stelt het bestuur een digitale operationele weerbaarheid strategie op korte, middellange en lange termijn vast.
- Het bestuur draagt de eindverantwoordelijkheid om, in lijn met de digitale operationele weerbaarheid strategie, periodiek het informatiebeveiligingsbeleid vast te stellen inclusief het daaruit volgend informatiebeveiligingsplan.
- Het bestuur overziet en neemt de verantwoordelijkheid dat het vastgestelde informatiebeveiligingsbeleid en informatie-beveiligingsplan worden uitgevoerd, gemonitord en waar nodig aangepast.
- Vervolgens zorgt het bestuur er binnen de *Risk Management Cycle* voor dat periodiek in het bestuur wordt nagegaan in hoeverre de informatiebeveiligings- en cybersecurity risico's van de instelling passen binnen de risicobereidheid van het bestuur. Hierbij kan worden afgewogen in hoeverre een effectieve mix van beheersmaatregelen – *People*, *Processes*, *Technology* en *Facilities* – is getroffen om risico's van de instelling te beheersen.
- Het bestuur waarborgt dat het governancesysteem van de instelling, in het bijzonder het risicobeheer- en het interne-controlesysteem, de beveiligingsrisico's van de instelling op adequate wijze beheert.
- Het bestuur en risk management zijn bekend met de belangrijkste ontwikkelingen en nemen de risico's en kansen daarvan mee in hun besluitvorming respectievelijk risicobeoordeling.
- Het bestuur ziet erop toe dat de instelling monitort dat haar dienstverleners afspraken nakomen in overeenstemming met het informatiebeveiligingsbeleid en – indien van toepassing – de uitvoering van het informatiebeveiligingsplan.
- Het bestuur monitort de resultaten van de relevante metrics die het goed functioneren van de beheersmaatregelen weergeeft en reageert adequaat indien deze zouden afwijken met een mogelijke materiële impact op het bedrijfsrisico. ■

Beheersmaatregelen:

- > 1.1 Information Security plan
- > 1.2 Information Security policies and procesmanagement
- > 2.1 Information Security Architecture
- > 2.2 Data classification scheme
- > 3.1 Risks and opportunities of future trends and regulations
- > 3.2 Technical standards

Organisation



In dit onderdeel treft u een korte samenvatting aan van de beheersmaatregelen voortkomend uit markt-standaarden en Good Practices die horen bij het element 'Organisation'.
Aan het einde van dit element staan 'hyperlinks' waarop kan worden doorgeklikt naar de beheers-maatregelen.

DNB verstaat onder dit element

De taken ten aanzien van informatiebeveiliging en cybersecurity zijn eenduidig binnen de instelling belegd en activiteiten op dit gebied zijn in overeenstemming met de strategie van de instelling, haar risicobereidheid en met wet- en regelgeving.

Goede voorbeelden van Organisation beheersmaatregelen voor de instelling

Bij het element *Organisation* documenteert en formaliseert de instelling de rollen en verantwoordelijkheden voor de risico-beheer- en informatiebeveiligingsfunctie. De instelling heeft taken, verantwoordelijkheden en bevoegdheden ten aanzien van informatiebeveiliging belegd op alle niveaus in de organisatie.
De instelling heeft daarbij bijvoorbeeld gedragsregels opgesteld en gecommuniceerd waarin staat dat medewerkers zorgvuldig omgaan met informatie (zoals veilig omgaan met wachtwoorden, e-mail en een clean desk policy).

De instelling zet, binnen haar governancesysteem en in overeen-stemming met het evenredigheidsbeginsel, een informatie-beveiligingsfunctie op, waarbij de verantwoordelijkheden zijn toegewezen aan een specifieke medewerker.
De instelling zorgt dat de onafhankelijkheid en objectiviteit van deze informatiebeveiligingsfunctie is gewaarborgd door deze op passende wijze te scheiden van verantwoordelijkheden inzake ICT-activiteiten en bedrijfsvoering.
De informatiebeveiligingsfunctie rapporteert aan het bestuur.

Het eigenaarschap van alle gegevens en informatiesystemen die de instelling gebruikt bij haar bedrijfsvoering, zijn eenduidig belegd. De instelling heeft de toegang tot gegevens en informatie-systemen door middel van toegangsrechten beheerst. Hierbij wordt gebruik gemaakt van de principes van functiescheiding gebaseerd op de inrichting van de administratieve organisatie/ interne controle van de instelling.

De instelling heeft daarbij bijvoorbeeld, op basis van een risico gebaseerde benadering, niet alleen de gewenste functie-scheidingen per applicatie in kaart gebracht, maar nadrukkelijk ook per proces indien dit proces wordt ondersteund door meerdere applicaties. Dit voorkomt dat functiescheidingen op procesniveau kunnen worden doorbroken, terwijl deze per individuele applicatie in het proces wel conform de eisen zijn ingericht. Tegelijkertijd brengen instellingen de accounts met hoge rechten terug tot een minimaal noodzakelijk aantal. Met een dergelijke aanpak kunnen ongewenste functievermengingen (toxic combinations) en de daarmee samenhangende risico's, worden gereduceerd. ▶

Rol van het bestuur bij de implementatie van deze beheersmaatregelen

Het bestuur van de instelling is eindverantwoordelijk voor een adequate organisatie van taken, verantwoordelijkheden en bevoegdheden en ziet erop toe dat alle elementen van informatie-beveiliging en cybersecurity zijn beheerst. U kunt hierbij bijvoorbeeld denken aan de volgende aspecten:

- Het bestuur heeft taken en verantwoordelijkheden op het gebied van het inrichten, beheren en controleren van informatiebeveiliging en cybersecurity helder belegd.
- Het bestuur ziet er op dat ongewenste functievermengingen (toxic combinations) en de daarmee samenhangende risico's door de instelling worden vermeden.
- Op grond van het risicoprofiel van de instelling en de risico-bereidheid van het bestuur, kan de organisatie beschikken over voldoende capaciteit, kennis en ervaring om invulling te geven aan deze taken en verantwoordelijkheden.
- Het bestuur draagt actief en zichtbaar het belang uit van informatiebeveiliging en cybersecurity voor de instelling en haar dienstverleners.
- Het bestuur ziet erop toe dat de instelling monitort dat haar dienstverleners afspraken nakomen over het beleggen van taken en verantwoordelijkheden voor informatiebeveiligings- en cybersecurity, eigenaarschap van gegevens en informatie-systemen en functiescheiding in hun organisaties.
- Het bestuur ziet erop toe dat de CISO voldoende autonoom kan handelen, voldoende middelen heeft en rechtstreekse communicatielijnen naar het bestuur heeft. ■

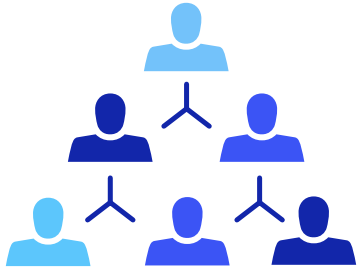
Beheersmaatregelen:

> 5.1 Responsibility for risk, security, compliance and Information Security function

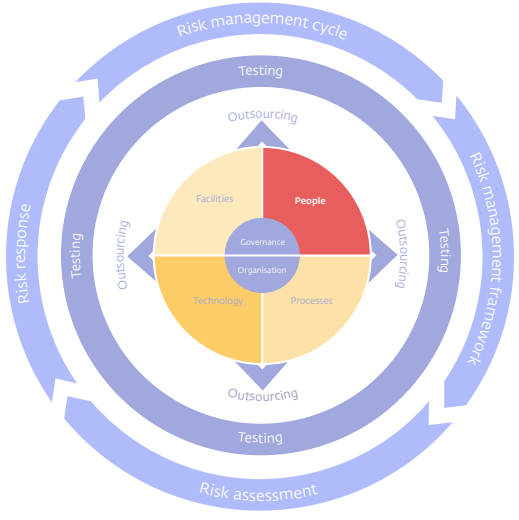
> 5.2 Management of information security and tasks of the information security function

> 6.1 Data and system ownership

> 7.1 Segregation of duties



People and Knowledge



In dit onderdeel treft u een korte samenvatting aan van de belangrijkste beheersmaatregelen voort-komend uit marktstandaarden en Good Practices die horen bij het element 'People'.
Aan het einde van dit element staan 'hyperlinks' waarop kan worden doorgeklikt naar de beheers-maatregelen.

DNB verstaat onder dit element

Alle medewerkers, externe inhuur en dienstverleners zijn bekend met het informatiebeveiligingsbeleid van de instelling, kennen hun verantwoordelijkheden en kunnen werken volgens dit beleid en de risicotoleranties van de instelling.

Goede voorbeelden van People beheers-maatregelen voor de instelling

Het belang van kennis en aandacht op het gebied van informatie-beveiliging en cyberrisico's wordt aan veel bestuurstafels onder-schreven. Bestuurlijke verankering van het hele stelsel aan controls en het op orde brengen en houden van kennis bij bestuurders en intern toezicht behoeft nadrukkelijke aandacht.

De menselijke factor is zeer bepalend voor de beheersing van de informatiebeveiliging en cybersecurity risico's. Bij *People* trekt de instelling medewerkers aan met kennis van informatiebeveiliging en cybersecurity die aansluit bij de ambitie en het risicoprofiel van de instelling en besteedt aandacht aan het behoud daarvan.

De instelling investeert in het op peil houden van het kennisniveau en de competenties van de medewerkers door middel van opleidingen en trainingen. Basiskennis van informatiebeveiliging en cyberdreigingen wordt breed binnen de instelling gedeeld.

Verdiepende kennis wordt aangereikt aan ICT-beheerders en informatiebeveiligings-specialisten. Met security awareness programma's besteedt de instelling expliciet aandacht aan cyberdreigingen. Hierbij is aandacht voor het belang van (permanente) educatie op het gebied van cybersecurity.

De instelling deelt kennis over cyberdreigingen met andere instellingen en instanties. De instelling participeert daarbij bijvoorbeeld in gremia waarin cyberdreigingen en cyberaanvallen vertrouwelijk worden gedeeld, zoals de sectorale Information Sharing and Analysis Centers (ISAC's).

De instelling bepaalt verder op grond van een risicoanalyse waar haar afhankelijkheid van individuen met kennis van informatie-beveiliging en cybersecurity haar risicotolerantie overschrijdt. De instelling treft beheersmaatregelen om te grote afhankelijkheid van individuen te beperken (key person risk).

Voorafgaand aan de indiensttreding, screened de instelling interne- en externe medewerkers afhankelijk van het risicoprofiel van de functie. Tijdens het dienstverband of langdurende inhuur-periode wordt deze screening periodiek herhaald.Bij functie-wijzigingen worden toegangsrechten waarover de medewerker of inhuurkracht uit hoofde van de (nieuwe) functie of bij beëindiging ▶

van de (oude) functie niet meer mag beschikken, zo snel mogelijk ingetrokken.

De instelling brengt bij hoge impact incidenten door middel van root cause analyses in kaart in hoeverre de cultuur cq de gedragingen van bepaalde medewerkers (bijvoorbeeld slordigheden, ontevreden (disgrunteld) employees) binnen bepaalde afdelingen heeft bijgedragen aan het incident. Naar aanleiding van deze analyse worden mitigerende beheersmaatregelen ingericht.

Rol van het bestuur bij de implementatie van deze beheersmaatregelen

Het bestuur van de instelling is eindverantwoordelijk voor het zorgdragen voor een passend kennisniveau van medewerkers en ziet erop toe dat alle elementen van informatiebeveiliging en cybersecurity zijn beheerst. U kunt hierbij bijvoorbeeld denken aan de volgende aspecten:

- Het bestuur, raad van toezicht, raad van commissarissen en sleutelfunctiehouders hebben aantoonbaar op hen toegesneden trainingen en opleidingen gevolgd om de belangrijkste ICT-risico's en beheersmaatregelen voor hun instelling te kunnen begrijpen en adresseren.
- Het bestuur vertoont goed voorbeeldgedrag ten aanzien van bewustzijn voor risico's op het gebied van informatiebeveiliging en cybersecurity en het naleven van procedures die de informatiebeveiliging borgen (tone-at-the-top).
- Zogeheten 'management overrides' van bestaande processen en procedures door het bestuur en senior management worden waar mogelijk vermeden.
- Het bestuur ziet erop toe dat de instelling monitort dat haar dienstverleners afspraken nakomen ten aanzien van de personele aspecten van informatiebeveiliging en cybersecurity zoals hierboven genoemd. ■

Beheersmaatregelen:

> 8.1 Personnel recruitment and retention

> 8.2 Personnel competencies and culture

> 8.3 Dependence upon individuals

> 8.4 Personnel clearance procedures

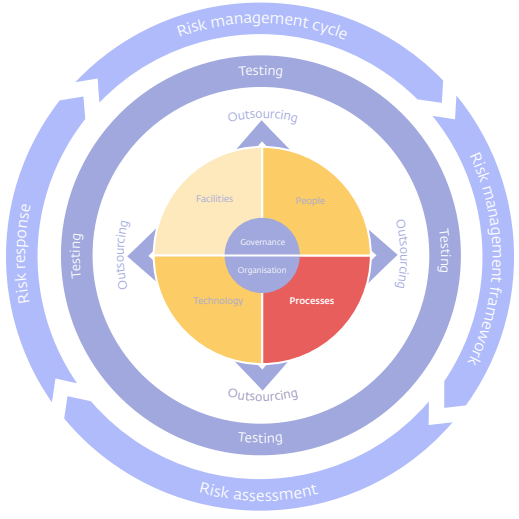
> 8.5 Job change and termination

> 9.1 Knowledge transfer to end users

> 9.2 Knowledge transfer to operations and support staff

> 9.3 Employee awareness

Processes



In dit onderdeel treft u een korte samenvatting aan van de belangrijkste beheersmaatregelen voort-komend uit marktstandaarden en Good Practices die horen bij het element 'Processes'.
Aan het einde van dit element staan 'hyperlinks' waarop kan worden doorgeklikt naar de beheers-maatregelen.

DNB verstaat onder dit element

Processen geven richting aan een beheerste bedrijfsvoering en zijn noodzakelijk bij de beheersing van de risico's op het gebied van informatiebeveiliging en cybersecurity.

Goede voorbeelden van Processes beheersmaatregelen voor de instelling

Bij het onderdeel *Processes* is het van belang dat de instelling een ICT-continuïteitsplan, gebaseerd op een reeks van verschillende scenario's, ontwikkelt en bijhoudt. Dit met als doel om de impact van een grote verstoring op de belangrijkste bedrijfsfuncties en -processen te beperken en de ongestoorde voortzetting van informatiebeveiligingsfuncties tijdens verstoringen of cyber-aanvallen te bevorderen. De instelling heeft als doel de schade uit beveiligingsincidenten, waaronder cybersecurity incidenten zoveel mogelijk te beperken en herhaling te voorkomen. De instelling beschikt daartoe over een geformaliseerd beleid voor incident-beheer, waarin een escalatieprocedure en escalatiecriteria zijn opgenomen. De instelling zorgt daarbij dat ze doeltreffende crisiscommunicatie beheersmaatregelen treft. Cybersecurity incidenten worden daarbij conform geldende regels gerapporteerd aan de autoriteiten. Oplossingen voor incidenten worden regel-matig geanalyseerd om processen en ICT-systemen te verbeteren. Een voorbeeld hierbij is het oprichten van een Computer Security Incident Reponse Team (CSIRT) binnen de instelling.

Als onderdeel van een solide beheer van de bedrijfscontinuïteit voert de instelling een business impact analyse uit om de bloot-stelling te beoordelen van de instelling aan ernstige bedrijfsonder-brekingen en de potentiële gevolgen ervan, zowel kwantitatief als kwalitatief, met behulp van interne en/of externe gegevens en scenarioanalyse. De business impact analysis houdt rekening met hoe kritiek de geïdentificeerde bedrijfsprocessen en -activiteiten hun onderlinge afhankelijkheden zijn.
De instelling zorgt ervoor dat hun ICT-systemen en ICT-diensten ontworpen en afgestemd zijn op hun business impact analysis.

In de business impact analysis en het ICT-continuïteitsplan zijn verschillende scenario's opgenomen waarbij rekening is gehouden met de continuïteit van de beveiligingsmaatregelen en de ongestoorde voortzetting van informatiebeveiligingsfuncties tijdens verstoringen en cyberaanvallen. Crisismanagement is ingericht, inclusief de daarbij behorende communicatieprotocollen. Alternatieve verwerkings- en herstelmogelijkheden voor alle kritieke ICT-services zijn in het ICT-continuïteitsplan voorhanden. Bij een storing of noodsituatie, en tijdens de uitvoering van de bedrijfscontinuïteit plannen, zorgt de instelling ervoor dat ze doeltreffende crisiscommunicatie maatregelen treft. Daarbij zijn alle relevante interne en externe belanghebbenden, waar-onder relevante toezichthoudende autoriteiten, tijdig op de hoogte gebracht. ▶

De instelling heeft op beheerste wijze wijzigingen doorgevoerd met als doel om te voorkomen dat deze wijzigingen (bedoeld of onbedoeld) leiden tot een lager informatiebeveiligingsniveau, leiden tot verstoringen in de bedrijfsprocessen en/of de data-integriteit negatief beïnvloeden. Wijzigingen, inclusief security patches, in ICT-applicaties, ICT-infrastructuur, ICT-processen en kritieke systeeminstellingen volgen een gestandaardiseerd en gecontroleerd pad, waarbij wijzigingen worden geregistreerd (audit trail) geaccordeerd en geëvalueerd. Dit geldt ook voor ICT-systemen die door eindgebruikers worden ontwikkeld en beheerd. De instelling houdt een register bij van de end user computing toepassingen die kritieke bedrijfsfuncties of -processen ondersteunen.

De instelling stelt criteria op voor het beschermen van test-gegevens en onderhoudt deze. Hierbij worden test- en productie-gegevens goed van elkaar gescheiden. Wijzigingen worden getest volgens een testplan waarin acceptatiecriteria zijn opgenomen; ook voor beveiliging en ICT-performance.

De instelling borgt de kwaliteit van de ICT-beheerprocessen. Daarbij implementeert en onderhoudt de instelling procedures met betrekking tot onder meer:

- configuratie (het bijhouden van de ICT-systemen die de instelling gebruikt en de verschillende parameters daarin),
- back-up en herstel van systemen en data,
- beschikbaarheid van (backup) gegevens op een externe locatie,
- de opslag, archivering en vernietiging van gegevens conform wet- en regelgeving,
- het verwijderen, overdragen, verwerken en verstrekken van gevoelige gegevens,
- compliance met huidige wet- en regelgeving,
- toegang tot informatiesystemen en data van de instelling.

De instelling verkrijgt periodiek onafhankelijke assurance over het functioneren van de beheersmaatregelen. Bijvoorbeeld in de vorm van een rapportage van de interne of externe auditor waarin een oordeel is gegeven over de opzet, bestaan en werking van beheersmaatregelen gedurende een bepaalde periode.

De instelling heeft procedures voor logische toegangscontrole of logische beveiliging (identiteits- en toegangsbeheer). Daarbij wordt de toegang (al dan niet op afstand) tot kritieke ICT-systemen alleen toegekend volgens kennisnemingsbehoefte en wanneer er sterke authenticatiemiddelen worden gebruikt.

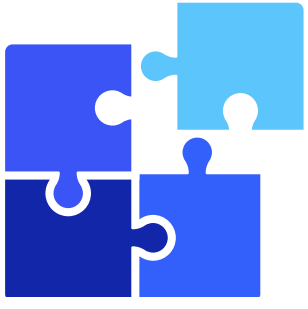
Rol van het bestuur bij de implementatie van deze beheersmaatregelen

Het bestuur van de instelling is eindverantwoordelijk voor het zorgdragen en/of controleren dat de strategie en het overall ICT-security plan in lijn is met de richtlijnen van het bestuur en de overige bedrijfsprocedures. U kunt hierbij bijvoorbeeld denken aan de volgende aspecten:

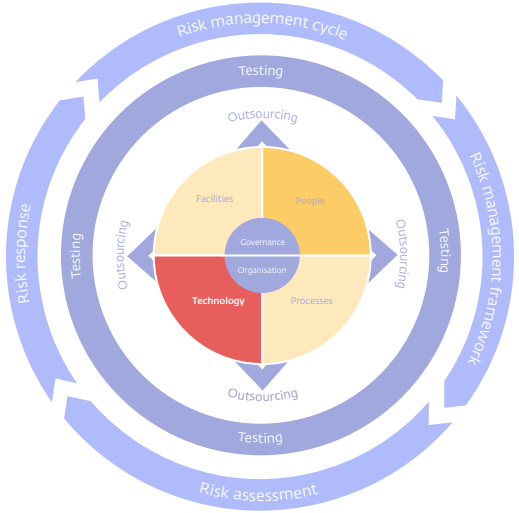
- Het bestuur is verantwoordelijk voor het vaststellen en goedkeuren van een business impact analysis en een daaruit voortvloeiend continuïteitsplan om de impact van een grote verstoring op de belangrijkste bedrijfsfuncties en -processen te beperken.
- Het bestuur controleert jaarlijks of de business impact analysis en het -continuïteitsplan actueel zijn. Het bestuur ziet erop toe dat belangrijke wijzigingen in ICT-systemen of dienstverlening direct in het continuïteitsplan worden verwerkt.
- Het bestuur is betrokken bij het opstellen van de continuïteits-plannen en neemt actief deel aan het testen van het ICT continuïteitsplan.
- De rapportage van de beveiligingsmonitoring geeft de instelling inzicht in de aard van zowel operationele als veiligheidsincidenten om het bestuur in staat te stellen passende beslissingen te nemen.
- Het bestuur facilteert onafhankelijk toezicht, geeft periodiek goedkeuring aan internal (ICT) audit plannen, ICT audits en materiële wijzigingen daarin.
- De instelling geeft aan het bestuur inzicht in het goed functioneren van de beheersmaatregelen door daar waar relevant metrics te genereren die gevoed worden met gegevens uit de infrastructuur en processen. ■

Beheersmaatregelen:

- > 10.1 Change standards and procedures
- > 10.2 Impact assessment, prioritisation and authorisation
- > 10.3 Test environment
- > 10.4 Testing of changes
- > 10.5 Promotion to Production
- > 11.1 ICT Business impact analysis and ICT Continuity plans
- > 11.2 Testing of the ICT Continuity plan
- > 11.3 Uncompromisable backup storage
- > 11.4 Restoration
- > 12.1 Storage and retention arrangements
- > 12.2 Disposal
- > 12.3 Security requirements for data management
- > 13.1 Configuration repository and baseline
- > 13.2 Identification and maintenance of configuration items
- > 15.1 Security incident policy and definition
- > 15.2 Incident escalation
- > 16.1 Security testing, surveillance and monitoring
- > 16.2 Monitoring of internal control framework
- > 16.4 Evaluation of compliance with external requirements
- > 16.5 Independent assurance
- > 17.1 Identity & Access Management
- > 17.2 User account management



Technology



In dit onderdeel treft u een korte samenvatting aan van de belangrijkste beheersmaatregelen voort-komend uit marktstandaarden en Good Practices die horen bij het element 'Technology'.
Aan het einde van dit element staan 'hyperlinks' waarop kan worden doorgeklikt naar de beheers-maatregelen.

DNB verstaat onder dit element

Informatiebeveiliging en cybersecurity krijgen mede vorm door het treffen van technische beheersmaatregelen.

Goede voorbeelden van Technology beheersmaatregelen voor de instelling

Bij het element *Technology* zijn technische beheersmaatregelen zodanig ingericht dat zij een hoog niveau van voortdurende beschikbaarheid, integriteit, vertrouwelijkheid en authenticiteit waarborgen. Daarbij houden risicoanalyses van de instelling rekening met actuele cyberdreigingen. Voorbeelden hierbij zijn de CIS[5] Top 18, dreigingsanalyses van het NCSC[6] en ENISA[7], en uitkomsten van penetration testing en ethical hacking. De instelling let erop dat het onderhoud aan de ICT-infrastructuur en ICT-applicaties planmatig en gestructureerd verloopt, in lijn met de change management procedures en het life-cycle-managementproces van de instelling.

De instelling zorgt er bijvoorbeeld voor dat de technologische veroudering van haar ICT-infrastructuur en ICT-applicaties binnen haar risicotolerantiegrenzen blijft en dat security updates worden toegepast. Daarnaast let DNB erop dat instellingen in beeld hebben van welke ICT-infrastructuur en ICT-applicaties hun bedrijfsprocessen afhankelijk zijn en in hoeverre de ICT-systemen kwetsbaar zijn voor cyberaanvallen. Daarbij wordt een analyse gemaakt van het netwerk om te zien waar vergaande netwerksegmentatie van het netwerk zinvol is, zoals rond de 'kroonjuwelen' van de instelling.

De instelling heeft zowel preventieve, detecterende als corrigerende beheersmaatregelen geïmplementeerd om ICT-systemen te beschermen tegen cyberaanvallen, zoals virussen, malware, ransomware, spyware en DDoS aanvallen. Wat betreft de preventieve beheersmaatregelen let DNB erop dat de instelling up-to-date technische beveiligingsmaatregelen toepast (zoals firewalls, netwerksegmentatie en intrusion detection) en daarbij behorende beheerprocedures heeft ingericht om de toegang tot de ICT-infrastructuur te beperken tot geautoriseerde personen. De instelling past daartoe bijvoorbeeld moderne firewall technologie toe die in lijn is met standaarden zoals GovCert[6], en ISO/IEC[8].

De instelling heeft verder beleid geformuleerd ten aanzien van het delen van vertrouwelijke informatie. Hierbij is een risico analyse ▶

5 Center for Internet Security. Zie https://www.cisecurity.org/controls/cis-controls-list.
6 Nationaal cybersecurity Centrum. Zie https://ncsc.nl
7 European Union Agency for Network and Information Security. Zie https://www.enisa.europa.eu/
8 International Standards Organisation. Zie https://www.iso.org

gemaakt waardoor de beveiligingsmaatregelen proportioneel worden toegepast. Voorbeelden hierbij zijn dat vertrouwelijke gegevens versleuteld worden vastgelegd op laptops en dat de instelling Data Loss Prevention software toepast ter controle van uitgaande berichten. De instelling zorgt daarbij dat het beheer van cryptografische sleutels op beheerste wijze plaatsvindt, ook ten aanzien van uitbestede activiteiten.

De risico's die afkomstig zijn van verouderde of niet-ondersteunde ICT-assets worden in kaart gebracht, beoordeeld en beperkt. Uit bedrijf genomen ICT-assets worden op veilige wijze verwerkt en afgevoerd. Hiertoe wordt een planning opgesteld die wordt afgestemd met alle betrokken bedrijfsonderdelen.

De instelling let erop dat een verhoogde focus op klantbeleving en time-to-market er niet toe leidt dat de implementatie van infrastructurele (beveiligings)maatregelen en investeringen in technologische ontwikkelingen (te) lang worden uitgesteld.

Rol van het bestuur bij de implementatie van deze beheersmaatregelen

Het bestuur van de instelling is eindverantwoordelijk voor het uitzetten en implementeren van de ICT-strategie. U kunt hierbij bijvoorbeeld denken aan de volgende aspecten:

- Het bestuur zorgt dat zij zich periodiek laat informeren over de risico's op het gebied van informatiebeveiliging en cyber-security en over nieuwe technologische ontwikkelingen (die zowel kansen als risico's met zich mee kunnen brengen op het gebied van informatiebeveiliging en cybersecurity).
- Deze risico's kunt u als bestuurder meewegen binnen de Risk Management Cycle zie daartoe ook het betreffende element in het model. ■

> 18.1 Infrastructure resource protection and availability

> 18.2 Infrastructure maintenance

> 18.3 Cryptography and Cryptographic key management

> 18.4 Network Security

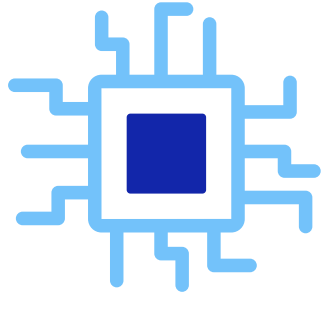
> 18.5 Protection of sensitive data

> 19.1 Malicious software prevention, detection and correction

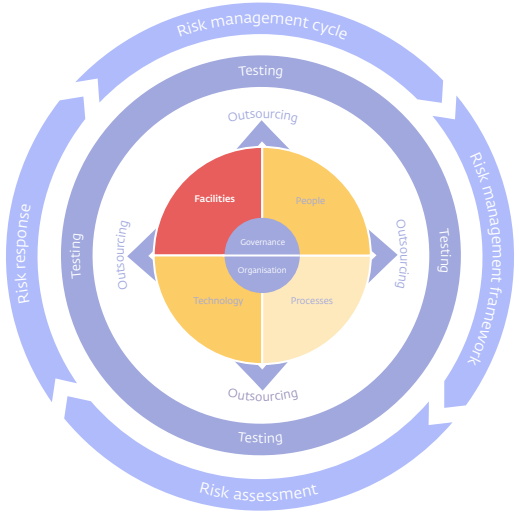
> 19.2 Vulnerability Management

> 19.3 Application Maintenance

> 20.1 Protection of security technology



Facilities



In dit onderdeel treft u een korte samenvatting aan van de belangrijkste beheersmaatregelen voort-komend uit marktstandaarden en Good Practices die horen bij het element 'Facilities'.
Aan het einde van dit element staan 'hyperlinks' waarop kan worden doorgeklikt naar de beheers-maatregelen.

DNB verstaat onder dit element

Onder dit element verstaat DNB onder andere dat toegang tot informatie ook fysiek is beveiligd, denk hierbij aan beheersmaat-regelen die de toegang tot gevoelige locaties zoals het terrein, kantoorgebouwen, de datacentra, bekabeling en thuiswerklocaties beschermen en (milieu)dreigingen beperken (zoals stroomstoringen, brand en waterschade).

Goede voorbeelden van Facilities beheersmaatregelen voor de instelling

Bij het onderdeel *Facilities* heeft de instelling in lijn met haar risicoprofiel fysieke beveiligingsmaatregelen vastgesteld, gedocumenteerd en uitgevoerd, ten aanzien van:

1. de fysieke beveiliging van kantoorgebouwen, terreinen en kritieke ICT-infrastructuur locaties, zoals datacenters en serverruimten tegen milieugevaren.
2. het verkrijgen van toegang tot gebouwen en terreinen die van belang zijn voor het uitvoeren van de bedrijfsprocessen.

Daarbij staan passende beheersmaatregelen ter bescherming tegen bedreigingen in verhouding tot het belang van de gebouwen en het kritieke karakter van de werkzaamheden of ICT-systemen die in deze gebouwen gevestigd zijn.

Een voorbeeld hierbij is dat de instelling ook beheersmaatregelen treft om de beveiligingssystemen zelf te beschermen. Hierbij kan worden gedacht aan aanvullende fysieke toegangsbeveiliging. De instelling controleert regelmatig de effectiviteit van fysieke toegangsbeveiligingsmaatregelen en rapporteert over de uitkomsten aan het senior management. Een voorbeeld hierbij is dat de instelling de fysieke toegangsbeveiligingsmaatregelen laat controleren door een "Mystery Guest".

Rol van het bestuur bij de implementatie van deze beheersmaatregelen

De rol van de bestuurder is hierbij met name van belang bij het bepalen, implementeren en controleren van het beleid. U kunt hierbij bijvoorbeeld denken aan de volgende aspecten:

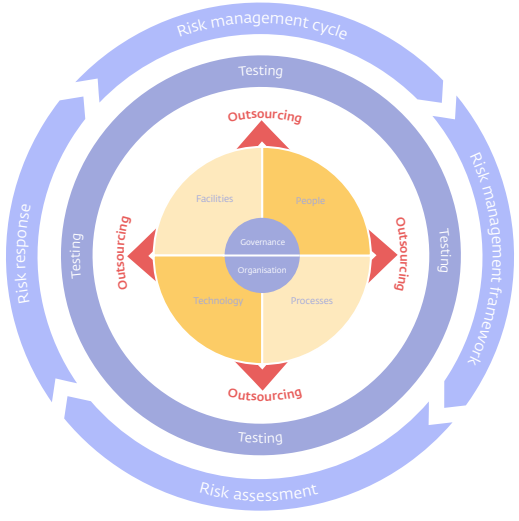
- Het bestuur laat zien belang te hechten aan afdoende fysieke toegangsbeveiliging en implementeert de benodigde beheersmaatregelen op basis van het risicoprofiel van iedere locatie.
- Het bestuur laat zich hierover informeren en spreekt de organisatie erop aan als er hiaten zijn (tone at the top). ■

Beheersmaatregelen:

> 21.1 Physical security measures

> 21.2 Physical access

Outsourcing



In dit onderdeel treft u een korte samenvatting aan van de belangrijkste beheersmaatregelen voort-komend uit marktstandaarden en Good Practices die horen bij het element 'Outscourcing'.
Aan het einde van dit element staan 'hyperlinks' waarop kan worden doorgeklikt naar de beheers-maatregelen.

DNB verstaat onder dit element

DNB ziet dat instellingen in toenemende mate kritieke of belangrijke bedrijfsprocessen zoals ICT, vermogensbeheer, klanten-, pensioen-, polis- en financiële administraties uitbesteden (*Outsourcing*). Tegenover de voordelen van uitbesteding staan ook risico's waar een instelling zich aan blootstelt. In het kader van de informatiebeveiliging en cyber-security is dat bijvoorbeeld de ongewenste omgang van de dienstverlener met vertrouwelijke gegevens van de instelling. Ook bestaat het risico dat de beveiliging en continuiteit van vertrouwelijke gegevens en systemen niet in overeenstemming is met het interne beleid als gevolg van onderuitbesteding door de dienstverlener.

Goede voorbeelden van Outscourcing beheersmaatregelen voor de instelling

Voor alle beheersmaatregelen uit deze Good Practice geldt dat bij uitbesteding van activiteiten/systemen de instelling eindverant-woordelijk blijft voor informatiebeveiliging en cybersecurity. Dit betekent dat de instelling bij elke beheersmaatregel een proces heeft ingericht dat ten minste het volgende waarborgt:

- de instelling maakt met dienstverleners, aan wie activiteiten zijn uitbesteed afspraken over een duidelijke verdeling van taken en verantwoordelijkheden. **Bij iedere beheersmaatregel** maakt de instelling risicogebaseerd afspraken met de dienst-verleners over de performance en het niveau van de interne beheersing. Deze afspraken werken ook door naar eventuele onderaannemers verderop in de keten.
- de instelling monitort en controleert periodiek en aantoonbaar de naleving van de gemaakte afspraken met de juiste periodiciteit, scope en diepgang. Dit doet zij aan de hand van rapportages of dashboards over de naleving van de Service Level afspraken en het niveau van de interne beheersing (zoals assurance en audit rapportages) en besluit indien nodig tot eigen audits of inspecties bij de dienstverleners.
- de instelling stuurt bij wanneer er afwijkingen zichtbaar zijn in de rapportages of dashboards (zie Risk Management Cycle) en besluit indien nodig tot eigen audits of inspecties bij de dienstverleners.

Uit deze drie beheersmaatregelen komt als goed voorbeeld naar voren dat de instelling specifieke prestatie en risicocriteria overeenkomt met haar dienstverleners, dat deze afspraken worden gemonitord en dat daarover wordt gerapporteerd aan belanghebbenden. Verantwoordingsrapportages van de dienst-verleners worden door de instelling geanalyseerd om trends en ontwikkelingen te identificeren en eventueel de dienstverlening bij te sturen. ▶

De instelling besteedt in de contractvoorbereidingsfase aandacht aan de wijze waarop de dienstverlener blijvend zal voldoen aan contractuele verplichtingen, aan wet- en regelgeving en dat de uitbesteding het toezicht niet belemmert. De instelling stelt in de contractvoorbereidingsfase verder samen met haar dienst-verleners een risicoanalyse op en bepaalt hoe zij met eventuele restrisico's omgaat. Bij deze analyse zijn risico's bij partijen waaraan diensten zijn onderuitbesteed meegenomen en is een exitplan overeengekomen met afspraken over een gecontroleerde beëindiging van de dienstverlening. Hierbij is onder meer bepaald hoe de (back-up) data van de instelling na de exit wordt verwijderd. Onderuitbesteding is hierbij in scope.

De instelling beschikt verder over een gedegen en goed gedocumenteerd incidentenbeheerproces, met inbegrip van de verantwoordelijkheden van alle betrokken partijen, bijvoorbeeld door vaststelling van een samenwerkingsmodel in geval van daadwerkelijke of vermoede incidenten.

Rol van het bestuur bij de implementatie van deze beheersmaatregelen

Het bestuur van de instelling is eindverantwoordelijk voor de effectieve beheersing van uitbestede activiteiten door contractuele afspraken te maken, te volgen in hoeverre die afspraken worden nageleefd en tijdig bij te sturen wanneer van de afspraken wordt afgeweken. U kunt hierbij bijvoorbeeld denken aan de volgende aspecten:

- Het bestuur geeft goedkeuring aan en herziet periodiek het uitbestedingsbeleid en bespreekt de uitbestedingsstrategie ook vanuit de invalshoek van informatiebeveiliging. Op basis van de evaluatie kunt u het uitbestedingsbeleid indien nodig aanpassen of u kunt aansturen op aanpassing of beëindiging van bestaande uitbestedingscontracten.
- Bij de te maken keuzes in de uitbestedingsstrategie, betrekt het bestuur de bijbehorende risico's op het gebied van informatiebeveiliging én de wijze waarop deze risico's doorlopend worden beheerst.
- De instelling heeft door middel van een analyse een actueel beeld van het inherente informatiebeveiligingsrisico van alle uitbestedingen en/of uitbestedingsketens. De instelling overziet welke beheersmaatregelen conform het informatiebeleid zijn getroffen en aantoonbaar werken. Het bestuur is en wordt daarvan op de hoogte gesteld. ■

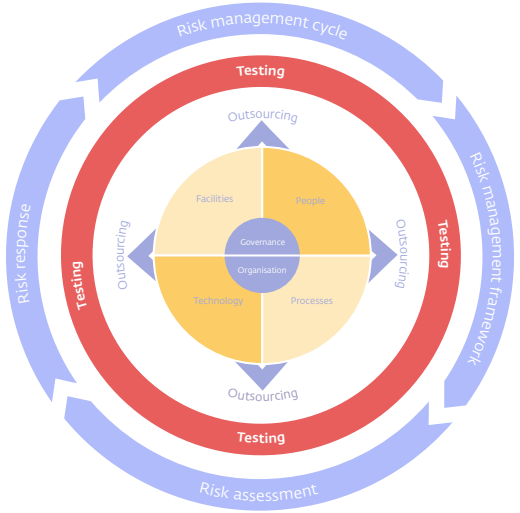
Beheersmaatregelen:

> 14.1 Third party and supplier risk management

> 14.2 Third party and supplier risk management

> 16.3 Internal control at third parties

Testing



In dit onderdeel treft u een korte samenvatting aan van de belangrijkste beheersmaatregelen voortkomend uit marktstandaarden en Good Practices die horen bij het element 'Testing'. Aan het einde van dit element staan 'hyperlinks' waarop kan worden doorgeklikt naar de beheersmaatregelen.

DNB verstaat onder dit element

Onderzoek toont aan dat het (laten) uitvoeren van Security testing effectief is om informatiebeveiliging en cyberweerbaarheid van instellingen continu te verbeteren. Security *Testing* kan zich richten op verschillende elementen uit het model van deze Q&A. Een test kan bijvoorbeeld zijn gericht op zwakheden in de infrastructuur (*Technology*), maar ook op menselijke gedrag en menselijk handelen (*People*) of op zwakke plekken in de toegang tot gebouwen (*Facilities*). De scope van Security testing kan zich richten op de interne organisatie, maar kan ook de kritieke of belangrijke uitbestedingen meenemen.

Goede voorbeelden van Testing beheersmaatregelen voor de instelling

De instelling voert een testprogramma uit dat gekoppeld is aan het riskmanagement framework, met een verscheidenheid aan verschillende evaluaties, beoordelingen en tests van de informatiebeveiliging om een doeltreffende identificatie van kwetsbaarheden in de ICT-systemen en -diensten te waarborgen. Op grond van een risicoanalyse en actuele cyberdreigingen wordt bepaald welke soorten beveiligingstests worden uitgevoerd alsmede de scope en diepgang van die tests. In de risicoanalyse is rekening gehouden met actuele cyberdreigingen, het veranderende landschap van ICT-risico's, eventuele specifieke risico's waaraan de instelling is of zou kunnen zijn blootgesteld en hoe kritiek de informatie-assets en geleverde diensten zijn.

De aard en frequentie van deze testen is afhankelijk van het risicoprofiel van de instelling, waarbij het testen van kritieke ICT-systemen en kwetsbaarheidsscans jaarlijks worden uitgevoerd. Verder worden beveiligingstests uitgevoerd in het geval van wijzigingen aan de infrastructuur, processen of procedures, en indien wijzigingen worden doorgevoerd wegens grote operationele of beveiligingsincidenten, of wegens de vrijgave van nieuwe of aanzienlijk gewijzigde kritieke toepassingen.

Een voorbeeld hierbij is dat de instelling verschillende typen beveiligingstests kan of laat uitvoeren, waaronder pentests gericht op de beveiliging van infrastructuur en applicaties, red teaming, het testen van de fysieke beveiliging en het testen van menselijk handelen in relatie tot informatiebeveiliging en cybersecurity. Deze testen kunnen uitgevoerd worden door interne of externe ingehuurde partijen.

De instelling gaat na dat de partij die de beveiligingstests uitvoert voldoende geëquipeerd is om dergelijke tests uit te voeren (hebben zij de juiste ervaring, certificeringen en referenties?). Een voorbeeld hierbij is dat de instelling op basis van een risicoanalyse *een jaarplan* maakt voor de uit te voeren soorten security tests. ▶

Rol van het bestuur bij de implementatie van deze beheersmaatregelen

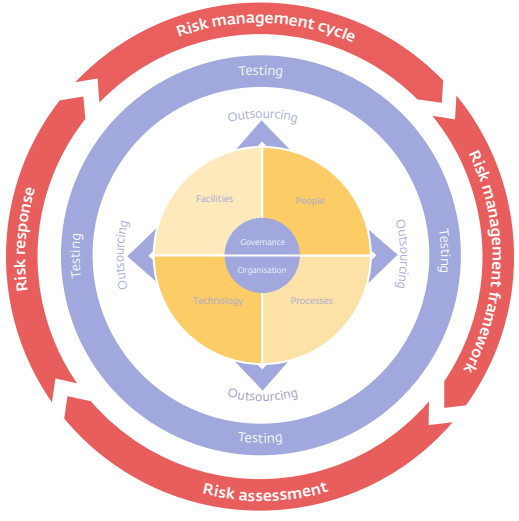
Het bestuur van de instelling is eindverantwoordelijk voor het aansturen, monitoren en uit laten voeren van Security testing. U kunt hierbij bijvoorbeeld denken aan de volgende aspecten:

- Het bestuur stelt voldoende middelen beschikbaar om het testprogramma te laten uitvoeren, bespreekt de belangrijkste uitkomsten van het testprogramma en zorgt ervoor dat er procedures zijn die erop toezien dat resultaten van de beveiligingstests gecontroleerd, geëvalueerd en geprioriteerd worden.
- Het bestuur zorgt dat geconstateerde kwetsbaarheden onverwijld gemitigeerd worden met duidelijke deadlines, rekening houdende met hoe kritiek de kwetsbaarheden en/of het getroffen ICT-systeem zijn. ■

Beheersmaatregelen:

> 22.1 Penetration testing and ethical hacking

Risk management cycle



In dit onderdeel treft u een korte samenvatting aan van de belangrijkste beheersmaatregelen voort-komend uit marktstandaarden en Good Practices die horen bij het element 'Risk Management Cycle'. Aan het einde van dit element staan 'hyperlinks' waarop kan worden doorgeklikt naar de beheers-maatregelen.

DNB verstaat onder dit element

De *Risk Management Cycle* is van toepassing op alle elementen uit het model. Het is belangrijk dat de instelling regelmatig de voor haar relevante risico's op het gebied van informatiebeveiliging en cybersecurity identificeert en analyseert. Op grond van deze risicoanalyse bepaalt de instelling haar reactie, treft beheersmaat-regelen om risico's te beperken en accepteert (tijdelijk) eventuele restrisico's. Geaccepteerde restrisico's worden periodiek opnieuw geëvalueerd en opnieuw ter acceptatie aangeboden.

Goede voorbeelden van Risk Management Cycle beheersmaatregelen voor de instelling

Bij het element Risk Management Cycle heeft de instelling de beheersing van risico's ten aanzien van informatiebeveiliging en cybersecurity geborgd door de implementatie van een ICT Risk Management Framework dat in lijn is met de eigen digitale operationele weerbaarheid strategie. Dit raamwerk is gebaseerd op een Plan-Do-Check-Act cyclus, waarover regelmatig wordt gerapporteerd aan het bestuur. De instelling hanteert in haar *ICT Risk Management Framework* eenduidige definities voor informatie-beveiliging en cybersecurity, die zijn ontleend aan markt standaarden zoals bijvoorbeeld NIST, ISO en Cobit. De definities worden consistent toegepast binnen alle documenten en rapportages. Een voorbeeld hierbij is dat actuele cyberdreigingen zoals malware, ransomware, DDoS aanvallen en phishing deel uitmaken van het ICT Risk Management Framework van de instelling.

De instelling voert regelmatig en ten minste één maal per jaar en bij elke belangrijke wijziging in de infrastructuur of relevante processen een risicoanalyse uit op basis van kwalitatieve en kwantitatieve methoden, waarin actuele cyberdreigingen zijn geanalyseerd en geprioriteerd. De instelling brengt daartoe bijvoorbeeld haar bedrijfsprocessen en -activiteiten, bedrijfs-functies, rollen en assets (zoals informatie- en ICT-assets) in kaart en werkt die regelmatig bij, om daarvan het belang voor ICT- en beveiligingsrisico's vast te stellen en hun onderlinge afhankelijk-heden te bepalen. Ook neemt ze daarbij nadrukkelijk haar legacy systemen mee.

Als belangrijke input voor de risicoanalyse wordt eerst het gespecificeerde dreigingsbeeld van de instelling in kaart gebracht of geüpdatet.

Daar waar nodig treft de instelling aanvullende beheersmaat-regelen. Daarnaast maakt de instelling expliciet welke risico's formeel worden geaccepteerd. Beheersmaatregelen die niet (meer) effectief werken worden aangepast, vervangen door andere beheersmaatregelen of uitgefaseerd. ▶

De instelling stelt voor niet geaccepteerde risico's een 'risk action plan' op dat uitwerking geeft aan de risk response. Het 'risk action plan' wordt daarbij geaccordeerd door het management niveau dat past bij de aard en omvang van de restrisico's. Een voorbeeld hierbij is dat de instelling voor actuele cyberdreigingen expliciet heeft gemaakt welke risico's formeel worden geaccepteerd en voor welke restrisico's aanvullende beheersmaatregelen noodzakelijk zijn.

De instelling borgt dat zowel de 1e, 2e en 3e lijn actief betrokken zijn bij de totstandkoming, uitvoering, onderhoud en evaluatie van de Risk Management Cycle.

Assurance door (ICT)-Auditors ten aanzien van de afzonderlijke controls en hun context in het hele stelsel van Informatie-beveiligingsmaatregelen kunnen ten aanzien van de Good Practice Informatiebeveiliging waarborgen geven aan bestuurders, raden van toezicht en raden van commissarissen.

Rol van het bestuur bij de implementatie van deze beheersmaatregelen

Het bestuur van de instelling is eindverantwoordelijk voor het aansturen, implementeren en elimineren van de beheersmaat-regelen die voortkomen uit de Risk Management Cycle. U kunt hierbij bijvoorbeeld denken aan de volgende aspecten:

- Het bestuur draagt de algehele verantwoordelijkheid voor het opzetten en goedkeuren van een digitale operationele weerbaarheid strategie op korte, middellange en lange termijn die uiteenzet hoe het Risk Management Framework wordt uitgevoerd.
- Het bestuur heeft daartoe een risicomanagementcyclus laten inrichten en wordt regelmatig geïnformeerd over informatiebeveiligingsrisico's en cyberdreigingen.
- Het bestuur evalueert jaarlijks, en bij grote ICT-gerelateerde incidenten, via een schriftelijk verslag het resultaat van het ICT-Risk Management Framework. Hierbij wordt rekening gehouden met actuele ontwikkelingen en risico's. Het ICT-Risk Management Framework wordt regelmatig onderworpen aan (interne) audits. Verzekeraars verwerken risico's in de ORSA, pensioenfondsen in de ERB en banken in de ICAAP.
- Het bestuur stelt voldoende middelen beschikbaar om effectieve beheersmaatregelen te treffen op grond van het risicoprofiel van de instelling en de risicobereidheid van het bestuur. Het bestuur gaat periodiek na in hoeverre de risico's die de instelling loopt op het gebied van informatiebeveiliging en cybersecurity zich bevinden binnen de risicotoleranties van het bestuur. Ook in het geval dat kritieke of belangrijke werkzaamheden zijn uitbesteed bij dienstverleners.
- Het bestuur weegt periodiek af in hoeverre een effectieve 'mix' van beheersmaatregelen – mensen, processen, techniek en faciliteiten – is getroffen om risico's van de instelling op het gebied van informatiebeveiliging en cybersecurity te mitigeren (vanuit een allesomvattende benadering). ■

Beheersmaatregelen:

> 4.1 ICT Risk Management framework

> 4.2 Risk assessment

> 4.3 Maintenance and monitoring of a risk action plan

Volwassenheidsmodel

Een instelling kan met een self-assessment vaststellen in hoeverre de beheersing van informatiebeveiliging en cybersecurity op het vereiste niveau is. Om dit niveau te kunnen vaststellen, hanteert DNB een volwassenheidsmodel gebaseerd op definities van in de markt bekende standaarden als COBIT [9].

Financiële instellingen zijn aantoonbaar 'in control'. In het door DNB gehanteerde model met 58 beheersmaatregelen komt dat overeen met ten minste een volwassenheidsniveau van '3': aantoonbare werking voor een minimum van 6 maanden voor 55 beheersmaatregelen. Voor de Risk Management Cycle controls, betreffende controls #4.1, #4.2 en #4.3, komt dit overeen met een volwassenheidsniveau van '4'.

Bij het invullen van het *self assessment* houdt de instelling bij het toekennen van de volwassenheidsniveaus, rekening met de definities in onderstaande tabel. In de eerste kolom staan de volwassenheidsniveaus van 0 t/m 5. In de tweede kolom staan de definities van de volwassenheidsniveaus welke DNB bij haar toezichtonderzoeken hanteert. In de derde kolom zijn criteria opgenomen ter verdere verduidelijking van het volwassenheidsniveau.

De criteria genoemd bij de niveaus tot en met 3 'gedefinieerd' (opzet, bestaan en werking) zien met name toe op de aantoonbaarheid en effectiviteit van de control zelf. De criteria voor de niveaus 4 en 5 zien met name op de aantoonbaarheid en de effectiviteit van het stelsel van controls en de rol die de specifieke control daarin speelt.

De criteria voor de volwassenheidsniveaus zijn tevens van toepassing op de beheersingsmaatregelen die in de uitbestedingsketen worden uitgevoerd.

De instelling heeft voor het vaststellen van het volwassenheidsniveau bepaald wat de taken en verantwoordelijkheden van de eerste, tweede en derde lijn hierin zijn.

9 In de oude GP Informatiebeveiliging sloot DNB zo dicht mogelijk aan bij de definities die DNB sinds 2014 hanteert en welke zijn ontleend aan "CobiT 4.1 Research, 2007, Appendix III—Maturity Model for Internal Control, page 175".

Niveau:	Definitie van het volwassenheidsniveau:	Criteria ter verduidelijking:
0	**Niet bestaand** – Aan deze beheersmaatregel is geen aandacht besteed.	
1	**Initieel** - De beheersmaatregel is (gedeeltelijk) gedefinieerd, maar wordt op inconsistente wijze uitgevoerd. Er is een grote afhankelijkheid van individuen bij de uitvoering van de beheersmaatregel.	■ Geen of beperkte beheersmaatregel geïmplementeerd. ■ De beheersmaatregel is ad-hoc uitgevoerd. ■ De beheersmaatregel is niet gedocumenteerd. ■ De wijze van uitvoering is afhankelijk van een individu en niet gestandaardiseerd. ■ De taken en en verantwoordelijkheden incl. noodzakelijke functiescheiding zijn beschreven voor deze control, maar worden in de praktijk veelal niet conform de beschrijving uitgevoerd. ■ Toetsing op werking van deze control vindt incidenteel plaats. ■ Het effect van de beheersmaatregel wordt niet beoordeeld.
2	**Herhaalbaar maar informeel** – De beheersmaatregel is aanwezig en wordt op consistente en gestructureerde, maar op informele wijze uitgevoerd.	■ Opzet en bestaan zijn beperkt aantoonbaar. ■ De beheersmaatregel is slechts deels bepaald, deels schriftelijk vastgelegd en deels ingebed in de organisatie. ■ De taken en verantwoordelijkheden incl. noodzakelijke functiescheiding zijn beschreven voor deze beheersmaatregel en worden in de praktijk uitgevoerd. ■ Het effect van de control kan niet worden aangetoond en/of is niet vastgelegd. ■ De werking van de beheersmaatregel wordt minder dan 6 maanden periodiek getoetst en vastgelegd **ofwel** de effectiviteit kan niet worden aangetoond over 6 maanden.
3	**Gedefinieerd (opzet bestaan en werking) –** De opzet van de beheersmaatregel is gedocumenteerd en wordt op gestructureerde en geformaliseerde wijze uitgevoerd. De vereiste effectiviteit van de beheersmaatregel is aantoonbaar en wordt getoetst. Daar waar nodig wordt de beheersmaatregel verbeterd.	■ Opzet, bestaan en effectieve werking zijn aantoonbaar. ■ De beheersmaatregel is gedefinieerd op basis van een risico assessment. ■ De beheersmaatregel is bepaald, schriftelijk vastgelegd en ingebed in de organisatie. ■ Taken en verantwoordelijkheden incl. noodzakelijke functiescheiding zijn uitgeschreven geïmplementeerd en getoetst op werking en worden geëvalueerd. ■ De effectieve werking is over een periode van minimaal 6 maanden risicogebaseerd getoetst, aangetoond en vastgelegd. ■ Over de uitvoering van de beheersmaatregel wordt aan het management gerapporteerd.
4	**Effectief en meetbaar stelsel van beheersmaatregelen –** Naast de effectiviteit van individuele beheersmaatregelen, wordt ook periodiek de effectiviteit van de samenhang van alle informatiebeveiligings-maatregelen geëvalueerd. Deze evaluatie van het stelsel van beheersmaatregelen wordt vastgelegd en gerapporteerd aan het management.	Criteria voor niveau 3 plus de volgende onderscheidende criteria: ■ De evaluatie van de beheersmaatregel vindt plaats in de context van het stelsel van informatiebeveiligingsmaatregelen. ■ De evaluatie is gedocumenteerd. ■ De taken en verantwoordelijkheden voor het evalueren zijn geformaliseerd. ■ De frequentie waarop wordt geëvalueerd is gebaseerd op het risicoprofiel van de instelling en vindt minimaal jaarlijks plaats. ■ Bij de periodieke toetsing van de effectieve werking van de control worden KCI's (metrics) gebruikt, worden (operationele) incidenten meegenomen en vindt benchmarking met peers plaats. ■ De uitkomst van de evaluatie wordt aan het management gerapporteerd.
5	**Continu verbeteren en toekomst gericht stelsel van beheersmaatregelen** – Er wordt continu gezocht naar verbetering van de effectiviteit van het stelsel van beheersmaatregelen door rekening te houden met toekomstige risico's. Hierbij wordt gebruik gemaakt van externe data en benchmarking. Medewerkers zijn pro-actief betrokken bij de toekomstgerichte verbetering van de de effectiviteit van de samenhang van informatiebeveiligingsmaatregelen.	Criteria voor niveau 4 plus de volgende onderscheidende criteria: ■ De beheersmaatregel wordt continu bijgewerkt. Evaluatie is gericht op de toekomst en neemt de benchmarking met peers mee. ■ Bij de inrichting van de beheersmaatregel is gebruik gemaakt van resultaten uit self-assessments, gap- en root cause analyses. ■ De getroffen beheersmaatregelen zijn gebenchmarkt op basis van externe data en zijn 'Best Practice' in vergelijking met andere organisaties. ■ De toetsing van de effectieve werking van de beheersmaatregel gebeurt aan de hand van KCI's (metrics). ■ Medewerkers zijn aantoonbaar voortdurend en pro-actief betrokken bij de verbetering van de beheersmaatregelen.

1.1 Information Security Plan

Marktstandaarden* geven aan dat de instelling een proces inricht dat onder meer het volgende waarborgt:

- Op basis van een risicoanalyse en dreigingsbeeld stelt het bestuurlijk of beleidsbepalend orgaan (hierna: "het bestuur") een digitale operationele weerbaarheid strategie op korte, middellange en lange termijn vast.
- Het bestuur draagt de eindverantwoordelijkheid om, in lijn met de digitale operationele weerbaarheid strategie, periodiek het informatiebeveiligingsbeleid vast te stellen inclusief het daaruit volgend informatiebeveiligingsplan.
- Het bestuur overziet en neemt de verantwoordelijkheid dat het vastgestelde informatiebeveiligingsbeleid en informatiebeveiligingsplan worden uitgevoerd en gemonitord.
- Het informatiebeveiligingsplan omvat een omschrijving van de belangrijkste taken en verantwoordelijkheden inzake informatiebeveiligingsbeheer en zet de vereisten voor budget, personeel, processen en technologie met betrekking tot informatiebeveiliging uiteen, waarbij medewerkers op alle niveaus verantwoordelijkheid dragen om de informatiebeveiliging van de instelling te waarborgen.
- Het informatiebeveiligingsbeleid en -plan hebben een relatie met de bedrijfsstrategie en de aard en omvang van de instelling (proportionaliteit) en ondersteunen de doelen uit de ICT-strategie.
- De instelling brengt de medewerkers en de dienstverleners op de hoogte van het actuele informatiebeveiligingsbeleid. Deze is van toepassing op alle medewerkers en relevante dienstverleners.

Let op!

Risicogebaseerd, uitbesteding en het three lines model

Good Practices hierbij zijn:

- De instelling heeft een informatiebeveiligingsbeleid opgesteld in lijn met internationaal geaccepteerde standaards zoals ISO27001/2 en het NIST cybersecurity framework.
- Het informatiebeveiligingsbeleid bevat zowel preventieve, detecterende, corrigerende als repressieve beheersmaatregelen. In het NIST cybersecurity framework komt dit bijvoorbeeld nader tot uitdrukking in fasen *Identify*, *Protect*, *Detect*, *Respond* en *Recover*.
- Het informatiebeveiligingsbeleid van de instelling beschrijft zowel (ICT) technische beheersmaatregelen als procedurele beheersmaatregelen in de bedrijfsprocessen.
- De instelling actualiseert het informatiebeveiligingsbeleid met een vaste periodiciteit die past bij de aard, omvang en complexiteit van de instelling (bijvoorbeeld twee jaarlijks) en met een hogere frequentie wanneer daartoe aanleiding bestaat, bijvoorbeeld bij fusies en overnames, majeure uitbestedingen of nieuwe cyberdreigingen.
- Medewerkers van de instelling zijn via awareness programma's bekend met de beleidslijnen op het gebied van informatie-beveiliging en kennen hun rol en verantwoordelijkheden in dat verband.

1.2 Information Security policies and procesmanagement

Marktstandaarden* geven aan dat de instelling een proces inricht dat onder meer het volgende waarborgt:

- Beheersmaatregelen die voortkomen uit het informatie-beveiligingsbeleid en -plan maken deel uit van gestandaardiseerde en voorspelbare (ICT) werkprocessen (beheerste en integere bedrijfsvoering) en sluiten aan bij het risicoanalyse- en dreigingsbeeld.
- Het bestuur waarborgt dat het governancesysteem van de instelling, in het bijzonder het risicobeheer- en het interne controlesysteem, de beveiligingsrisico's van de instelling op adequate wijze beheerst.
- (ICT) werkprocessen en procedures zien toe op een beheerste ICT-systeemontwikkeling, verwerving van veilige hard- en software uit onbetwiste bron, verwerking en opslag van gegevens, ICT-systeemonderhoud en ICT-support.
- Het informatiebeveiligingsbeleid waarborgt dat de instelling logbestanden bij houdt en kritieke ICT-activiteiten monitort, zodat fouten kunnen worden opgespoord, geanalyseerd en gecorrigeerd.
- Noodprocedures zijn opgesteld voor situaties waarin de standaardprocedures niet voorzien.

Let op!

Risicogebaseerd, uitbesteding en het three lines model

Good Practices hierbij zijn:

- De instelling heeft (ICT) werkprocessen en procedures beschreven en/of ingericht in workflow tooling die een beheerste uitvoering van die (ICT) werkprocessen en procedures waarborgen. De workflow tooling dwingt bijvoorbeeld het 4-ogen principe af bij het aanpassen van kritieke ICT-systemen, systeemparameters of data en dat alle activiteiten herleidbaar zijn (logging).
- De procedures zijn gebaseerd op internationaal geaccepteerde standaarden, zoals ITIL, BISL en PRINCE II.
- De instelling actualiseert de ingerichte beheersmaatregelen in relatie tot de (herijkte) risico's. Daarbij past zij de (opzet van) (ICT) werkprocessen en procedures aan met een vaste periodiciteit (bijvoorbeeld jaarlijks) en met een hogere frequentie wanneer daartoe aanleiding bestaat, bijvoorbeeld bij fusies en overnames, uitbesteding van de (ICT) werkprocessen of incidenten in de uitvoering. Bij nieuwe of in intensiteit toenemende vormen van cyberdreigingen, bekijkt de instelling of (ICT) werkprocessen en procedures dienen te worden aangescherpt. De instelling stelt vast in hoeverre haar medewerkers, inhuurkrachten en dienstverleners zich houden aan de vastgestelde (ICT) werkwijzen en zich ervan bewust zijn dat een beheerste uitvoering van hun werkzaamheden bijdraagt aan informatiebeveiliging en weerbaarheid tegen cyberdreigingen.

2.1 Information Security Architecture

Marktstandaarden* geven aan dat de instelling een proces inricht dat onder meer het volgende waarborgt:

- Bedrijfsprocessen en ICT-systemen zijn opgezet volgens een door de instelling vastgestelde informatiearchitectuur waarin onder meer is geadresseerd:
  - Visie op de informatievoorziening;
  - Doelarchitectuur van ICT-systemen en processen;
  - Cybersecurity- en privacy vereisten;
  - Systeem- en dataclassificatie;
  - Rationalisatie van huidige ICT-systemen; het uitfaseren van legacy ICT-systemen en ICT-systemen die kwetsbaar zijn voor cyberdreigingen;
  - De ICT-architectuur is in lijn met de ICT-strategie.

Let op!

Risicogebaseerd, uitbesteding en het three lines model

Good Practices hierbij zijn:

- De instelling werkt volgens een Information Security Architectuur waarin inzichtelijk is gemaakt hoe de ICT-systemen en dataverzamelingen de bedrijfsstrategie en bedrijfsprocessen ondersteunen.
- De informatiearchitectuur is gebaseerd op internationaal geaccepteerde standaarden zoals TOGAF en DYA waarbij de daarin uitgewerkte aandachtsgebieden ook zijn bekeken vanuit een security perspectief.
- De instelling heeft een visie ontwikkeld waaruit blijkt hoe de ICT-systemen en organisatiestructuur zullen evolueren om de bedrijfsstrategie op (midden)lange termijn te ondersteunen; kritieke of belangrijke afhankelijkheden van derden / partners zijn daarbij in kaart gebracht.
- In deze visie worden elementen van NIST ZERO Trust architectuur betrokken zoals het aanbrengen van een scheiding (logisch of mogelijk fysiek) van 1. De communicatiestromen die worden gebruikt om het netwerk en de applicatie/dienst te besturen en te configureren (control plane) en 2. De communicatiestromen die worden gebruikt om het eigenlijke werk van de organisatie uit te voeren (data plane).
- De instelling hanteert architectuurprincipes die erop zijn gericht dat informatie zo eenvoudig, flexibel, betrouwbaar en veilig mogelijk aan daartoe geautoriseerde medewerkers, klanten en derden beschikbaar wordt gesteld.

2.2 Data classification scheme

Marktstandaarden* geven aan dat de instelling een proces inricht dat onder meer het volgende waarborgt:

- Het eigenaarschap van systemen en data is door het bestuur van de organisatie vastgesteld.
- De instelling heeft een data classificatiebeleid vastgesteld, waarbij alle relevante informatiebeveiligingsrisico's waaraan zij zijn blootgesteld, worden geïdentificeerd, geclassificeerd en gemeten.
- De meting van de ICT- en beveiligingsrisico's wordt uitgevoerd op basis van de vastgestelde ICT- en beveiligingsrisico criteria, waarbij rekening wordt gehouden met hoe kritiek de bedrijfsprocessen en -activiteiten, bedrijfsfuncties, rollen en assets (zoals informatie- en ICT-assets), de omvang van bekende kwetsbaarheden en eerdere incidenten die invloed hebben gehad op de instelling, zijn.
- De methoden die worden gebruikt ter bepaling van hoe kritiek deze zijn waarborgen dat de beschermingsvereisten consistent en alomvattend zijn.
- Op basis van bovenstaand classificatiebeleid worden relevante beveiligingsmaatregelen getroffen met betrekking tot toegang, versleuteling, opslag, retentie, opschoning, etc.
- De instelling controleert periodiek of medewerkers het classificatiebeleid naleven.

Let op!

Risicogebaseerd, uitbesteding en het three lines model

Good Practices hierbij zijn:

- De instelling heeft een dataclassificatieschema opgesteld dat gebaseerd is op de risico's aan de hand waarvan alle ICT-systemen en data worden ingedeeld in bijvoorbeeld: Beschikbaarheid, Integrititeit, Vertrouwelijkheid (BIV), Hoog/Midden/Laag en Publiek/Vertrouwelijk/Geheim.
- Op basis van de classificatie treft de instelling beheersmaat-regelen, zoals encrypted opslag van alle gegevens in de categorie Geheim.
- De instelling heeft zicht op de datacenter locatie(s) waar haar bedrijfskritieke informatie is opgeslagen. Dit instelling stelt periodiek vast dat de locaties in overeenstemming zijn met haar informatiebeveiligingsbeleid.
- De instelling monitort actief met behulp van DLP-tooling in hoeverre gevoelige data vanuit het bedrijfsnetwerk naar buiten wordt verzonden en of dat in overeenstemming is met de dataclassificatie.

3.1 Risks and opportunities of future trends and regulations

Marktstandaarden* geven aan dat de instelling een proces inricht dat onder meer het volgende waarborgt:

- Het bestuur en risk zijn op de hoogte van de belangrijkste toepassingen van technologische ontwikkelingen en dreigingen en nemen de risico's en kansen daarvan mee in hun besluitvorming.
- Ontwikkelingen in de sector worden in kaart gebracht, onder meer op het gebied van cybersecurity, waarbij ook onderwerpen als 'technologie' en 'risicomanagement' betrokken worden.
- De potentiële impact van al deze ontwikkelingen/dreigingen wordt gewogen, indien van toepassing worden passende beheersmaatregelen getroffen om risico's te mitigeren.

Let op!
Risicogebaseerd, uitbesteding en het three lines model

Good Practices hierbij zijn:

- Medewerkers zijn actief op internetfora en/of geabonneerd op cybersecurity nieuwsbrieven.
- De instelling neemt een dienst af van een externe partij die gerichte security intelligence levert.
- De instelling is lid van beroeps- en/of vakverenigingen of andere sectorale organisaties die kennis en ervaring uitwisselen op het gebied van cybersecurity zoals ISAC's.
- De instelling onderhoudt nauwe contacten met overheids-instanties, die zich richten op cybersecurity, zoals het NCSC of het Digital Trust Center.
- De instelling heeft contractuele afspraken gemaakt met kritieke of belangrijke uitbestedingspartners over samenwerking en informatieuitwisseling op het gebied van informatiebeveiliging en cybersecurity.
- Ontwikkelingen op het gebied van Quantum technologie worden in kaart gebracht, zowel voor praktische toepassingen van Quantum op het gebied van beveiliging als voor risico's die voortkomen uit Quantum technologie zoals risico's op het gebied van cryptografie.
- De instelling volgt de toepassingen van nieuwe technologieën, zoals Artificial Intelligence en blockchain en heeft daarbij oog voor zowel kansen als risico's.
- De instelling onderhoudt nauwe contacten met overheids-instanties, die zich richten op cybersecurity zoals het NCSC of het Digital Trust Center.

3.2 Technical standards

Marktstandaarden* geven aan dat de instelling een proces inricht dat onder meer het volgende waarborgt:

- De instelling werkt volgens geaccepteerde (technische) standaarden op het gebied van informatiebeveiliging en cybersecurity. Deze zijn toegespitst op de aard, omvang en complexiteit van de instelling.
- Het werken volgens standaarden is naar medewerkers gecommuniceerd; zij zijn bekend met de voor hun werkzaamheden relevante standaarden.
- Nieuwe ICT-systemen en wijzigingen in ICT-systemen voldoen aan op de vastgestelde standaarden.
- De instelling gaat na dat volgens de vastgestelde standaarden wordt gewerkt.

Let op!

Risicogebaseerd, uitbesteding en het three lines model

Good Practices hierbij zijn:

- De instelling werkt volgens internationaal geaccepteerde standaarden voor informatiebeveiliging en cybersecurity, zoals bijvoorbeeld het MITRE Att@CK framework, ISO27001/2, NIST cybersecurity framework, NCSC Guidelines en/of CIS Baselines.
- De standaarden zijn gecommuniceerd en bekend bij intern en ingehuurd personeel, zoals ICT-security officers, ICT-architecten, projectmanagers, software ontwikkelaars, functioneel- en technisch beheerders, ICT-riskmanagers en ICT-auditors.
- Van afwijkingen ten opzichte van security baselines wordt aan de hand van het beveiligingsrisico de opvolging bepaald.
- De ICT-security officer van de instelling beoordeelt nieuwe standaarden op het gebied van informatiebeveiliging en cybersecurity en doet voorstellen hoe deze de informatie-beveiliging en cybersecurity beheersmaatregelen van de instelling kunnen versterken.
- De door de instelling geformaliseerde ICT-architectuur en standaarden zijn van toepassing verklaard op de dienst-verleners van de instelling. Periodiek wordt vastgesteld in hoeverre de dienstverleners hun ICT-omgeving conform deze standaarden hebben ingericht.
- De ICT-infrastructuur en het ICT-applicatielandschap wordt jaarlijks getoetst aan de meest actuele security baselines en marktstandaarden.

4.1 ICT-Risk Management Framework

Marktstandaarden* geven aan dat de instelling een proces inricht dat onder meer het volgende waarborgt:

- Het bestuur heeft een risicomanagementcyclus ingericht en laat zich regelmatig informeren over informatiebeveiligingsrisico's en cyberdreigingen.
- De instelling adresseert risico's en beheersmaatregelen op het gebied van informatiebeveiliging en cybersecurity in het ICT-Risk Management raamwerk in lijn met de eigen digitale operationele weerbaarheid strategie.
- Het ICT-Risk Management Framework is onderdeel van het overall Risk Management raamwerk van de instelling.
- De risicotoleranties ten aanzien van informatiebeveiliging en cybersecurity zijn bepaald en vastgelegd.
- Het bestuur stelt voldoende middelen beschikbaar om effectieve beheersmaatregelen te treffen op grond van het risicoprofiel van de instelling en de risicobereidheid van het bestuur. Het bestuur weegt periodiek af, en betrekt actief risk daarbij, in hoeverre een effectieve 'mix' van beheersmaat-regelen – mensen, processen, techniek en faciliteiten – is getroffen om risico's van de instellingen op het gebied van informatiebeveiliging en cybersecurity te mitigeren (vanuit een allesomvattende benadering).
- Het bestuur evalueert jaarlijks risicogebaseerd het gewenste/benodigde niveau van volwassenheid van de 58 beheers-maatregelen.
- Het bestuur evalueert jaarlijks, en bij grote ICT-gerelateerde incidenten, via een schriftelijk verslag over het resultaat van het ICT-Risk Management raamwerk. Hierbij wordt rekening gehouden met actuele ontwikkelingen en risico's.
- Het ICT-Risk Management raamwerk wordt regelmatig onderworpen aan (interne) audits.

Let op!

Risicogebaseerd, uitbesteding en het three lines model

Good Practices hierbij zijn:

- De instelling hanteert in haar ICT-Risk Management Framework eenduidige definities voor informatiebeveiliging en cybersecurity; deze zijn ontleend aan markt standaarden zoals NIST CF, ISO 27000 en CobiT en worden consistent binnen alle documenten en rapportages in het ICT-Risk Management Framework gehanteerd.
- Verzekeraars verwerken risico's in de ORSA, pensioenfondsen in de ERB en banken in de ICAAP. De digitale operationele weerbaarheid strategie omvat de volgende elementen;
  - uitleg hoe het ICT-Risk Management Framework de bedrijfsstrategie en doelstellingen van de instelling ondersteunt;
  - vaststelling van het risicotolerantielimiet voor ICT-risico (in overeenstemming met de risicobereidheid) en een analyse van de impacttolerantie voor ICT-verstoringen;
  - duidelijke doelstellingen voor informatiebeveiliging, met inbegrip van essentiële prestaties, indicatoren en belangrijke risicomaatstaven;
  - uitleg van de ICT-referentiearchitectuur;
  - een schets van de verschillende beheersmaatregelen die zijn ingesteld of worden ingesteld om effecten van ICT-gerelateerde incidenten op te sporen, te beschermen en te voorkomen en zicht te krijgen hoe die met elkaar samenhangen;
  - het aantonen van de huidige digitale operationele weerbaarheid op basis van het aantal gemelde grote ICT-gerelateerde incidenten en de effectiviteit van preventieve beheersmaatregelen;
  - het uitstippelen van een communicatiestrategie in het geval van ICT-gerelateerde incidenten. Actuele cyberdreigingen

zoals malware, ransomware, DDoS aanvallen en phishing maken deel uit van het Risk Management raamwerk.

- In de keten van uitbestede diensten werken partijen in overeenstemming met het ICT-Risk Management Framework van de instelling.
- De instelling beoordeelt periodiek in hoeverre partijen aan wie activiteiten/systemen zijn uitbesteed, werken in overeenstemming met het ICT-Risk Management Framework van de instelling.
- De instelling verkrijgt op grond van interne rapportages en rapportages van dienstverleners een integraal beeld van de beheersing van de risico's in de keten op het gebied van informatiebeveiliging en cybersecurity.
- De taken van het controleren van de naleving van de ICT-risicobeheervereisten kunnen worden uitbesteed aan intra groeps- of externe ondernemingen. Bij een dergelijke uitbesteding blijft de instelling eind verantwoordelijk voor het integraal risicobeeld.

4.2 Risk assessment

Marktstandaarden* geven aan dat de instelling een proces inricht dat onder meer het volgende waarborgt:

- Het bestuur gaat periodiek na in hoeverre de risico's die de instelling loopt op het gebied van informatiebeveiliging en cybersecurity zich bevinden binnen de door het bestuur vastgestelde risicotoleranties. Ook in het geval dat kritieke of belangrijke werkzaamheden zijn uitbesteed bij dienstverleners.
- De instelling voert regelmatig of ten minste één maal per jaar, en bij elke belangrijke wijziging in de infrastructuur of relevante processen, ICT-risicoanalyses uit op basis van kwalitatieve en kwantitatieve methoden. Daarbij neemt ze nadrukkelijk ook haar verouderde en legacy systemen mee. Als belangrijke input voor de risicoanalyse wordt eerst het gespecificeerde dreigingsbeeld van de instelling in kaart gebracht of geüpdatet.
- De kans en impact van inherente risico's op het gebied van informatiebeveiliging en van restrisico's worden hierbij in kaart gebracht.
- De instelling neemt de risico's die samenhangen met de toepassingen van nieuwe technologieen mee in ICT-risicoanalyes en het dreigingsbeeld.
- De instelling stelt onder andere op basis van haar risicobeoordeling beheersmaatregelen vast, voert die uit, meet waar relevant hun effectiviteit met KCI's (metrics) en toetst periodiek hun effectiviteit om de geïdentificeerde ICT- en beveiligingsrisico's te beheren en de informatie-assets te beschermen in overeenstemming met hun classificatie.
- Restrisico's worden ter (tijdelijke) acceptatie voorgelegd op het management niveau dat past bij de aard en omvang van het restrisico.
- Geaccepteerde restrisico's worden periodiek opnieuw geëvalueerd en opnieuw ter acceptatie aangeboden wanneer zij buiten de risicotolerantie van de instelling vallen.

Let op!

Risicogebaseerd, uitbesteding en het three lines model

Good Practices hierbij zijn:

- De instelling voert jaarlijks een ICT-risicoanalyse uit met alle voor de analyse relevante stakeholders binnen de instelling. Op basis hiervan worden actuele cyberdreigingen gewogen en geprioriteerd.
- De instelling brengt daartoe haar bedrijfsprocessen en -activiteiten, bedrijfsfuncties, rollen en assets (zoals informatie- en ICT-assets) in kaart en werkt die regelmatig bij, om daarvan het belang voor ICT- en beveiligingsrisico's vast te stellen en de onderlinge afhankelijkheden te bepalen.
- De instelling voert daarnaast regelmatig en ten minste jaarlijks een specifieke ICT-risicobeoordeling uit op alle legacy ICT-systemen.
- Om haar eigen dreigingsbeeld in kaart te brengen maakt de instelling gebruik van verschillende externe en interne bronnen en van threat intelligence, zoals het One Financial Threat Landscape for the Netherlands (1FTL-NL).
- De instelling brengt haar 'kroonjuwelen' in kaart, evalueert deze periodiek en relateert deze aan actuele cyberdreigingen en getroffen beheersmaatregelen. Daar waar nodig treft de instelling aanvullende beheersmaatregelen. Beheersmaatregelen die niet (meer) effectief werken worden aangepast, vervangen door andere beheersmaatregelen, of uitgefaseerd.
- De instelling beoordeelt periodiek de risicoanalyses van partijen in de keten op relevantie en stelt vast in hoeverre deze voldoen aan de eisen van de instelling.
- De gewogen en geprioriteerde risico's op het gebied van informatiebeveiliging en cyberdreigingen worden door de instelling geadresseerd en beperkt naar een acceptabel niveau dat past bij de risicotolerantie van de instelling.

- De instelling analyseert de risico's die samenhangen met de toepassingen van cryptografische technologie ter ondersteuning van haar bedrijfsprocessen op de korte (1 jaar), middellange (1-5 jaar) en lange (>5 jaar) termijn. Daarbij neemt zij de ontwikkeling van Quantum computing en de mogelijk daaruit voortvloeiende dreigingen voor de instelling in acht.
- De instelling maakt een jaarlijkse update van deze analyse.
- De instelling bespreekt de inventarisatie in het kader van de Risk Management Cycle op niveau van het bestuur.

4.3 Maintenance and monitoring of a risk action plan

Marktstandaarden* geven aan dat de instelling een proces inricht dat onder meer het volgende waarborgt:

- De instelling stelt voor niet geaccepteerde risico's een 'risk action plan' op dat verdere uitwerking geeft aan de risk response.
- In dit 'risk action plan' zijn onder meer restrisico's en de daarvoor benodigde compenserende beheersmaatregelen opgenomen. Deze beheersmaatregelen worden in samenhang met de andere te nemen informatiebeveiliging-maatregelen afgewogen en geprioriteerd ingevoerd.
- Restrisico's op het gebied van cybersecurity zijn onderdeel van het 'risk action plan' van de instelling.
- Het risk action plan wordt geaccordeerd door het management niveau dat past bij de aard, omvang en complexiteit van de restrisico's.
- Het risk action plan is actueel; opvolging van de acties wordt bewaakt.

Let op!

Risicogebaseerd, uitbesteding en het three lines model

Good Practices hierbij zijn:

- De instelling heeft voor actuele cyberdreigingen expliciet gemaakt welke risico's formeel worden geaccepteerd en voor welke restrisico's aanvullende beheersmaatregelen noodzakelijk zijn.
- Beoogde acties op het gebied van cybersecurity en de status van uitvoering zijn beschreven in het risk action plan. Afwijkingen ten opzichte van de oorspronkelijke planning worden periodiek gerapporteerd aan het verantwoordelijk management niveau dat past bij de aard, omvang en complexiteit van deze restrisico's. De instelling laat het lijnmanagement jaarlijks een 'in control' statement (ICS) opstellen.
- De instelling legt periodiek de (her)prioritering van de informatiebeveiliging-maatregelen vast en geeft akkoord op inzet van de rescources. Hierbij wordt de afweging vastgelegd waarom tot welke prioritering is over gegaan.
- De instelling beoordeelt op periodieke basis de risk action plannen van dienstverleners in de keten op relevantie en stelt vast dat deze voldoen aan de eisen van de instelling. Bij afwijkingen maakt de instelling afspraken met die partijen om het risico te beperken naar een acceptabel niveau dat past binnen de risicotolerantie van de instelling.
- De instelling neemt op periodieke basis in haar risk action plannen die controls mee waarbij de dienstverleners niet aan de informatiebeveiliging-eisen van de instelling kan voldoen. De instelling neemt aanvullende beheersmaatregelen als dat nodig is.

5.1 Responsibility for risk, security, compliance and Information Security function

Marktstandaarden* geven aan dat de instelling een proces inricht dat onder meer het volgende waarborgt:

- Het bestuur heeft taken en verantwoordelijkheden op het gebied van het inrichten, beheren en controleren van informatiebeveiliging en cybersecurity belegd.
- Het bestuur draagt actief en zichtbaar het belang uit van informatiebeveiliging en cybersecurity voor de instelling en haar dienstverleners.
- Binnen de instelling heerst een bewustzijnscultuur met betrekking tot de verantwoordelijkheid van de medewerkers om beveiligingsprocessen en -procedures na te leven en te onderhouden.
- De instelling zet, binnen haar governancesysteem en in overeenstemming met het evenredigheidsbeginsel, een informatiebeveiligingsfunctie op, waarbij de verantwoordelijkheden zijn toegewezen aan een specifieke medewerker.
- De instelling zorgt dat de onafhankelijkheid en objectiviteit van deze informatiebeveiligingsfunctie is gewaarborgd door deze op passende wijze te scheiden van verantwoordelijkheden voor processen inzake ICT-activiteiten en bedrijfsvoering.
- De informatiebeveiligingsfunctie rapporteert aan het bestuur.

Let op!

Risicogebaseerd, uitbesteding en het three lines model

Good Practices hierbij zijn:

- Het bestuur van de instelling draagt het belang van informatiebeveiliging en cybersecurity zichtbaar en actief uit.
- De instelling heeft taken, verantwoordelijkheden en bevoegdheden ten aanzien van informatiebeveiliging belegd op alle organisatieniveaus.
- De instelling heeft een Chief Information Security Officer (CISO) benoemd die rechtstreeks rapporteert aan het bestuur.
- Specifieke verantwoordelijkheden op het gebied van informatiebeveiliging en cybersecurity beheersmaatregelen zijn belegd bij een Computer Security Incident Response Team (CSIRT) of Security Operations Center (SOC).
- De instelling gaat zowel bij het aangaan van kritieke of belangrijke uitbestedingsrelaties als bij het monitoren van die relaties na dat bovenstaande punten van toepassing zijn bij haar ketenpartners.

5.2 Management of information security and tasks of the information security function

Marktstandaarden* geven aan dat de instelling een proces inricht dat onder meer het volgende waarborgt:

- De instelling heeft een informatiebeveiligingsfunctie ingericht.
- De taken van de informatiebeveiligingsfunctie zien ten minste op:
  a. het ondersteunen van het bestuur bij het opstellen en bijhouden van het informatiebeveiligingsbeleid, de controle van de uitrol en implementatie daarvan;
  b. het aan het bestuur regelmatig en op ad-hoc basis verslag uitbrengen en advies geven over de status van de informatiebeveiliging en de ontwikkelingen ervan;
  c. het monitoren en beoordelen van de uitvoering van de informatiebeveiligingsmaatregelen;
  d. het zorgen dat aan de vereisten op het gebied van informatiebeveiliging wordt voldaan in het geval dat werkzaamheden zijn uitbesteed aan dienstverleners;
  e. het waarborgen dat alle medewerkers en dienstverleners die toegang hebben tot informatie en systemen, op passende wijze zijn geïnformeerd over de beleidslijnen voor informatiebeveiliging;
  f. het coördineren van onderzoek naar operationele of beveiligingsincidenten en de relevante incidenten rapporteren aan het bestuur.

Let op!

Risicogebaseerd, uitbesteding en het three lines model

Good Practices hierbij zijn:

- Het uitrollen van opleidings- en bewustmakingssessies over informatiebeveiliging voor medewerkers.
- Voor de inrichting van informatiebeveiliging en cybersecurity maakt de instelling gebruik van internationaal geaccepteerde standaarden, zoals de ISO 27000 serie.
- Informatiebeveiliging (inclusief cybersecurity) is onderdeel van het takenpakket van zowel de 1e, 2e als 3e lijn. Dit komt tot uitdrukking in organisatieschema's en functiebeschrijvingen.
- De instelling voert regelmatig overleg met haar dienstverleners op verschillende niveaus over de beheersing van risico's op het gebied van informatiebeveiliging en cybersecurity. De instelling maakt hiervan een vastlegging.
- Hierin wordt nagegaan op welke punten in de keten verbeteringen en/of acties noodzakelijk zijn (PDCA cyclus). De opvolging van deze acties wordt gevolgd.
- Zowel vanuit de 1e, 2e als 3e lijn (bij de instelling en bij de dienstverleners) wordt input gegeven aan deze periodieke bespreking.
- Over de beheersing van risico's op het gebied van informatiebeveiliging en cybersecurity wordt regelmatig door de informatiebeveiligingsfunctie verantwoording afgelegd aan het bestuur/directie van de instelling.

6.1 Data and system ownership

Marktstandaarden* geven aan dat de instelling een proces inricht dat onder meer het volgende waarborgt :

- Het eigenaarschap van alle gegevens en informatiesystemen die de instelling gebruikt bij haar bedrijfsvoering is eenduidig belegd.
- Gegevens en informatiesystemen zijn door de systeemeigenaar geclassificeerd. Beheersmaatregelen zijn in overeenstemming met deze classificatie bepaald. Zie beheersmaatregel 2.2.

Let op!

Risicogebaseerd, uitbesteding en het three lines model

Good Practices hierbij zijn:

- De instelling heeft in een beleidsdocument uitgangspunten geformuleerd ten aanzien van eigenaarschap, bewaarlocaties, bewaartermijnen en van toepassing zijnde wet- en regelgeving.
- De instelling houdt een overzicht bij van alle informatie-systemen en gegevens en de daarvoor verantwoordelijke eigenaren.
- De instelling heeft voor uitbestede ICT-systemen en cloud-diensten overeenkomsten met de clouddienstverleners afgesloten. Hierin is vastgesteld wie de eigenaar is van de gegevens en de informatiesystemen en waar deze zich bevinden.
- De instelling heeft gedragsregels opgesteld en gecommuniceerd waarin staat dat medewerkers zorgvuldig omgaan met gegevens (veilig omgaan met e-mail en clean desk policy). Op naleving van de gedragsregels wordt toegezien.
- De instelling heeft toegang tot klantdossiers beperkt op basis van whitelisting op dossier/klantniveau. Specifieke data-elementen zijn afgeschermd, zoals bijzondere persoonsg-egevens en inkomensgegevens. Het raadplegen van dossiers wordt gelogd; de logging wordt periodiek gereviewd en uitzonderingen worden uitgezocht met de data eigenaar.

7.1 Segregation of duties

Marktstandaarden* geven aan dat de instelling een proces inricht dat onder meer het volgende waarborgt:

- Het bestuur ziet er op toe dat ongewenste functie-vermengingen (toxic combinations) en de daarmee samenhangende risico's door de instelling worden vermeden ook in het geval dat kritieke of belangrijke werkzaamheden zijn uitbesteed.
- Functiescheidingen zijn gebaseerd op de inrichting van de AO/IC van de instelling.
- Functiescheidingen zijn verder uitgewerkt op basis van een risicoanalyse, geïmplementeerd en goedgekeurd door het senior management.
- Bij het definiëren en implementeren van functiescheiding zijn de principes "need-to-know" en "least privileged" als uitgangspunt gebruikt en is het concept meegenomen dat kritieke taken en functies over meer dan 1 persoon zijn verdeeld.
- De implementatie van relevante procedures ten aanzien van functiescheiding worden periodiek beoordeeld en herzien indien nodig.

Let op!

Risicogebaseerd, uitbesteding en het three lines model

Good Practices hierbij zijn:

- De instelling heeft een formeel vastgestelde norm voor functiescheidingen in de vorm van een autorisatiematrix opgesteld.
- Aan de hand van de autorisatiematrix (soll) controleert de instelling periodiek of autorisaties conform de vereisten van functiescheiding in de ICT-systemen (ist) zijn afgedwongen (soll-ist vergelijking).
- De implementatie van functiescheidingen in ICT-systemen wordt periodiek beoordeeld. Nadat majeure wijzigingen in ICT-systemen zijn aangebracht vindt een tussentijdse beoordeling plaats.
- De instelling heeft op basis van een risicogebaseerde benadering niet alleen de gewenste functiescheidingen per applicatie in kaart, maar nadrukkelijk ook per proces indien dit proces wordt ondersteund door meerdere applicaties. Dit voorkomt dat functiescheidingen op procesniveau kunnen worden doorbroken, terwijl deze per individuele applicatie in het proces wel conform de eisen zijn ingericht.
- De instelling minimaliseert het aantal accounts met hoge rechten. Met een dergelijke aanpak kunnen ongewenste functievermengingen (toxic combinations) en de daarmee samenhangende risico's worden vermeden.
- De instelling is alert op het voorkomen dat rollen van projectmedewerkers conflicteren met hun rol in de uitvoering van hun lijntaken. Uitzonderingen worden gedetecteerd en ter (tijdelijke) acceptatie voorgelegd aan het management.
- Voor accounts met hoge rechten (bijvoorbeeld beheerdersaccounts) past de instelling two-factor authenticatie toe.
- De instelling staat het gebruik van generieke en gedeelde accounts niet toe; voor uitzonderingen op deze regel tekent senior management af.
- De functiescheiding wordt ondersteund door een adequaat Identity and Access Managementsysteem (IAM), zie ook de controls 17.1 en 17.2.

8.1 Personnel recruitment and retention

Marktstandaarden* geven aan dat de instelling een proces inricht dat onder meer het volgende waarborgt:

- De instelling trekt voldoende medewerkers aan met ervaring en kennis van informatiebeveiliging en cybersecurity die past bij de ambitie en het risicoprofiel van de instelling.
- De instelling investeert in het op peil houden van het kennisniveau van medewerkers door middel van opleidingen en trainingen op het gebied van informatiebeveiliging en cybersecurity.

Let op!

Risicogebaseerd, uitbesteding en het three lines model

Good Practices hierbij zijn:

- De instelling heeft overeenkomsten gesloten met gespecialiseerde partijen om kennis van haar medewerkers en beleidsbepalers op het gebied van informatiebeveiliging en cybersecurity actueel te houden.
- De instelling heeft een gap analyse opgesteld waaruit blijkt hoe zij in de toekomst het kennisniveau op het gebied van informatiebeveiliging en cybersecurity van haar medewerkers up-to-date houdt.
- Het bestuur is zich voldoende bewust en handelt daarnaar, dat zij zelf het doelwit van een aanval kunnen zijn.

8.2 Personnel competencies and culture

Marktstandaarden* geven aan dat de instelling een proces inricht dat onder meer het volgende waarborgt:

- Het bestuur, raad van toezicht, raad van commissarissen en sleutelfunctiehouders hebben aantoonbaar trainingen en opleidingen gevolgd om de belangrijkste ICT-risico's en beheersmaatregelen voor hun instelling te kunnen begrijpen.
- Het bestuur vertoont goed voorbeeldgedrag ten aanzien van bewustzijn voor risico's op het gebied van informatiebeveiliging en cybersecurity en het naleven van procedures die de informatiebeveiliging borgen (tone-at-the-top).
- Zogeheten 'management overrides' van bestaande processen en procedures door het bestuur en senior management worden waar mogelijk vermeden.
- Kennis en competenties van medewerkers en beleidsbepalers op het gebied van informatiebeveiliging en cybersecurity sluiten aan bij de (digitale) ambities van de instelling.
- Periodiek gaat de instelling na in hoeverre de kennis en competenties van medewerkers en beleidsbepalers op het gebied van informatiebeveiliging en cybersecurity (nog) aansluiten bij de (digitale) ambities van de instelling.
- De instelling brengt bij hoge impact incidenten door middel van root cause analyses in kaart in hoeverre de cultuur cq de gedragingen van bepaalde medewerkers heeft bijgedragen aan het incident. Naar aanleiding van deze analyse worden mitigerende beheersmaatregelen ingericht.

Let op!

Risicogebaseerd, uitbesteding en het three lines model

Good Practices hierbij zijn:

- Budgetten voor permanente educatie op gebied van informatiebeveiliging en cybersecurity zijn vastgesteld en toereikend.
- Beleidsbepalers binnen de instelling beschikken ten minste over basiskennis van informatiebeveiliging en cybersecurity. Zij hebben aantoonbaar trainingen en opleidingen gevolgd om de belangrijkste ICT-risico's en beheersmaatregelen voor hun instelling te kunnen begrijpen.
- In functiebeschrijvingen is opgenomen welke kennis en competenties van medewerkers ten aanzien van informatie-beveiliging en cybersecurity wordt verwacht.
- De instelling heeft een opleidingsplan uitgewerkt op grond waarvan de kennis van cybersecurity experts bijblijft bij actuele ontwikkelingen rondom cyberdreigingen. De realisatie van dit plan wordt gemonitord.
- De instelling heeft in een root cause analyse cultuuraspecten (bijvoorbeeld slordigheden, ontevreden medewerkers) op bepaalde afdelingen waar incident(en) hebben plaats gevonden betrokken.
- De instelling betrekt cultuuraspecten (bijvoorbeeld slordig-heden, ontevreden medewerkers) in root cause analyses van incidenten.

8.3 Dependence upon individuals

Marktstandaarden* geven aan dat de instelling een proces inricht dat onder meer het volgende waarborgt:

- De instelling heeft geïnventariseerd op welke voor de uitoefening van haar bedrijf kritieke processen/activiteiten zij afhankelijk is van een beperkt aantal medewerkers.
- Op grond van een risicoanalyse bepaalt de instelling waar de afhankelijkheid van individuen haar risicotolerantie overschrijdt.
- De instelling treft beheersmaatregelen om te grote afhankelijkheid van individuen te beperken binnen haar risicotolerantiegrenzen.

Let op!

Risicogebaseerd, uitbesteding en het three lines model

Good Practices hierbij zijn:

- De instelling heeft een inventarisatie gemaakt waaruit het key person risk blijkt.
- Uitgewerkte trainingsprogramma's zijn er onder meer op gericht om kennis en ervaring ook op het gebied van informatiebeveiliging en cybersecurity breder te verspreiden.
- Taakroulatie en successieplanning voor kritieke functies binnen de instelling.
- De instelling past aantoonbaar taakroulatie en successie-planningen voor kritieke functies toe.

8.4 Personnel clearance procedures

Marktstandaarden* geven aan dat de instelling een proces inricht dat onder meer het volgende waarborgt:

- Voorafgaand aan de indiensttreding wordt personeel gescreend in relatie tot het risicoprofiel van de functie.
- Tijdens het dienstverband wordt de screening periodiek herhaald.
- Bovenstaande is van toepassing op zowel eigen medewerkers als op ingehuurde medewerkers.

Let op!

Risicogebaseerd, uitbesteding en het three lines model

Good Practices hierbij zijn:

- De instelling heeft functieprofielen opgesteld waarin onderscheid is gemaakt tussen functies met een hoog, gemiddeld en laag risicoprofiel.
- De pre-employment screeningsvereisten zijn vastgelegd, bekrachtigd en worden gehanteerd binnen het werving- en selectieproces.
- De instelling heeft aantoonbaar verklaringen omtrent gedrag (VOG) opgevraagd voor functies met een gemiddeld of hoog risicoprofiel en trekt referenties na.
- Risicogebaseerd wordt periodiek een in-employment screening uitgevoerd voor gemiddelde en hoge risico functies.

8.5 Job change and termination

Marktstandaarden* geven aan dat de instelling een proces inricht dat onder meer het volgende waarborgt:

- Bij functiewijzigingen worden rechten in ICT-systemen en processen zo snel mogelijk aangepast. Toegangsrechten waarover de medewerker uit hoofde van de nieuwe functie niet meer mag beschikken, worden per direct ingetrokken.
- De instelling trekt bij uitdiensttreding rechten in systemen en processen per direct in. Hierbij wordt ook aandacht besteed aan toegangsrechten tot systemen / diensten die buiten het beheer van de instelling vallen, zoals bijvoorbeeld internetportalen of cloud toepassingen waarop de (ex) werknemer namens de instelling geabonneerd is.

Let op!

Risicogebaseerd, uitbesteding en het three lines model

Good Practices hierbij zijn:

- De instelling maakt gebruik van User Provisioning, waarbij toegangsrechten in ICT-systemen automatisch, vanuit het HR-systeem worden aangemaakt, gewijzigd, geblokkeerd en verwijderd.
- Bij het Identity Access Management wordt specifieke aandacht besteed aan *joiners*, *leavers* en *movers*. Zie ook beheersmaatregelen 17.1 en 17.2.
- De instelling houdt (handmatig of geautomatiseerd) een register bij van tools, portalen en/of cloud toepassingen waar haar medewerkers uit hoofde van hun functie toegang toe hebben. Bij uitdiensttreding of functiewijziging worden de toegangsrechten van de desbetreffende medewerker overgedragen naar een andere medewerker.

9.1 Knowledge transfer to end users

Marktstandaarden* geven aan dat de instelling een proces inricht dat onder meer het volgende waarborgt:

- Medewerkers beschikken over de kennis en vaardigheden om correct gebruik te maken van ICT-applicaties en ICT-systemen in overeenstemming met procedures en werkinstructies van de instelling.
- Medewerkers weten hoe informatietechnologie hun kritieke bedrijfsprocessen ondersteunt en kennen de met die technologie verband houdende risico's ten aanzien van informatiebeveiliging en cybersecurity. Medewerkers passen die kennis toe in hun dagelijkse operationele werkzaamheden.

Let op!

Risicogebaseerd, uitbesteding en het three lines model

Good Practices hierbij zijn:

- Medewerkers ontvangen periodiek functionele trainingen over het correct gebruik van ICT-applicaties en ICT-infrastructuur, waarbij tevens aandacht wordt geschonken aan informatiebeveiligings- en cybersecurity aspecten.
- Werkinstructies voor het correct gebruik van ICT-applicaties en ICT-infrastructuur zijn beschikbaar in de vorm van interne wiki's, intranet en helpfuncties in de applicaties en systemen.
- De instelling is er in (SLR) gesprekken met dienstverleners alert op dat kennisontwikkeling en kennisdeling door medewerkers ook bij de dienstverlener voldoende aandacht krijgt.

9.2 Knowledge transfer to operations and support staff

Marktstandaarden* geven aan dat de instelling een proces inricht dat onder meer het volgende waarborgt:

- ICT-medewerkers beschikken over de kennis en vaardigheden om applicaties en systemen te ontwikkelen, aan te schaffen, te implementeren en te beheren in overeenstemming met procedures en werkinstructies van de instelling.
- ICT-medewerkers weten hoe informatietechnologie hun kritieke bedrijfsprocessen ondersteunt en kennen de met die technologie verband houdende risico's ten aanzien van informatiebeveiliging en cybersecurity. ICT-medewerkers passen die kennis toe in hun dagelijkse operationele werkzaamheden.
- ICT-medewerkers zetten hun specialistische kennis actief in om informatiebeveiligingsrisico's en cyberdreigingen te herkennen en met passende beheersmaatregelen te beheersen. Hierbij is aandacht voor het belang van (permanente) educatie op het gebied van cybersecurity (naast het monitoren van ontwikkelingen).

Let op!
Risicogebaseerd, uitbesteding en het three lines model

Good Practices hierbij zijn:

- Gerichte security trainingen voor specifieke doelgroepen, zoals ICT-systeemontwikkelaars, helpdeskmedewerkers, ICT-beheerders en medewerkers met een rol in informatiebeveiliging en cybersecurity.
- De instelling is er in (SLR) gesprekken met dienstverleners alert op dat kennisontwikkeling en permanente educatie van specialisten ook bij de dienstverlener voldoende aandacht krijgt.

9.3 Employee awareness

Marktstandaarden* geven aan dat de instelling een proces inricht dat onder meer het volgende waarborgt:

- Het bestuur heeft aantoonbaar op hen toegesneden trainingen en opleidingen gevolgd om de belangrijkste ICT-risico's en beheersmaatregelen voor haar instelling te kunnen begrijpen en adresseren.
- Het bestuur vertoont goed voorbeeldgedrag ten aanzien van bewustzijn voor risico's op het gebied van informatiebeveiliging en cybersecurity en het naleven van procedures die de informatiebeveiliging borgen (tone-at-the-top). Vastgestelde richtlijnen en gedragscodes met betrekking tot informatiebeveiliging en cybersecurity. Deze zijn bekend bij medewerkers in alle lagen van de instelling.
- Het verhogen van het beveiligingsbewustzijn maakt deel uit van het informatiebeveiligingsbeleid, waarbij een security awareness (opleidings)programma is geïmplementeerd. Hierin wordt expliciet aandacht besteed aan cybersecurity risico's.
- De instelling zorgt ervoor dat het opleidingsprogramma regelmatig opleiding verzorgt voor alle personeelsleden.
- Medewerkers weten hoe te handelen wanneer zij vermoeden of signaleren dat risico's op het gebied van informatiebeveiliging en cybersecurity zich voordoen.

Let op!

Risicogebaseerd, uitbesteding en het three lines model

Good Practices hierbij zijn:

- In het kader van *security awareness* is een trainingsprogramma opgesteld voor alle medewerkers om ervoor te zorgen dat zij zijn opgeleid om hun taken en verantwoordelijkheden uit te voeren in overeenstemming met het relevante informatie-beveiligingsbeleid en procedures om menselijke fouten, diefstal, fraude, misbruik of verlies te verminderen.
- De instelling zet een mix van middelen in om security awareness te onderhouden en te verbeteren bij haar eigen medewerkers en externen. Hiertoe zijn security coördinatoren binnen de instelling aangesteld.
- Voor het verder verbeteren van security awareness worden presentaties, phishing campagnes, mystery guests en e-learnings toegepast. Deelname aan e-learnings is door de instelling verplicht gesteld; resultaten worden gemeten en opgevolgd.
- De instelling gebruikt aansprekende voorbeelden uit de (eigen) praktijk in het *security awareness* programma, zoals beveiligingsincidenten die zich hebben voorgedaan. Hierbij is aandacht besteed aan o.a. CEO fraude, gijzelsoftware en spear phishing in periodes waarin de instelling mogelijk kwetsbaarder is door (einde jaar) drukte, vakanties of onderbezetting.
- Zogeheten 'management overrides' van bestaande processen en procedures door het bestuur en senior management worden vermeden.
- De instelling onderneemt initiatieven om samen met uitbestedingspartners bewustwording op het gebied van cybersecurity te vergroten.

10.1 Change standards and procedures

Marktstandaarden* geven aan dat de instelling een proces inricht dat onder meer het volgende waarborgt:

- Wijzigingen, inclusief security patches in ICT-applicaties, ICT-infrastructuur, ICT-processen en kritieke systeeminstellingen volgen een gestandaardiseerd en gecontroleerd pad, worden geprioriteerd en geëvalueerd.
- Taken en verantwoordelijkheden met betrekking tot het controleren en goedkeuren van wijzigingsverzoeken zijn belegd.
- Technische doelstellingen en functionele en niet-functionele vereisten, waaronder die op het gebied van informatiebeveiliging zijn gedefinieerd en vastgelegd, voordat ontwikkelingsactiviteiten of systeemverwerkingen worden gestart.
- Beheersaatregelen zijn getroffen om onbedoelde wijziging of opzettelijke manipulatie van de ICT-systemen tijdens de ontwikkeling te voorkomen.
- Wijzigingen in kritieke systemen en infrastructuur worden niet door één en dezelfde persoon aangevraagd, goedgekeurd en geïmplementeerd (functiescheiding).
- De ontwikkeling, uitvoering, werking en/of configuratie van de ICT-systemen vinden in gescheiden systemen plaats en worden gedocumenteerd (audit trail).
- De ICT-systemen die worden ontwikkeld of beheerd door eindgebruikers volgen eveneens een gestandaardiseerd en gecontroleerd pad dat voorziet in passende beheersing op het gebied van prioritering, registratie en evaluatie.

Let op!

Risicogebaseerd, uitbesteding en het three lines model

Good Practices hierbij zijn:

- De instelling borgt dat verzoeken tot systeemontwikkeling op een gestructureerde wijze worden vastgelegd en afgehandeld, bijvoorbeeld in een centraal registratiesysteem.
- Het changemanagementproces is gebaseerd op internationale standaarden en werkwijzen, zoals ITIL, Agile, Scrum, Devops.
- De instelling werkt volgens het shift left principe dat ervan uitgaat dat Agile, Scrum, Devops teams applicatiebeveiliging in de vroegste stadia van systeemontwikkeling meeneemt.
- De instelling gebruikt ook bij Agile, Scrum, Devops een workflow systeem dat het gehele proces van wijzigingsverzoek tot en met implementatie ondersteunt, inclusief logging en documentatie.
- De instelling heeft functiescheiding toegepast in haar Agile, Scrum, Devops systeemontwikkeling met betrekking tot bijvoorbeeld operations en control cq development en security.
- Beheersmaatregelen zijn getroffen ter bescherming van de integriteit van de broncode van ICT-systemen.
- Secure Coding richtlijnen worden gehanteerd door interne ontwikkelaars, dan wel dienstverleners die appplicatiediensten aanbieden waar ontwikkelactiviteiten door worden ondernomen.
- Geautomatiseerde scans/review van code vinden op deze Secure Coding Richtlijnen plaats zoals ook geautomatiseerde scans/review van code en configuratie op kwetsbaarheden (zoals OWASP bij web ontwikkeling).
- Bij gebruik van open source libraries in de code worden deze vóór in productiename geautomatiseerd en gecontroleerd op kwetsbaarheden.
- De impactanalyse van een wijziging houdt rekening met een terugval scenario voor het geval dat de wijziging niet succesvol is.
- De instelling heeft een Change Advisory Board (CAB) ingesteld waarin verschillende disciplines zoals business, ICT en ICT-Risk/ ICT Security besluiten nemen over wijzigingen.

- Verschillende disciplines zoals business, ICT en ICT Risk/ICT Security zijn voldoende en tijdig betrokken bij besluiten over wijzigingen.
- De instelling herijkt de changemanagement procedure jaarlijks.

10.2 Impact assessment, prioritisation and authorisation

Marktstandaarden* geven aan dat de instelling een proces inricht dat onder meer het volgende waarborgt:

- De instelling gaat na in hoeverre voorgenomen wijzigingen in de operationele omgeving gevolgen hebben voor de bestaande beveiligingsmaatregelen en of er aanvullende beheersmaat-regelen noodzakelijk zijn om het risico's in kwestie te verminderen. In deze beoordeling worden de belangen van alle relevante stakeholders meegewogen in de besluitvorming over wijzigingsverzoeken.
- De instelling prioriteert wijzigingen voortkomend uit de impact assessment.
- Dringende of op korte termijn noodzakelijke ICT-wijzigingen zijn traceerbaar en worden gemeld aan de betreffende eigenaar van de ICT-asset voor analyse achteraf.

Let op!
Risicogebaseerd, uitbesteding en het three lines model

Good Practices hierbij zijn:

- De informatiebeveiligingsrol of -functionaris binnen de instelling is betrokken bij de beoordeling van de impact van wijzigingsverzoeken op de beheersmaatregelen die in het kader van informatiebeveiliging en cybersecurity zijn getroffen.
- De instelling weegt bij het bepalen van de impact en prioriteit van wijzigingsverzoeken de informatiebeveiligingsaspecten van de wijzigingen expliciet mee.
- De instelling prioriteert de uitkomsten van een impact assessment door middel van een classificatie van de wijziging (bijvoorbeeld: standaard, normaal, urgent, spoed).

10.3 Test environment

Marktstandaarden* geven aan dat de instelling een proces inricht dat onder meer het volgende waarborgt:

- Criteria voor het beschermen van testgegevens zijn opgesteld en worden onderhouden.
- Toegang tot test- en productie ICT-systemen is strikt gescheiden. Dit wordt voor alle omgevingen vooraf en achteraf gecontroleerd.
- De instelling heeft een omgeving beschikbaar waarin zij de effectiviteit van security beheersmaatregelen test.
- De instelling let op het versiebeheer wanneer de software versie van de testomgeving gelijk is aan de productieomgeving.
- Test- en productiegegevens worden niet vermengd.
- De instelling gebruikt in de test omgeving geen ongeschoonde productiedata.

Let op!

Risicogebaseerd, uitbesteding en het three lines model

Good Practices hierbij zijn:

- Het User-ID en password of andere authenticatie van beheerders in de testomgeving zijn nooit gelijk aan die van de productie omgeving.
- De instelling test uitsluitend met geanonimiseerde representatieve testdata in een van de productie afgescheiden testomgeving.
- De instelling gebruikt specifieke software voor het schonen en anonimiseren van data.
- Test- en productiesystemen zijn logisch of fysiek gescheiden. De instelling hanteert de OTAP modellen en checkt aan de hand van steekproeven de naleving van de scheiding tussen omgevingen.
- De instelling heeft een representatieve omgeving om de effectiviteit van nieuwe en gewijzigde (security) infrastructuur zoals IDS, SIEM, Web Application Firewall (WAF), routers etc. te testen.

10.4 Testing of changes

Marktstandaarden* geven aan dat de instelling een proces inricht dat onder meer het volgende waarborgt:

- Wijzigingen in de ICT-infrastructuur en ICT-applicaties worden getest voordat zij in gebruik (productie) worden genomen.
- De tests worden uitgevoerd volgens een testplan waarin ook acceptatiecriteria voor informatiebeveiliging en ICT-performance zijn opgenomen.
- De instelling heeft een autorisatieflow gedefinieerd waarin staat welke personen geautoriseerd zijn om te kunnen testen.
- Security testen maken onderdeel van het ontwikkel en test proces voordat wijzigingen worden doorgevoerd.
- De instelling scant gewijzigde ICT-systemen voor inproductie-name op kwetsbaarheden voor cyberdreigingen op grond van een risico-inschatting.

Let op!

Risicogebaseerd, uitbesteding en het three lines model

Good Practices hierbij zijn:

- De instelling voert verschillende tests uit (zoals een systeem-test, gebruikers acceptatietest, regressietest en integratietest) om de effectiviteit van beveiligingsmaatregelen in gewijzigde applicaties en infrastructuur vast te stellen. Bij een agile werkwijze wordt software getest op grond van acceptatie-criteria (definition of done).
- In de acceptatiecriteria is opgenomen dat onder meer aan de volgende elementen wordt voldaan: de toegangsbeveiliging functioneert, autorisaties werken conform specificaties, vertrouwelijke gegevens zijn versleuteld, kritieke handelingen worden gelogd en de systeemperformance voldoet aan de gestelde eisen.
- Bij het testen van wijzigingen worden beheersmaatregelen van informatiebeveiliging en cybersecurity expliciet meegenomen, bijvoorbeeld door middel van security & vulnerability scanning en source code reviews.
- Daar waar ICT-applicaties zijn uitbesteed, stelt de instelling risicogebaseerd vast dat de belangrijkste functionaliteit en beveiligingsmaatregelen werken conform specificaties.

10.5 Promotion to production

Marktstandaarden* geven aan dat de instelling een proces inricht dat onder meer het volgende waarborgt:

- Beheerste overdracht van wijzigingen in productiesystemen vindt plaats.
- De belangrijkste belanghebbenden bij systeemwijzigingen, zoals gebruikers, systeemeigenaar, functioneel en technisch beheerders zijn betrokken bij de overdracht van de wijzigingen en het goedkeuringsproces.
- In logs wordt bijgehouden en daarna gecheckt of wijzigingen conform de afspraken zijn uitgevoerd door daartoe geautoriseerde personen.
- Op grond van een risicoanalyse bepaalt de instelling of een nieuw of aangepast ICT-systeem parallel naast het oude systeem gebruikt wordt. Bij risicovolle aanpassingen heeft de instelling voorzien in een fall-back plan.

Let op!

Risicogebaseerd, uitbesteding en het three lines model

Good Practices hierbij zijn:

- De instelling stelt overdrachtsprocedures vast voor het in gebruik nemen van wijzigingen in de ICT-infrastructuur en ICT-applicaties.
- De autorisaties om wijzigingen in productie door te voeren zijn niet voortdurend aan medewerkers toegekend maar worden op tijdelijke basis toegekend.
- De instelling gebruikt een workflow systeem ten behoeve van de gecontroleerde overdracht en registratie van wijzigingen in de productieomgeving.
- De instelling maakt gebruik van privileged acces management tools die tijdelijke autorisaties afgeven en volgen.
- Wijzigingen in bedrijfskritieke systemen en wijziging van beveiligingsparameters vinden plaats onder het 4-ogen principe.
- De instelling logt alle wijzigingen in de productieomgeving. Op basis hiervan wordt periodiek nagegaan dat geen ongeautoriseerde wijzigingen hebben plaatsgevonden.
- De instelling houdt verscherpte aandacht voor security issues nadat majeure of kritieke wijzigingen in productie zijn genomen, gedurende een van te voren bepaalde periode.

11.1 ICT Business impact analysis and ICT Continuity plans

Marktstandaarden* geven aan dat de instelling een proces inricht dat onder meer het volgende waarborgt:

- Het bestuur is verantwoordelijk voor het vaststellen en goedkeuren van een business impact analysis en een daar uit voortvloeiend continuïteitsplan om de impact van een grote verstoring op de belangrijkste bedrijfsfuncties en -processen te beperken.
- Het bestuur controleert jaarlijks of het business impact analysis en het -continuïteitsplan actueel zijn. Het bestuur ziet erop toe dat belangrijke wijzigingen in IT-systemen of dienstverlening direct in het continuïteitsplan worden verwerkt.
- De instelling voert de business impact analysis uit om de blootstelling aan ernstige bedrijfsonderbrekingen, zowel kwantitatief als kwalitatief, te beoordelen met behulp van interne en/of externe gegevens en scenarioanalyses.
- De instelling zorgt ervoor dat de beschikbaarheid van kritieke ICT-systemen en ICT-diensten ontworpen en afgestemd zijn op hun business impact analysis.
- In het business impact analysis en ICT-continuïteitsplan zijn verschillende scenario's opgenomen waarbij rekening is gehouden met de continuïteit van cybersecurity beheersmaatregelen en de ongestoorde voortzetting van informatiebeveiligingsfuncties tijdens verstoringen en cyberaanvallen.
- Crisismanagement is ingericht, inclusief de daarbij behorende communicatieprotocollen.
- Alternatieve verwerkings- en herstelmogelijkheden voor alle kritieke ICT-services zijn in het ICT-continuïteitsplan voorhanden.
- Bij een storing of noodsituatie, en tijdens de uitvoering van de bedrijfscontinuïteitplannen, zorgt de instelling ervoor dat ze doeltreffende crisiscommunicatie maatregelen treft.
- Daarbij zijn alle relevante interne en externe belanghebbenden, waaronder relevante toezichthoudende autoriteiten, tijdig op de hoogte gebracht.

Let op!

Risicogebaseerd, uitbesteding en het three lines model

Good Practices hierbij zijn:

- De instelling heeft een crisibeheersingsfunctie die, onder meer, duidelijke procedures vaststelt voor het geval dat IT Business Continuity-plannen geactiveerd worden. Dit omvat ook interne en externe crisiscommunicatie.
- De instelling heeft haar beleidslijnen voor ICT-continuïteit op passende wijze gecommuniceerd binnen de instelling, bijvoorbeeld via een interne website naar alle relevante personeelsleden en, waar van toepassing, ook naar externe dienstverleners.
- De instelling heeft hard copies van de continuïteitsplannen op een voor de direct- betrokken medewerkers bekende en toegankelijke locatie. Een lijst van belangrijke telefoonnummers en e-mailadressen is onderdeel daarvan.
- De instelling heeft per afdeling in kaart gebracht welke processen kritiek zijn en welke personen direct betrokkenen zijn.
- Bij het implementeren van een nieuw systeem of applicatie neemt de instelling deze op in een geactualiseerde versie van het ICT-continuïteitsplan en bijbehorende testcyclus.
- De instelling maakt gebruik van dienstverleners om hinder van DDoS-aanvallen te voorkomen, bijvoorbeeld van NaWas: de nationale wasstraat van de Nationale Beheersorganisatie Internet Providers, NBIP.

11.2 Testing of the ICT Continuity plan

Marktstandaarden* geven aan dat de instelling een proces inricht dat onder meer het volgende waarborgt:

- Het bestuur is betrokken bij het opstellen van de continuïteitsplannen en neemt actief deel aan het testen van het ICT continuïteitsplan.
- Testscenario's worden in kaart gebracht van waaruit een test kalender/planning wordt opgesteld voor het testen van de ICT-continuïteitsplannen.
- Het testen van het ICT-continuïteitsplan toont aan dat de instelling kan functioneren op een vooraf vastgesteld minimum essentieel dienstenniveau totdat de volledige werking weer is hersteld.
- De weerbaarheid tegen cyberaanvallen met een impact op de beschikbaarheid, wordt in de scenario's meegenomen en getest.
- Het testen van de continuïteitsmaatregelen dekt de gehele keten van systemen en applicaties af die de kritieke bedrijfsprocessen ondersteunen.
- Testresultaten worden gedocumenteerd en geïdentificeerde tekortkomingen worden geanalyseerd, opgevolgd en gerapporteerd aan het bestuur.

Let op!

Risicogebaseerd, uitbesteding en het three lines model

Good Practices hierbij zijn:

- De instelling bereidt het testen van het ICT-continuïteitsplan zorgvuldig voor, rapporteert over de testresultaten en zorgt voor opvolging van actiepunten. Bij majeure bevindingen of tekortkomingen voert de instelling een hertest uit om vast te stellen dat geadresseerde bevindingen en tekortkomingen daadwerkelijk tot het gewenste resultaat leiden.
- De instelling plant structureel capaciteit bij zowel business als ICT staff voor het testen van business continuity of uitwijk testen.
- De instelling neemt ketenpartners mee in het testen van continuïteitsmaatregelen. Uitkomsten van de testen worden met de ketenpartners besproken en indien van toepassing worden verbeteracties bepaald.
- Bij het implementeren van een nieuw systeem of applicatie neemt de instelling deze op in een vernieuwde versie van het ICT-continuïteitsplan en bijbehorende testcyclus.
- In haar testscenario's neemt de instelling expliciet cybersecurity dreigingen zoals (D)DoS en Advanced Persistent Threats (APT's) op. Voor het opzetten van continuïteitstesten maakt de instelling gebruik van ervaringen van testen binnen de sector en incidenten met impact op de bedrijfscontinuïteit, bijvoorbeeld via de sector ISAC.

11.3 Uncompromisable back-up storage

Marktstandaarden* geven aan dat de instelling een proces inricht dat onder meer het volgende waarborgt:

- De instelling beschikt over meer dan één locatie voor de opslag van data die nodig is voor de uitoefening van een beheerste bedrijfsvoering.
- De instelling bepaalt op grond van de business impact analyse welke back-up data onveranderbaar, volledig en juist moet blijven en treft daarbij passende beheersmaatregelen.
- De locaties zijn veilig, bevinden zich op voldoende afstand van elkaar en zijn toegankelijk voor geautoriseerde personen om zo de continuïteit van kritieke of belangrijke functies te kunnen waarborgen in het geval dat de primaire verwerkingslocatie niet meer beschikbaar is. Hierbij wordt rekening gehouden met catastrofale scenario's.
- Het risicoprofiel van de locaties is zodanig dat een calamiteit niet alle locaties tegelijkertijd kan treffen.
- De inhoud van de back-up wordt periodiek door de eigenaars van de bedrijfsprocessen en het ICT-personeel bepaald.
- De beschikbaarheid van de data op de verschillende locaties (back-up / data mirroring) is conform het beleid voor gegevensclassificatie van de instelling.
- Compatibiliteit van hardware en software om gearchiveerde gegevens te herstellen en periodiek gearchiveerde gegevens terug te zetten, is geborgd.
- De instelling heeft beheersmaatregelen getroffen om cyberdreigingen die gericht zijn op het beschadigen van back-ups te voorkomen, te detecteren en te mitigeren.

Let op!

Risicogebaseerd, uitbesteding en het three lines model

Good Practices hierbij zijn:

- De instelling heeft op grond van een risicoanalyse bepaald op welke externe locatie de back-ups worden bewaard.
- De instelling gaat periodiek na of de offsite back-up bruikbaar is door deze terug te zetten in een testomgeving. De gebruikers zijn hierbij nauw betrokken.
- De instelling gaat periodiek na dat back-ups beschikbaar en bruikbaar zijn voor het herstellen van schade als gevolg van een cyberaanval (offline/air-gapped back-up).

11.4 Restoration

Marktstandaarden* geven aan dat de instelling een proces inricht dat onder meer het volgende waarborgt:

- De instelling heeft op basis van de business impact analyse procedures in het IT continuïteitsplan geïmplementeerd voor herstel van ICT-systemen, ICT-applicaties, gegevens en documentatie voor zowel de korte als, indien noodzakelijk, ook voor de middellange en lange termijn.
- De instelling kan op passende wijze reageren binnen de doelstelling van hun eigen Recovery Time Objectives[10] en hun eigen Recovery Point Objectives (RPO's, de maximale tijd waarbinnen een systeem of proces moet worden hersteld na een incident). De procedures en plannen zijn gedocumenteerd, breed beschikbaar en gemakkelijk raadpleegbaar in geval van nood, met inbegrip van een duidelijke definitie van rollen en verantwoordelijkheden.
- De procedures en plannen worden voortdurend bijgewerkt in overeenstemming met de lessen die getrokken worden uit de incidenten, tests, nieuwe risico's en bedreigingen, dit geldt ook voor de RTO's en RPO's.
- Het maken en herstellen van back-ups voldoet aan het beleid van de instelling voor wat betreft de voortdurende beschikbaarheid, integriteit, vertrouwelijkheid en authenticiteit van systemen en gegevens. Hierbij zijn de inhoud en frequentie van back-ups vastgesteld in overeenstemming met de bedrijfsvereisten inzake herstel. De back-up- en herstel-procedures worden op regelmatige basis getest en geëvalueerd.
- Bij het herstellen van een ICT-gerelateerd incident worden de benodigde controles uitgevoerd om de integriteit van de data te borgen. Hierbij is aandacht voor consistentie tussen systemen.

Let op!

Risicogebaseerd, uitbesteding en het three lines model

Good Practices hierbij zijn:

- De instelling heeft afspraken gemaakt met haar dienstverleners en ook intern tussen business en ICT over Recovery Point Objectives (RPO's) en Recovery Time Objectives (RTO's) en het testen daarvan.
- In de procedures en plannen voor back-up en herstel van ICT-systemen wordt gespecificeerd welke omstandigheden activering van de plannen op gang kunnen brengen, en welke acties worden ondernomen om de beschikbaarheid, integriteit, continuïteit en het herstel van ten minste de kritieke ICT-systemen, ICT-diensten en gegevens te waarborgen.
  De plannen zijn erop gericht de hersteldoelstellingen met betrekking tot de activiteiten van de instelling te verwezenlijken.
- Na een storing of majeure systeemuitval kan de instelling met behulp van backups of "snapshots" haar data en ICT-systemen binnen de gestelde tijdslimiet herstellen zodat haar kritieke bedrijfsprocessen met integere data en correct werkende systemen kan worden voortgezet.
- De instelling test periodiek of de back-up en het terugzetten hiervan correct werkt.
- De instelling heeft een maximale *downtime* en het maximale verlies van data van haar kritieke processen bepaald en vastgesteld op basis van realistische tests dat herstelwerkzaamheden (bijvoorbeeld: het terugzetten van back-ups) binnen deze maximale downtime haalbaar is.

10

- De instelling heeft een recovery scenario opgesteld voor het geval zich cybersecurity incidenten voordoen.
- De instelling heeft diverse beheersmaatregelen getroffen om de toegang tot back-ups te bewaken en te monitoren: offline back-up, netwerkzonering, detectie van afwijkende back-up/restore activiteiten.
- Voortdurend wordt bekeken of voldoende capaciteit aanwezig is voor de back-up zodat kritieke data altijd volledig hersteld kan worden.

12.1 Storage and retention arrangements

Marktstandaarden* geven aan dat de instelling een proces inricht dat onder meer het volgende waarborgt:

- De instelling heeft een beleid betreft gegevensopslag, retentie en archivering van data. Deze wordt periodiek geactualiseerd en gecontroleerd.
- De instelling heeft procedures gedefinieerd en geïmplementeerd voor gegevensopslag, retentie en archivering van data in lijn met de bedrijfsdoelstellingen.
- Kritische gegevensopslag en de omgeving waarop de gegevensopslag wordt gehost, zijn beschermd tegen Ransomware aanvallen (zoals het hanteren van air gap, Write Once-Read Many (WORM) etc).
- Bij de opslag van data wordt rekening gehouden met de wettelijke vereisten ten aanzien van bewaartermijnen.
- Periodiek wordt bekeken of voldoende capaciteit aanwezig is voor de back-up zodat kritieke data altijd volledig hersteld kan worden.

Good Practices hierbij zijn:

- De instelling houdt een vervalkalender bij van opgeslagen data op grond waarvan gegevens worden vernietigd.
- De instelling heeft afspraken gemaakt met de dienstverleners ten aanzien van de bewaartermijn van data conform het beleid van de instelling. Deze werken door naar eventuele onderaannemers.
- De instelling gaat periodiek na in hoeverre de dienstverleners zich houden aan de afgesproken bewaartermijnen, bijvoorbeeld door middel van SLR en/of assurance rapportages.
- De instelling beoordeelt periodiek of dienstverleners en onderaannemers voldoen aan de eisen van de instelling op het gebied van gegevensopslag, archivering en retentie.

Let op!

Risicogebaseerd, uitbesteding en het three lines model

12.2 Disposal

Marktstandaarden* geven aan dat de instelling een proces inricht dat onder meer het volgende waarborgt:

- De instelling heeft procedures gedefinieerd en geïmplementeerd om ervoor te zorgen dat aan bedrijfsvereisten voor de bescherming van gevoelige gegevens en software is voldaan, wanneer gegevens en hardware worden verwijderd of overgedragen.

Let op!

Risicogebaseerd, uitbesteding en het three lines model

Good Practices hierbij zijn:

- De instelling hanteert vernietigingsprotocollen voor het schonen en vernietigen van documenten en elektronische gegevensdragers zoals laptops, mobiele telefoons, harde schijven, SSD opslagmedia en USB sticks.
- De instelling heeft met dienstverleners afspraken gemaakt over het veilig verwijderen en vernietigen van gegevens. De instelling controleert periodiek of dienstverleners nog voldoen aan deze afspraken.

12.3 Security requirements for data management

Marktstandaarden* geven aan dat de instelling een proces inricht dat onder meer het volgende waarborgt:

- De instelling heeft beleid en procedures gedefinieerd en geïmplementeerd ten aanzien van het veilig ontvangen, verwerken, opslaan en verstrekken van data conform het beleid van de instelling.

Let op!

Risicogebaseerd, uitbesteding en het three lines model

Good Practices hierbij zijn:

- De instelling neemt in haar informatiebeveiligingsbeleid op hoe medewerkers met gevoelige informatie omgaan op basis van haar dataclassificatiebeleid (zie beheersmaatregel 2.2).
- De instelling verstrekt de juiste middelen die haar medewerkers in staat stelt om op veilige wijze data te kunnen versturen en te kunnen ontvangen, zoals encrypted USB sticks, versleutelde internet verbindingen, secure e-mail, document vaults, etc.
- Periodiek controleert de instelling of zij nog voldoet aan wet- en regelgeving omtrent dataopslag. Daar waar nodig stelt zij haar beleid en procedures bij.
- De instelling beoordeelt op periodiek of dienstverleners in de keten voldoen aan de eisen van de instelling op het gebied van data management.

13.1 Configuration repository and baseline

Marktstandaarden* geven aan dat de instelling een proces inricht dat onder meer het volgende waarborgt:

- De instelling beheert, inventariseert, volgt, corrigeert en verwijdert ongeautoriseerde en onbeheerde ICT-assets waarvan haar bedrijfsprocessen afhankelijk zijn, zowel intern als in haar uitbestedingsketen.
- De inventaris van de ICT-assets is voldoende gedetailleerd om snel een identificatie van een ICT-asset, de locatie, relatie met andere ICT-assets, de beveiligingsclassificatie en de eigenaar ervan mogelijk te maken.
- De instelling houdt een register bij van end user computing toepassingen die kritieke bedrijfsfuncties of -processen ondersteunen.
- De instelling heeft inzicht in de configuratie(parameters) van die ICT-assets.
- De instelling evalueert aanbevelingen van leveranciers en externe partijen voor een veilige inrichting van ICT-infrastructuur en ICT-applicaties en legt vast hoe zij haar ICT-assets 'veilig' configureert (baselines).
- De verantwoordelijkheid voor de configuratie (baselines) van de verschillende ICT-assets is toebedeeld aan de betreffende onderdelen binnen de instelling en is vastgelegd.

Let op!

Risicogebaseerd, uitbesteding en het three lines model

Good Practices hierbij zijn:

- De instelling bepaalt de (security) baselines op basis van diverse bronnen als leveranciers, best-practices in de markt en richtsnoeren.
- De instelling heeft haar ICT-assets geïnventariseerd en vastgelegd in centrale repository zoals een Configuration Management Database (CMDB).
- De instelling gebruikt de CMDB ter verificatie van de werkelijk aanwezige ICT-assets. Verschillen worden geanalyseerd en opgevolgd.
- De instelling gebruikt de CMDB om te bepalen in hoeverre ICT-assets zijn verouderd en in hoeverre zij worden ondersteund met security updates.

13.2 Identification and Maintenance of Configuration Items

Marktstandaarden* geven aan dat de instelling een proces inricht dat onder meer het volgende waarborgt:

- Wijzigingen in de configuratie management database (zie beheersmaatregel 13.1) vinden beheerst plaats. Dat wil zeggen dat wijzigingen zijn geaccordeerd en worden gelogd. De instelling heeft de configuratiemanagementprocedure vastgelegd.
- De configuratiemanagementprocedure is geïntegreerd met procedures voor wijzigingsbeheer, incidentbeheer en probleembeheer.

Let op!

Risicogebaseerd, uitbesteding en het three lines model

Good Practices hierbij zijn:

- De configuratiemanagementprocedures zijn gebaseerd op internationale standaarden zoals ITIL.
- De instelling voert periodiek geautomatiseerde scans (inventarisatie) uit op de ICT-infrastructuur. De uitkomst van deze scans wordt vergeleken met de inhoud van de CMDB en indien hierin afwijkingen voorkomen, worden deze geanalyseerd en wordt actie ondernomen.

14.1 Third party and supplier services management

Marktstandaarden* geven aan dat de instelling een proces inricht dat onder meer het volgende waarborgt:

- Het bestuur geeft goedkeuring aan en herziet periodiek het uitbestedingsbeleid.
- Voordat de instelling overgaat tot uitbesteding, stelt zij conform beleid en geldende regelgeving een passend beschermingsniveau vast voor de vertrouwelijkheid van gegevens, de continuïteit van de uitbestede activiteiten en de integriteit en herleidbaarheid van gegevens en systemen.
- De instelling verwerkt de eisen, die voortvloeien uit deze beschermingsniveaus, in afspraken met de dienstverleners op alle schakels in de kritieke of belangrijke uitbestedingsketens.
- De instelling is specifieke kwantitatieve en kwalitatieve prestatiecriteria overeengekomen met haar dienstverleners die daarover rapporteren aan de instelling in rapportages of dashboards.
- De rapportages of dashboards worden verder geanalyseerd om zowel positieve als negatieve trends en ontwikkelingen te identificeren voor zowel instelling specifieke als generieke diensten.
- Het verantwoordelijk lijnmanagement wordt zowel over de kwantitatieve en kwalitatieve prestaties als over de trend analyses geïnformeerd.

Let op!

Risicogebaseerd, uitbesteding en het three lines model

Good Practices hierbij zijn:

- De instelling ontvangt periodiek rapportages of heeft toegang tot dashboards waarin de daadwerkelijk gemeten servicelevels op inzichtelijke wijze zijn opgenomen en zijn afgezet tegen de in de Service Level Agreement afgesproken service-level doelstellingen (prestatie- en kwaliteitsnormen).
- De instelling ontvangt een geïntegreerde rapportage van haar ICT-dienstverleners waarin prestaties van onderaannemers zijn geïntegreerd in de gemeten prestatie criteria.
- Geaggregeerde rapportages geven het management van de instelling op verschillende managementniveaus inzicht in alle uitbestedingsrisico's, afgezet tegen haar risicobereidheid.
- De instelling besteedt aandacht aan de mechanismen voor integratie van de clouddiensten in de systemen van de instelling, bijvoorbeeld de programmeringsinterfaces van applicaties (API's) en een goed gebruikers- en toegangs-beheerproces.
- De instelling sluit alleen regelingen met dienstverleners die voldoen aan haar normen op het gebied van informatie-beveiliging en continuïteit. Wanneer die contractuele afspraken zien op kritiek of belangrijke functies, stelt de instelling, alvorens de regelingen te sluiten, terdege vast of door deze dienstverleners de meest actuele en hoogste kwaliteitsnormen voor informatiebeveiliging worden toegepast.
- Vóór het sluiten van een regeling beoordeelt de instelling:
  - of de regeling betrekking heeft op kritieke of belangrijke functies;
  - of aan de toezichtvoorwaarden is voldaan;
  - alle relevante risico's inclusief de mogelijkheid tot een versterking van het concentratierisico;
  - of de dienstverlener geschikt is op basis van uitkomsten due-diligence onderzoeken;
  - belangenconflicten die kunnen voortkomen uit de regeling.

14.2 Third party and supplier risk management

Marktstandaarden* geven aan dat de instelling een proces inricht dat onder meer het volgende waarborgt:

- De instelling houdt een register bij met alle contractuele regelingen als onderdeel van het beheersingskader voor IT- en uitbestedingsrisico's.
- De instelling heeft de risico's die zij lopen vanuit dienstverleners geïnventariseerd en heeft een strategie ten aanzien van deze risico's in het uitbestedingsbeleid opgenomen. Deze risico's worden regelmatig geëvalueerd, waarbij ook het concentratie-risico en de gevolgen van complexe uitbestedingsketens op het risicoprofiel worden beoordeeld.
- De instelling heeft door middel van deze analyse een actueel beeld van het inherente informatiebeveiligingsrisico van alle uitbestedingen en/of uitbestedingsketens. De instelling overziet zelf welke beheersmaatregelen conform het informatiebeleid zijn getroffen en in hoeverre die aantoonbaar werken. Het bestuur is en wordt daarvan op de hoogte gesteld.
- De instelling heeft vastgesteld voor haar dienstverleners en eventueel daarin gelieerde onderaannemers, welke beheersmaatregelen vanuit de instelling en/of deze Good Practice van toepassing zijn en welke rapportages verkregen dienen te worden.
- In het register wordt onderscheid gemaakt tussen dienstverleners die kritieke of belangrijke functies ondersteunen en dienstverleners die dat niet doen.
- Contracten zijn opgesteld volgens marktstandaarden en zijn in overeenstemming met geldende wettelijke bepalingen.
- De instelling beoordeelt continue de beschikbaarheid van kritieke of belangrijke uitbestede dienstverlening, fall back mogelijkheden om de dienstverlening op een alternatieve wijze voort te zetten en conformiteit met standaards op het gebied van informatiebeveiliging en cybersecurity.
- De instelling hanteert een risico gebaseerde benadering met betrekking tot informatiebeveiliging ten aanzien van de locatie(s) (d.w.z. land of regio) voor gegevensopslag en verwerking.
- De instelling beschikt over een gedegen en goed gedocumenteerd incidentenbeheerproces, met inbegrip van de verantwoordelijkheden van alle betrokken partijen, bijvoorbeeld door vaststelling van een samenwerkingsmodel in geval van daadwerkelijke of vermoede incidenten.
- De instelling heeft ten aanzien van de dienstverleners die kritieke en belangrijke functies ondersteunen een alomvattende exitstrategie gedocumenteerd en daar waar mogelijk getest en/of geoefend.

Let op!

Risicogebaseerd, uitbesteding en het three lines model

Good Practices hierbij zijn:

- De instelling stelt samen met haar dienstverleners een risicoanalyse en een strategie met betrekking tot de continuïteit en betrouwbaarheid van de dienstverlening op en actualiseert deze met een vaste frequentie. Risico's bij dienstverleners waaraan diensten zijn onderuitbesteed zijn meegenomen in de risicoanalyses.
- Het uitbestedingsbeleid bevat een strategie inzake het gebruik van ICT-diensten ter ondersteuning van kritieke of belangrijke functies die worden geleverd door ICT-dienstverleners en hun ketenpartners.
- Om het concentratierisico te beoordelen wordt beoordeeld of het contract met een dienstverlener makkelijk substitueerbaar is en of er meerdere contractuele regelingen zijn met dezelfde dienstverlener of met nauw verbonden dienstverleners. De kosten en baten van alternatieve oplossingen worden tegenover elkaar afgewogen met het oog op de digitale veerkracht.

- Wanneer er een mogelijkheid is dat een dienstverlener een kritieke of belangrijke taak onderuitbesteedt, worden de baten en risico's afgewogen die hieruit kunnen voortkomen, met name wanneer de onderaannemer is gevestigd in een land waarin de instelling zelf niet is gevestigd.
- De instelling is met haar dienstverleners een exit plan overeengekomen. Hierin staan afspraken over een gecontroleerde beëindiging van de dienstverlening, zoals de wijze van transitie / migratie, de aansprakelijkheid en het verwijderen van de (back-up) data van de instelling na de exit. Onderuitbesteding is in scope van de exit plannen. De instelling heeft beheersmaatregelen getroffen om de continuïteit van onderhoud aan software die specifiek voor de instelling is ontwikkeld (zelfbouw en maatwerk), te waarborgen. Hiertoe zijn Escrow overeenkomsten gesloten en/of afspraken over voortzetting. De instelling gaat voor kritieke of belangrijke systemen na in hoeverre deze afspraken in de overeenkomsten zijn nageleefd.
- De instelling beschikt over een standaard geheimhoudings-verklaring voor elke organisatie die een contractuele relatie aangaat met de instelling. De ondertekening van de verklaring door relevante partijen wordt bewaakt.
- De instelling beoordeelt periodiek de solvabiliteit en wendbaarheid van haar kritieke of belangrijke dienstverleners en neemt waar nodig actie.
- De instelling bepaalt vooraf op risicogebaseerde wijze de frequentie en scope van de audits en inspecties en of de uitvoerende auditors/externe accountants passende vaardigheden en kennis hebben.
- De instelling beëindigt contractuele regelingen:
  - bij overtreding van wetten, voorschriften of bepalingen door de dienstverlener;
  - bij omstandigheden die ongewenste wijzigingen kunnen brengen in de uitvoering van de uitgevoerde dienstverlening door de dienstverlener;
  - bij zwakheden van de dienstverlener in het algemeen beheer van het ICT-risico;
  - wanneer de bevoegde autoriteit niet langer doeltreffend toezicht kan uitvoeren.

15.1 Security incident policy and definition

Marktstandaarden* geven aan dat de instelling een proces inricht dat onder meer het volgende waarborgt:

- De instelling beschikt over een geformaliseerd proces voor incident management, waaraan een escalatieprocedure en escalatiecriteria zijn gekoppeld.
- De escalatieprocedure is gebaseerd op overeengekomen serviceniveaus voor incidenten die niet onmiddellijk kunnen worden opgelost. De instelling hanteert een eenduidige definitie voor beveiligingsincidenten die bij alle belanghebbenden bij de instelling bekend is.
- In het incidentmanagement proces zijn (cyber) beveiligins-incdidenten afzonderlijk geclassificeerd met als doel dat op dergelijke incidenten snel en met de juiste expertise wordt gereageerd. Bij de afhandeling van (cyber)beveiligings-incidenten worden alle stappen met bijbehorende informatie in een log vastgelegd.
- De instelling heeft procedures vastgesteld met betrekking tot het melden van cybersecurity incidenten, het reageren op (cyber)beveiligingsincidenten, het beperken van schade als gevolg van die incidenten en het uitvoeren van herstelwerk-zaamheden.
- (Cyber)security incidenten worden conform geldende regels gerapporteerd aan de autoriteiten.
- Na grote ICT-gerelateerde incidenten die de kernactiviteiten van de instelling verstoren worden de oorzaken van de verstoring geanalyseerd en de noodzakelijke verbeteringen geïdentificeerd en tijdig geïmplementeerd.

Let op!

Risicogebaseerd, uitbesteding en het three lines model

Good Practices hierbij zijn:

- De instelling heeft een proces ingericht dat waarborgt dat alle (potentiële) beveiligingsincidenten centraal worden gemeld en worden geregistreerd.
- De instelling classificeert ICT-gerelateerde incidenten en bepaalt hun impact op basis van onder meer de volgende criteria:
  - het aantal en/of de relevantie van de getroffen cliënten of financiële tegenpartijen en indien van toepassing, het bedrag of het aantal transacties dat wordt beïnvloed door het ICT-gerelateerde incident, en of het ICT-gerelateerde incident reputatieschade heeft veroorzaakt;
  - de duur van het ICT-gerelateerde incident met inbegrip van de uitvaltijd van de dienst;
  - de geografische spreiding met betrekking tot de door het ICT-gerelateerde incident getroffen gebieden, vooral als het meer dan twee regio's betreft;
  - het dataverlies dat het ICT-gerelateerde incident met zich meebrengt, zoals voortdurende beschikbaarheid, integriteit, vertrouwelijkheid of authenticiteitsverlies;
  - het kritieke karakter van de betrokken diensten, met inbegrip van de transacties van de instelling en operaties;
  - de economische impact, met name directe en indirecte kosten en verliezen, van het ICT-gerelateerde incident, zowel in absolute als relatieve zin.
- De evaluatie van het incident bepaalt of de vastgestelde procedures werden gevolgd en de genomen beheers-maatregelen effectief waren, onder meer t.a.v.:
  - de snelheid waarmee wordt gereageerd, het bepalen van de impact van ICT-gerelateerde incidenten en de ernst ervan;
  - de kwaliteit en snelheid bij het uitvoeren van forensische analyses;
  - de doeltreffendheid van de escalatie van incidenten;
  - de doeltreffendheid van interne en externe communicatie.

15.2 Incident escalation

Marktstandaarden* geven aan dat de instelling een proces inricht dat onder meer het volgende waarborgt:

- Significante incidenten worden gerapporteerd aan het bestuur waarbij zij ten minste op de hoogte wordt gebracht van de impact, de reactie en de lessons-learned.
- De instelling heft menskracht, expertise en procedures beschikbaar om als een Computer Security Security Incident Response Team (CSIRT) op te treden.
- Categorisering en prioritering van incidenten gebeurt op basis van impactanalyse, gedefinieerde criteria en serviceniveaus.
- De gepaste criteria en drempelwaarden worden vastgelegd om een gebeurtenis te classificeren als een veiligheidsincident, evenals vroegtijdige waarschuwingsindicatoren om een vroegtijdige detectie van deze incidenten mogelijk te maken.
- Het reageren op informatiebeveiliging en cybersecurity incidenten wordt getraind.
- Incidenten zijn toegewezen aan een eigenaar.
- Escalatieprocedures en verantwoordelijkheden omtrent besluitvorming bij (cyber)incidenten zijn binnen de instelling bekend en worden nageleefd. Procedures voor incident-meldingen en activatie van crisismanagement zijn opgesteld.
- (Cyber)security incidenten worden conform geldende regels gerapporteerd aan de autoriteiten.

Let op!

Risicogebaseerd, uitbesteding en het three lines model

Good Practices hierbij zijn:

- De instelling heeft een CSIRT opgericht, bestaande uit gespecialiseerde ICT-professionals, dat in staat is snel te handelen in het geval van een informatiebeveiligings- of cybersecurity incident. Het CSIRT heeft als doel schade te reduceren en snel herstel van de dienstverlening te bevorderen.
- Het CSIRT maakt bijvoorbeeld gebruik van het cybersecurity incident response proces zoals beschreven door het SANS instituut waarbij ze kijkt naar de volgende stappen 1. Preparation. 2. Identification. 3. Containment. 4. Eradication. 5. Recovery 6. Post Incident.
- De Security Officer beoordeelt (ten minste) dagelijks de geregistreerde beveiligingsincidenten en bepaalt de impact hiervan.
- De instelling en de dienstverleners werken proactief samen bij het detecteren van en het reageren op cybersecurity incidenten in de keten van uitbestede diensten en ICT-infrastructuur. De instelling heeft hiervoor Security Operations Center (SOC) of Cyber Defence Center ingericht.
- De instelling maakt als alternatief voor het inrichten van een eigen SOC cq Cyber Defence Center gebruik van een commerciële externe SOC of een SOC die zij samen met andere instellingen beheert.
- De instelling maakt gebruik van tooling zoals een SIEM om ICT-gerelateerde beveiligingsinformatie te verzamelen, te combineren en te analyseren, met als doel om tijdig inzicht te krijgen in en proactief te reageren op (mogelijke) beveiligingsincidenten.
- Het CSIRT van de instelling richt zich ook op de preventie van cybersecurity incidenten en de voorbereiding van de instelling op dergelijke incidenten.
- Het bestuur geeft indien nodig sturing aan deze respons en evalueert achteraf het incident en neemt de uitkomsten van deze evaluatie mee in de risicomanagement cyclus.
- Specifieke externe communicatieplannen voor kritieke bedrijfsfuncties en -processen worden opgesteld om:
  i. Samen te werken met de relevante belanghebbenden;
  ii. Tijdige informatie, met inbegrip van incidentrapportage, te verstrekken aan externe partijen (bv. klanten, andere marktdeelnemers, de relevante (toezichthoudende) autoriteiten, indien van toepassing en in overeenstemming met geldende regelgeving).

16.1 Security testing, surveillance and monitoring

Marktstandaarden* geven aan dat de instelling een proces inricht dat onder meer het volgende waarborgt:

- De resultaten van beveiligingsmonitoring worden gerapporteerd aan het bestuur. De rapportage geeft inzicht in zowel operationele als beveiligingsincidenten en stelt het bestuur in staat passende bijsturende beslissingen te nemen over het verbeteren van maatregelen.
- De instelling heeft beveiligingsmaatregelen getroffen en vastgelegd. Deze maatregelen worden getest en periodiek geëvalueerd zodat deze blijven voldoen aan vastgestelde security baselines.
- De instelling heeft Security Operations Center (SOC) of Cyber Defence Center diensten ingericht.
- Monitoring van ongebruikelijke activiteiten in ICT-systemen vindt plaats, uitzonderingen worden gesignaleerd en opgevolgd.
- Deze monitoring omvat ten minste het volgende:
  - de activiteiten van gebruikers worden op een risico-evenredige manier gelogd;
  - interne en externe factoren, inclusief bedrijfs- en ICT-beheersfuncties;
  - transacties door dienstverleners.

Let op!

Risicogebaseerd, uitbesteding en het three lines model

Good Practices hierbij zijn:

- De instelling heeft beveiligingsmaatregelen getroffen die onder meer bestaan uit:
  - Logbestanden. Deze zijn beveiligd om ongeoorloofde wijziging of verwijdering te voorkomen. Logfiles worden bijgehouden gedurende een periode die in verhouding staat tot het kritieke karakter van de geïdentificeerde bedrijfsfuncties, ondersteunende processen en informatie-assets. Instellingen gebruiken deze gegevens om de identificatie en het onderzoek te vergemakkelijken van onregelmatigheden die worden geconstateerd bij het verlenen van de diensten.
  - SIEM. De instelling heeft een SIEM (Security Information and Event Management) oplossing geïmplementeerd om aan de hand van logging snel afwijkende patronen te kunnen herkennen en daarop in te spelen.
- De instelling stelt periodiek management rapportages op met een overzicht van alle geregistreerde beveiligingsincidenten en de status van opvolging.
- Op basis van logging van gemonitorde systemen signaleert het SIEM events die een securityrisico kunnen vormen ('alerts'). De alerts worden door analisten van het SOC beoordeeld en geprioriteerd. Wanneer de potentiële ernst van een alert nader onderzoek vereist wordt een case aangemaakt. Van deze cases wordt een case-rapport opgesteld.
- De instelling maakt voor het optimaliseren van haar SOC gebruik van de NOREA publicatie *Good Practice on assessing the maturity of a Security Operations Center (SOC) using the SOC Maturity Framework (SOC-MF)*[11].
- De instelling maakt gebruik van het MAGMA framework (ontwikkeld door NL FI-ISAC) en/of het Mitre ATT&CK framework om dreigingsmodellen te ontwikkelen, de effectiviteit van beveiligingstools te evalueren, detectie-strategieën te ontwikkelen en prioriteit te geven aan beveiligingsinvesteringen.

11 www.norea.nl

16.2 Monitoring of internal control framework

Marktstandaarden* geven aan dat de instelling een proces inricht dat onder meer het volgende waarborgt:

- De instelling beheerst haar ICT risico's en risico's op het gebied van informatiebeveiliging en cybersecurity. Hiertoe heeft de instelling een ICT-beheersingsraamwerk (internal control framework) opgesteld waarin onder meer een informatiebeveiligingsbeleid, standaarden, procedures, (key) controls en ICT General Controls zijn opgenomen in lijn met de doelstellingen van de instelling.
- De instelling evalueert regelmatig de opzet, bestaan en werking van het internal control framework.

Let op!

Risicogebaseerd, uitbesteding en het three lines model

Good Practices hierbij zijn:

- De risicomanagementfunctie, interne auditor en externe accountant rapporteren regelmatig hun oordeel, bevindingen en aanbevelingen over de opzet, bestaan en aantoonbare werking van het ICT-beheersingsraamwerk.
- De instelling monitort de opvolging van aanbevelingen en legt dit vast.
- De instelling vergelijkt Service Level rapportages en zekerheidsrapportages van interne en externe leveranciers met de overeengekomen dienstverlening en de ervaringen van de instelling met de geleverde diensten.
- De instelling analyseert trends en ontwikkelingen ten opzichte van voorgaande rapportage periodes.

16.3 Internal control at third parties

Marktstandaarden* geven aan dat de instelling een proces inricht dat onder meer het volgende waarborgt:

- De instelling is en blijft volledig verantwoordelijk voor de naleving van alle verplichtingen uit relevante wet- en regelgeving.
- De instelling besteedt bij contractvoorbereiding aandacht aan de wijze waarop de dienstverlener blijvend voldoet aan contractuele verplichtingen, wet- en regelgeving en te treffen rapportage- en controleregelingen.
- De instelling vormt zich een oordeel over de interne beheersmaatregelen bij haar dienstverleners en eventuele onderaannemers.
- De dienstverlener voldoet aan wettelijke en contractuele bepalingen.
- De instelling heeft contractueel vastgelegd dat als gevolg van de uitbesteding, het toezicht door de gehele keten van uitbesteding niet wordt belemmerd.
- De instelling legt de afspraken met de dienstverleners centraal en voor de partijen toegankelijk vast.

Let op!

Risicogebaseerd, uitbesteding en het three lines model

Good Practices hierbij zijn:

- De instelling let erop dat haar contracten met de dienstverleners ten minste het volgende omvatten:
  - een volledige beschrijving van de uitbestede functies en diensten;
  - taken en verantwoordelijkheden van betrokken partijen;
  - toezegging van de dienstverlener dat blijvend wordt voldaan aan alle toepasselijke wet- en regelgeving;
  - de locaties waar de functies en diensten worden geleverd en waar gegevens zijn opgeslagen en worden verwerkt;
  - bepalingen over toegankelijkheid, beschikbaarheid, integriteit, beveiliging en bescherming van persoonsgegevens;
  - beschrijvingen van het niveau van de dienstverlening en nauwkeurige kwantitatieve en kwalitatieve prestatiedoelstellingen;
  - voorwaarden waaronder de dienstverlener verder mag uitbesteden, waarbij plichten en verantwoordelijkheden onverlet worden gelaten;
  - kennisgevingstermijnen en rapportageverplichtingen van de dienstverlener;
  - verplichting van de dienstverlener om bij een incident bijstand te verlenen zonder extra kosten of tegen een vooraf bepaalde prijs;
  - verplichtingen voor de dienstverlener om bedrijfsnoodplannen te voeren, te testen en te beschikken over beveiligingsmaatregelen om veilige dienstverlening te waarborgen;
  - recht om de prestaties van de dienstverlener permanent te monitoren;
  - verplichting van de dienstverlener om samen te werken met bevoegde autoriteiten;
  - recht van beëindiging en minimale opzegtermijn;
  - exit-strategieën, waaronder de invoering van een verplichte passende overgangsperiode;
  - deelname van medewerkers van dienstverleners aan programma's en trainingen in digitale operationele weerbaarheid.
- Bij contracten met dienstverleners die kritieke of belangrijke diensten ondersteunen omvatten verder:
  - nauwkeurige kwantitatieve en kwalitatieve prestatiedoelstellingen binnen de overeengekomen serviceniveaus om effectieve monitoring mogelijk te maken en zo nodig passende corrigerende maatregelen te nemen;
  - opzegtermijnen en rapportageverplichtingen, inclusief kennisgeving van elke ontwikkeling die een materiële impact kan hebben op het leveren van die kritieke of belangrijke functies;

- het uitvoeren en testen van bedrijfsnoodplannen;
- de verplichting van de dienstverlener om deel te nemen aan en volledig mee te werken aan Threat-Led Penetration Testing programma van de financiële instelling;
- het recht om doorlopend toezicht te houden op de prestaties van dedienstverlener. Exit-strategieën en met name de vaststelling van een verplichte adequate overgangsperiode.

- De instelling houdt bij het opstellen van het contract rekening met het gebruik van modelcontractbepalingen.
- De instelling heeft haar "right-to-audit" bij de dienstverlener en de onderaannemers contractueel vastgelegd en oefent deze zonodig uit.
- De instelling verplicht de dienstverlener de instelling in kennis te stellen van alle voorgenomen belangrijke wijzigingen van de in de oorspronkelijke overeenkomst genoemde onderaannemers. De kennisgevingstermijn voor dergelijke wijzigingen wordt zodanig bepaald dat de instelling in staat is de risico's als gevolg van de voorgestelde wijziging te beoordelen en indien nodig corrigerende beheersmaatregelen kan nemen of de exit clausule in werking kan zetten.
- De instelling evalueert kritieke of belangrijke uitbestedingen minimaal jaarlijks aantoonbaar, waarbij de performance- en resultaatafspraken en de mate waarin de dienstverlener past bij de strategie en doelstellingen worden beoordeeld, alsook de risicobereidheid van de dienstverlener t.o.v. de eigen risicobereidheid.
- Gedurende de looptijd van het contract ontvangt de instelling periodiek (assurance)rapportages van de dienstverlener over de performance en aantoonbaar doorlopende werking van de getroffen interne beheersmaatregelen bij de dienstverlener.
- De dienstverlener geeft jaarlijks aan de instelling een assurance verklaring af over de ICT-beheersing zoals een COS/SOC 2 rapport type II. Beheersmaatregelen op het gebied van informatiebeveiliging en cybersecurity maken deel uit van de scope van de assurance verklaring. De scope beslaat de gehele uitbestedingsketen met inbegrip van kritieke of belangrijke onderaannemers. De instelling bespreekt afwijkingen/ uitzonderingen met de dienstverlener. Deze worden door de dienstverlener tijdig en effectief geadresseerd. De instelling bewaakt de afloop en maakt hiervan een vastlegging.
- De instelling gebruikt geen type 1 assurance rapportages of ISO certificaten om de werking van de beheersmaatregelen aan te tonen.

16.4 Evaluation of compliance with external requirements

Marktstandaarden* geven aan dat de instelling een proces inricht dat onder meer het volgende waarborgt:

- De instelling beoordeelt periodiek in hoeverre haar ICT-beleid en procedures in lijn zijn met wet- en regelgeving.

Let op!

Risicogebaseerd, uitbesteding en het three lines model

Good Practices hierbij zijn:

- De compliance officer van de instelling beoordeelt jaarlijks in hoeverre de ICT-beleidslijnen in lijn zijn met actuele wet- en regelgeving. Daar waar nodig worden aanpassingen doorgevoerd.
- Bij invoering van een nieuwe wetgeving op het gebied van informatiebeveiliging en cybersecurity beoordeelt de instelling de impact hiervan en voert daar waar nodig aanpassingen door.
- De instelling laat zich proactief informeren bij wijzigingen op het gebied van relevante externe regelgeving.

16.5 Independent assurance

Marktstandaarden* geven aan dat de instelling een proces inricht dat onder meer het volgende waarborgt:

- Het bestuur beoordeelt en geeft periodiek goedkeuring aan de ICT-interne auditplannen, ICT-audits en de materiële wijzigingen daarin.
- De governance, systemen en processen van de instelling voor hun ICT- en beveiligingsrisico's worden periodiek gecontroleerd in overeenstemming met het auditplan van de instelling.
- Dit gebeurt door auditors met voldoende kennis, vaardigheden en deskundigheid op het gebied van ICT- en beveiligingsrisico's om onafhankelijke assurance te kunnen verstrekken aan het bestuur over de effectiviteit van de getroffen beheers-maatregelen.
- De frequentie en gerichtheid van dergelijke audits is evenredig aan de relevante ICT- en beveiligingsrisico's.
- De resultaten van de onafhankelijke beoordeling worden voorgelegd aan het management van de instelling.

Let op!

Risicogebaseerd, uitbesteding en het three lines model

Good Practices hierbij zijn:

- De instelling laat de interne- of externe auditor op basis van een risicoanalyse ICT-objecten zoals de informatiebeveiliging en cybersecurity van ICT-infrastructuur periodiek beoordelen. Deze beoordeling heeft betrekking op de opzet, bestaan en aantoonbare werking van beheersmaatregelen.

17.1 Identity & Access Management

Marktstandaarden* geven aan dat de instelling een proces inricht dat onder meer het volgende waarborgt:

- Processen voor logische toegangsbeveiliging zijn gedefinieerd, gedocumenteerd, uitgevoerd en omvatten de controle op en herstel van onregelmatigheden.
- Authenticatiemethoden staan in verhouding tot het kritieke karakter van de ICT-systemen, de informatie of het proces waar toegang tot wordt verkregen. Dit betreft ten minste sterke wachtwoorden of sterkere authenticatiemethoden (zoals twee factor zoals of out-of-band authenticatie), gebaseerd op relevante risico's.
- Toegang tot informatiesystemen en data van de instelling is te herleiden naar uniek te identificeren personen (intern, extern en inhuur) of naar ICT-services (bijvoorbeeld scripts en batch jobs) met een uniek te identificeren eigenaar.
- Toegang tot ICT-systemen en data worden "functie gebaseerd"' en alleen verleend op basis van 'least privilege' principes. De naleving van deze principes wordt periodiek geëvalueerd
- De instelling heeft de toegang tot informatiesystemen en data bepaald, goedgekeurd en vastgelegd (SOLL autorisatie matrices) en gebaseerd op de vereiste functiescheidingen en bedrijfsregels (zie beheersmaatregel 7.1).
- De opzet van de logische toegangsbeveiliging (SOLL autorisatie matrices) wordt regelmatig geëvalueerd.
- Toegang tot informatiesystemen en data van de instelling wordt gecontroleerd en bewaakt in de ICT-infrastructuur en in ICT-applicaties, conform de geaccordeerde SOLL autorisatie matrices.
- Toegangsrechten in ICT-systemen (IST) regelmatig worden vergeleken met de SOLL autorisatie matrices.
- Instellingen handhaven authenticatiemethoden die voldoende robuust zijn om er passend en doeltreffend voor te zorgen dat beleidslijnen en procedures inzake toegangscontrole worden nageleefd.

Let op!

Risicogebaseerd, uitbesteding en het three lines model

Good Practices hierbij zijn:

- De instelling kent unieke user-id's toe aan alle personen met toegang tot de ICT-systemen en data. Hierbij is het HR systeem van de instelling leidend.
- Gebruikersidentiteiten en toegangsrechten worden bijgehouden in een centrale repository.
- De instelling maakt gebruik van sterke wachtwoorden (complexiteit regels, numeriek, gebruik van symbolen, leeftijd, historie) voor verschillende soorten accounts: system, normal, superuser.
- De instelling maakt gebruik van out-of-band authenticatie, een vorm van twee-factor authenticatie (2FA) die een secundaire verificatiemethode vereist via een afzonderlijk communicatiekanaal. Hierbij zijn verschillende kanalen betrokken: de internetverbinding van de klant en het draadloze netwerk waarop zijn mobiele telefoon werkt.
- De instelling past het principe van 'Role Based Access' toe waarbij ze periodiek definieert welke rol welke identiteit heeft. Hiertoe brengt zij in kaart: Wie krijgt access, Wat wordt bij access verstrekt, Wanneer, Waar, Waarom en Hoe.
- De instelling gebruikt een Identity & Access Management (IAM) tool ter ondersteuning van de inrichting van de toegangsbeveiliging en de controle daarop door bedrijfsproceseigenaren en ICT-systeembeheerders.
- De toegang op afstand tot kritieke ICT-systemen worden alleen toegekend volgens kennisnemingsbehoefte en wanneer er sterke authenticatiemiddelen worden gebruikt.

17.2 User account management

Marktstandaarden* geven aan dat de instelling een proces inricht dat onder meer het volgende waarborgt:

- Het aanvragen, wijzigen of intrekken van toegangsrechten tot informatiesystemen en data volgt geformaliseerde stappen waarin goedkeuring wordt verleend door de eigenaren van de desbetreffende bedrijfsprocessen, informatiesystemen en data.
- Functiescheiding of 4-ogen principe verhindert dat de voornoemde stappen door 1 persoon worden uitgevoerd.
- Alle activiteiten met betrekking tot het aanvragen, wijzigen of intrekken van toegangsrechten worden gelogd en zijn herleidbaar naar personen.
- Toegangsrechten van personen waarmee het dienstverband / contract wordt beëindigd, worden zo snel mogelijk verwijderd of geblokkeerd. Het verlenen, aanpassen en intrekken van toegangsrechten wordt zodanig geregistreerd dat inzicht en analyse worden vergemakkelijkt.
- Beheersmaatregelen worden uitgevoerd voor geprivilegieerde systeemtoegang door accounts met hoge toegangsrechten (zoals beheerdersaccounts) strikt te beperken en hier nauw op toe te zien.
- Toegang van applicaties tot gegevens en ICT-systemen die niet herleidbaar zijn tot personen worden beperkt tot het minimum dat nodig is om de desbetreffende diensten te kunnen aanbieden.

Let op!

Risicogebaseerd, uitbesteding en het three lines model

Good Practices hierbij zijn:

- De instelling maakt gebruik van User Provisioning, waarbij user accounts in de ICT-infrastructuur en business ICT-applicaties zo veel mogelijk automatisch, vanuit het centrale HR-systeem worden aangemaakt, gewijzigd, geblokkeerd en verwijderd.
- De instelling blokkeert een user account automatisch nadat deze een vooraf ingestelde periode niet wordt gebruikt om mee in te loggen.
- Voor het aanvragen, wijzigen of intrekken van toegangsrechten tot informatiesystemen wordt goedkeuring gegeven door de data- of systeemeigenaar.
- De instelling beperkt het gebruik van generieke en gedeelde user-id's, waaronder administrator accounts met hoge bevoegdheden zoveel mogelijk. Het gebruik van deze user-id's wordt beheerst met zowel technische als procedurele maatrelen, zoals: goedkeuring voor het gebruik, krachtige authenticatieoplossingen (2-factor authenticatie, biometrie), 4-ogen principe op de activiteiten, (digitale) password kluis, logging en monitoring van activiteiten en evaluatie na gebruik van het desbetreffende administrator user-id.

18.1 Infrastructure resource protection and availability

Marktstandaarden* geven aan dat de instelling een proces inricht dat onder meer het volgende waarborgt:

- De beheersmaatregelen in de ICT-infrastructuur componenten zijn gebaseerd op een dreigings- en risicoanalyse en zijn zodanig ingericht dat zij een hoog niveau van voortdurende beschikbaarheid, integriteit, vertrouwelijkheid en authenticiteit van informatie waarborgen.
- Plannings- en monitoringsprocessen met betrekking tot prestaties en capaciteit worden uitgevoerd om belangrijke prestatieproblemen van ICT-systemen en ICT-capaciteits-tekorten te voorkomen en tijdig op te sporen en aan te pakken.
- Het ontwerp en de implementatie van deze beheersmaatregelen wordt gemonitord en geëvalueerd.

Let op!

Risicogebaseerd, uitbesteding en het three lines model

Good Practices hierbij zijn:

- Risicoanalyses voor infrastructuur componenten houden rekening met actuele cyberdreigingen, zoals bijvoorbeeld vastgelegd in de ENISA/NCSC dreigingsbeelden of gebaseerd op uitkomsten van recent uitgevoerde red teaming oefeningen en pentesten, etc.
- Security baselines zijn bepaald voor technische platformen (bijvoorbeeld: Windows, Unix, firewalls, IDS en IPS) en conform die baselines geïmplementeerd.
- Er vindt monitoring plaats dat alle platformen voldoen aan de security baselines. Uitzonderingen worden opgevolgd.
- De instelling heeft anti-DDoS maatregelen getroffen. Hierbij is onderscheid gemaakt in bescherming tegen volume gerichte DDoS aanvallen en applicatie gerichte DDoS aanvallen.
- De instelling heeft een risicoanalyse uitgevoerd omtrent gedistribueerde opslag en beheer van ‘private keys’ en wachtwoorden. Daarbij is een onderbouwde afweging gemaakt op welke interne of externe locatie sleutels en wachtwoorden worden opgeslagen.
- De beveiliging en beschikbaarheid van de ICT-infrastructuur is een vast agendapunt in de relevante gremia in de eerste, tweede en derde lijn van de instelling.
- De instelling maakt gebruik van geautomatiseerde controles, bijvoorbeeld voor het monitoren van kwetsbaarheden in de infrastructuur.

18.2 Infrastructure maintenance

Marktstandaarden* geven aan dat de instelling een proces inricht dat onder meer het volgende waarborgt:

- Onderhoud aan de ICT-infrastructuur verloopt planmatig, gestructureerd, volgt de eigen baselines en is in lijn met de change management procedures van de instelling. Daarbij wordt bij wijzigingen aan de ICT-infrastructuur nagelopen of de veiligheid van de instelling het juiste niveau blijft houden.
- De instelling bewaakt dat de ICT-infrastructuur die zij gebruikt wordt ondersteund door de ontwikkelaar/leverancier en dat beveiligingsupdates (patches) beschikbaar worden gesteld. Ook vindt monitoring plaats op de end-of-support datum van gebruikte hard-, firm-, middleware, zodat tijdig mitigerende beheersmaatregelen genomen kunnen worden.
- De instelling heeft de infrastructuurcomponenten geclassificeerd om prioritering aan te kunnen brengen in de uitvoering van onderhoud van de ICT-infrastructuur.
- Oplossingen voor kwetsbaarheden in de ICT-infrastructuur zoals patches hebben invloed op de prioritering van onderhoudswerkzaamheden aan de ICT-infrastructuur.
- Hierbij worden change management processen gevolgd die rekening houden met in hoeverre de kwetsbaarheden kritiek zijn binnen het patchmanagement. Dit is gebaseerd op change risk assessments (cra's), risicoanalyses die onderdeel uitmaken van het changemanagement proces.
- Bij de cra's wordt expliciet aandacht besteed aan cyberdreigingen, kroonjuwelen en aanvalspaden. Deze zijn van invloed op de prioritering van implementatie van de changes.
- De risico's die ontstaan door het gebruik van verouderde of niet-ondersteunde ICT-infrastructuur worden in kaart gebracht, beoordeeld en beperkt. Uit bedrijf genomen ICT-infrastructuur worden op veilige wijze verwerkt en afgevoerd. Hiertoe wordt een planning opgesteld die wordt afgestemd met alle betrokken bedrijfsonderdelen. Een verhoogde focus bij de instelling op klantbeleving en time-to-market leidt er niet toe dat de implementatie van infrastructurele (beveiligings) maatregelen en investeringen in technologische ontwikkelingen (te) lang worden uitgesteld.

Let op!

Risicogebaseerd, uitbesteding en het three lines model

Good Practices hierbij zijn:

- Het implementeren van kritieke beveiligingspatches in de ICT-infrastructuur is een specifiek onderdeel van het patchmanagementproces.
- De status van de ICT-infrastructuur inclusief de kwetsbaarheid voor cyberdreigingen wordt periodiek met behulp van tools geïnventariseerd. Hierover wordt gerapporteerd en actie op achterstallig onderhoud wordt genomen.
- De instelling heeft in haar configuratiemanagement database (CMDB) de vervangingstermijn opgenomen van ICT-infrastructuur componenten en op basis hiervan wordt vervanging ingepland.

18.3 Cryptography and Cryptographic key management

Marktstandaarden* geven aan dat de instelling een proces inricht dat onder meer het volgende waarborgt:

- Het beheer van cryptografische sleutels vindt op beheerste en risicogebaseerde wijze plaats. De instelling heeft beleid en procedures uitgewerkt met betrekking tot het genereren, veranderen, intrekken, vernietigen, distribueren, certificeren, opslaan, installeren, gebruiken en archiveren van de cryptografische sleutels.
- Risico's van modificatie en het bekend worden van de sleutels tijdens deze processen zijn geïdentificeerd en mitigerende beheersmaatregelen zijn getroffen.
- Hierbij is een risicoanalyse gemaakt waardoor de beveiligings-maatregelen proportioneel worden toegepast aan het belang van de betreffende sleutel.
- De instelling heeft de risico's van cyberaanvallen gericht op het modificeren en onderscheppen van de cryptografische sleutels onderkend en met passende beheersmaatregelen beheerst.

Let op!

Risicogebaseerd, uitbesteding en het three lines model

Good Practices hierbij zijn:

- De instelling gebruikt Hardware Security Modules (HSM's) bij het genereren, veranderen, intrekken, vernietigen, distribueren, certificeren, opslaan, inbrengen, gebruiken en archiveren van de cryptografische sleutels.
- Processen, procedures en parameterisering zijn zodanig ingericht dat deze de cryptografische sleutels optimaal en proportioneel beschermen.
- De beschikbaarheid van cryptografische sleutels (over de gehele uitbestedingsketen) is meegenomen in de continuïteitsplannen van de instelling.
- De instelling beschikt over een inventarisatie van het cryptografisch landschap (encryptieprotocollen en certificaten voor netwerk connecties, key management en data opslag). Bijgehouden wordt op welke termijn (bijvoorbeeld kort, middellang, lang) de toegepaste protocollen niet meer veilig zijn en hoe lang vervanging of mitigatie van een protocol naar verwachting duurt.
- De instelling monitort op het gebruik van onveilige encryptie protocollen en stuurt notificaties naar beheerders als onveilige protocollen gebruikt worden.
- De instelling maakt een roadmap voor haar cryptografisch landschap die in de pas loopt met aankomende dreigingen op korte, middellange en lange termijn.
- De instelling voert jaarlijkse een Cryptography Risk Assessment uit.
- De instelling verkent de risico's en mogelijkheden van Quantum technologie, zoals bijvoorbeeld Quantum key distrubutie of Quantum random number generators.

18.4 Network Security

Marktstandaarden* geven aan dat de instelling een proces inricht dat onder meer het volgende waarborgt:

- De instelling past up-to-date technische beveiligingsmaatregelen toe, zoals firewalls, SIEM, (micro) netwerksegmentatie, intrusion detection, systemen voor de preventie van gegevenslekken (DLP) en de versleuteling van netwerkverkeer.
- De instelling maakt een analyse van het netwerk om te bepalen waar eventueel vergaande netwerk (micro) segmentatie alsmede het "never trust always verify" (ook intern) principe zoals rond de kroonjuwelen van de instelling noodzakelijk is.
- De instelling past endpoint security toe op laptops, tablets, werkstations. Endpoints die niet voldoen aan de security baselines worden geweerd van het netwerk en/of hebben beperkt toegang tot data of ICT-systemen.

Let op!

Risicogebaseerd, uitbesteding en het three lines model

Good Practices hierbij zijn:

- De instelling heeft kennis genomen van onder andere NIST publicaties over een zero trust architecture zoals de *NIST Special Publication (SP) 800-207*, Zero Trust Architecture en de *NIST SP 1800-35A Implementing a Zero Trust Architecture (draft)* waarin 'inherent vertrouwen' geen onderdeel meer is van de netwerkbeveiliging.
- Beheer interfaces van netwerk en security voorzieningen zijn niet direct bereikbaar vanuit (semi)publieke zone's.
- De instelling:
  1. Definieert de delen van het ICT-netwerk dat de kroonjuwelen bevat, zoals specifieke Data, Applicaties, Assets en Services (DAAS).
  2. Brengt de transactiestromen tussen deze delen in kaart.
  3. Definieert en bouwt aan de hand daarvan voor die delen een "Zero Trust-architectuur" door de implementatie van een specifieke set aan beheersmaatregelen.
  4. Stelt Zero Trust beleidsregels op aan de hand van *Wie* krijgt access, *Wat* wordt bij access verstrekt, *Wanneer*, *Waar*, *Waarom*, en *Hoe*.
  5. Monitort en onderhoudt log events van activiteiten op het netwerk.
- De instelling past voor de hiervoor gedefinieerde delen van het netwerk het "*never trust always verify*" principe toe wat inhoudt dat inherent vertrouwen wordt verwijderd uit deze delen van het netwerk en alle handelingen expliciete verificatie vereisen, ook intern.
- De instelling maakt gebruik van tooling die in de netwerkinfrastructuur actief speurt naar ongeautoriseerde apparatuur zoals laptops, routers en Wi-Fi access points met de daarbij behorende beheerprocedures om de toegang tot de ICT-infrastructuur te beperken tot geautoriseerde personen, ICT-services en netwerken. De instelling maakt gebruik van moderne en veilige standaards/protocollen zoals IEEE[12] 802.1X voor Port-based Network Access Control (PNAC), Wi-Fi Protected Access (WPA3) en voert periodieke controles uit op de beheersmaatregelen die zich richten op netwerksegmentering, zoals Access control lists (ACL), VLANs en firewalls tussen de verschillende netwerksegmenten.

12 IEEE staat voor het Institute of Electrical and Electronics Engineers

18.5 Protection of sensitive data

Marktstandaarden* geven aan dat de instelling een proces inricht dat onder meer het volgende waarborgt:

- De instelling heeft beleid geformuleerd ten aanzien van het beveiligd opslaan en delen van vertrouwelijke gegevens en de integriteit van informatie en monitort of dit beleid wordt nageleefd.
- De instelling heeft in kaart gebracht welke informatie vertrouwelijk is en wanneer en waar extra beheersmaatregelen noodzakelijk zijn voor de beveiliging van vertrouwelijke gegevensuitwisseling .
- De instelling maakt gebruik van up to date beveiligde kanalen en integriteitscontroles bij de uitwisseling van vertrouwelijke gegevens.
- De instelling versleutelt in overeenstemming met het data classificatiebeleid data in rust, data in gebruik en data op reis.
- Ten aanzien van uitbestede activiteiten wordt nagegaan of er extra specifieke beheersmaatregelen nodig zijn voor gegevens op reis, opgeslagen gegevens in het geheugen en gegevens in rusttoestand, bijvoorbeeld de toepassing van versleutelings-technieken (encryptie) in combinatie met een passend sleutelbeheer.
- De instelling verstrekt de juiste middelen die haar medewerkers in staat stelt om op veilige wijze data te kunnen versturen en te kunnen ontvangen.

Let op!

Risicogebaseerd, uitbesteding en het three lines model

Good Practices hierbij zijn:

- De instelling past actuele authenticatie en encryptietechnieken toe op netwerkbindingen met partijen die zij vertrouwt.
- In de netwerkinfrastructuur van de instellingen zijn controles ingebouwd die de authenticiteit en de integriteit van berichten waarborgt, alsook de bevestiging van verzending, van ontvangst en de identiteit van de afzender en ontvanger van vertrouwelijke gegevens.
- Vertrouwelijke gegevens worden versleuteld vastgelegd op laptops, harde schijven, USB sticks en andere informatie-dragers. De instelling maakt gebruikt van technieken om de beveiliging van e-mail te verhogen, bijvoorbeeld door middel van anti-spam, DMARC, SPF, DKIM en encryptie van mail.
- De instelling past Data Loss Prevention software toe ter controle van uitgaande berichten en datastromen.

19.1 Malicious software prevention, detection and correction

Marktstandaarden* geven aan dat de instelling een proces inricht dat onder meer het volgende waarborgt:

- De instelling heeft zowel preventieve, detecterende als corrigerende beheersmaatregelen geïmplementeerd om ICT-systemen en applicaties te beveiligen tegen cyberdreigingen, zoals virussen, wormen, malware, ransomware, en spyware.[13]
- De instelling heeft aantoonbaar een afweging gemaakt tussen de samenstelling van de verschillende sets aan tools waarbij kwaliteit en volledigheid in dekking de overhand heeft boven kwantiteit.
- De instelling kijkt bij het toepassen van deze beheersmaatregelen naar de risico's en kansen van technologische ontwikkelingen en neemt actuele informatie over (cyber)dreigingen (Threat Intelligence) mee.

Let op!

Risicogebaseerd, uitbesteding en het three lines model

Good Practices hierbij zijn:

- De instelling maakt bij het in kaart brengen van aanvals-technieken en (technische) beheersmaatregelen gebruik van van verschillende bronnen, waaronder bijvoorbeeld het Mitre ATT&CK framework.
- De instelling heeft tools geïmplementeerd voor de automatische detectie en blokkade van virussen, wormen, malware en spyware zoals moderne firewall technologie, virusscanners, tooling voor e-mail beveiliging (zoals anti-phishing, domain spoofing, spam), Intrusion Detection Systems (IDS) en Intrusion Prevention Systems (IPS), Extended Detection and Response (XDR), Endpoint Detection and Response (EDR) en 'defender tools' met technologie die ziet op Attack Surface Reduction rules.
- De instelling analyseert en leert van incidenten die bij peers of andere vergelijkbare ondernemingen plaats hebben gevonden.
- Logfiles uit voornoemde systemen worden naar een Security Incident and Event Monitoring (SIEM) systeem gestuurd ten behoeve van analyse en (re)actie; de instelling prioriteert de (re)acties op grond van een risico-inschatting.
- De instelling bewaakt voortdurend in hoeverre firewalls, virusscanners, IDS-en, IPS-en up to date zijn en rapporteert daar maandelijks over.
- De instelling gaat na in hoeverre dienstverleners er voor zorgdragen dat firewalls, virusscanners, IDS-en, IPS-en hun infrastructuur up-to-date zijn. De dienstverlener rapporteert hierover aan de instelling die beveiligingstoepassingen voor de instelling beheren.

13 Zie MITRE ATT&CK®

19.2 Vulnerability management

Marktstandaarden* geven aan dat de instelling een proces inricht dat onder meer het volgende waarborgt:

- De belangrijkste ICT-assets zijn op basis van een risicoanalyse geïdentificeerd en geclassificeerd.
- Periodiek worden op basis van Threat Intelligence en vulnerability scans aan de ICT-assets gerelateerde (cyber) kwetsbaarheden vastgesteld en wordt de ernst van het beveiligingsprobleem en mogelijke impact bepaald.
- De scope en passende frequentie van de vulnerability scans wordt vastgesteld.
- De (cyber)kwetsbaarheden worden risicogebaseerd opgepakt.
- De instelling bepaalt een risk response op basis van haar risicotoleranties en monitort de opvolging van de risk response aan de hand van gedefinieerde KCI's (metrics).
- Een impact analyse van de (cyber)kwetsbaarheden wordt periodiek gemaakt.
- Op basis van deze impactanalyse worden risicomitigerende acties bepaald voor bedreigingen die buiten de risicotolerantie van de instelling vallen. Indien nodig worden (tijdig) mitigerende beheersmaatregelen genomen en vindt aanvullende (netwerk)monitoring plaats om misbruik te detecteren.

Let op!

Risicogebaseerd, uitbesteding en het three lines model

Good Practices hierbij zijn:

- De instelling inventariseert regelmatig van welke ICT-assets de bedrijfsprocessen gebruik maken.
- Potentiële kwetsbaarheden worden voorkomen door ervoor te zorgen dat ICT-systemen bijgewerkt zijn, met inbegrip van de software die door de instelling aan haar interne en externe gebruikers wordt verstrekt. Dit doet zij door kritieke security updates gecontroleerd te implementeren, met inbegrip van updates van antivirusdefinities of door compenserende beheersmaatregelen te treffen, bijvoorbeeld (tijdelijke) isolatie van kwetsbare systemen.
- De instelling inventariseert frequent (dagelijks) kwetsbaarheden op basis van Threat Intelligence.
- De instelling stemt de frequentie en het type scan (zoals authenticated of non-authenticated) af op het segment en de risicoanalyse van de eigen organisatie. Daartoe is een analyse gemaakt die periodiek wordt geëvalueerd.
- De instelling bepaalt structureel en risicogebaseerd, wat de impact van deze kwetsbaarheden op de eigen ICT-assets is.
- De instelling inventariseert periodiek voor welke software geen of niet tijdig security updates beschikbaar worden gesteld. Met leveranciers worden heldere KPI's overeengekomen voor oplostijden. Ook wordt bewaakt dat software (overeenkomstig met de gebruikerstermijn) voorzien wordt van security updates. Voor software die (binnenkort) end-of-life is worden mitigerende beheersmaatregelen getroffen.
- Waar mogelijk wordt controle op (delen van) security baselines meegenomen in vulnerability scans.
- De instelling bespreekt met haar dienstverleners regelmatig rapportages / dashboards omtrent de resultaten van uitgevoerde vulnerability scans.

19.3 Application Maintenance

Marktstandaarden* geven aan dat de instelling een proces inricht dat onder meer het volgende waarborgt:

- Onderhoud aan ICT-applicaties verloopt planmatig, gestructureerd en in lijn met de change management procedures van de instelling.
- De instelling bewaakt dat de ICT-applicaties die zij gebruikt, worden ondersteund door de ontwikkelaar/leverancier en dat beveiligingsupdates (patches) beschikbaar worden gesteld. Ook vindt monitoring plaats op de end-of-life datum van gebruikte applicatiesoftware, zodat tijdig mitigerende beheersmaatregelen genomen kunnen worden. De instelling brengt prioritering aan in de uitvoering van onderhoud van de IT applications.
- Oplossingen voor kwetsbaarheden in applicaties zoals patches hebben invloed op de prioritering van reguliere onderhoudswerkzaamheden aan ICT-applicaties.
- Hierbij worden change management processen gevolgd die rekening houden met in hoeverre de kwetsbaarheden kritiek zijn binnen het patchmanagement. Dit is gebaseerd op risicoanalyses die onderdeel uitmaken van het change-management proces (change risk assessments (cra's)).
- Bij de cra's wordt expliciet aandacht besteed aan cyber-dreigingen, kroonjuwelen en aanvalspaden. Deze zijn van invloed op prioritering van implementatie van de changes.
- De risico's die ontstaan door het gebruik van verouderde of niet-ondersteunde ICT-applicaties worden in kaart gebracht, beoordeeld en beperkt. Uit bedrijf genomen ICT-applicaties worden op veilige wijze verwerkt en afgevoerd. Hiertoe wordt een planning opgesteld die wordt afgestemd met alle betrokken bedrijfsonderdelen.
- Een verhoogde focus bij de instelling op klantbeleving en time-to-market leidt er niet toe dat de implementatie van applicatie (beveiligings)maatregelen en investeringen in technologische ontwikkelingen (te) lang worden uitgesteld.

Let op!

Risicogebaseerd, uitbesteding en het three lines model

Good Practice hierbij zijn:

- De instelling hanteert bij de ontwikkeling en aanschaf van ICT-applicaties acceptatiecriteria op het gebied van informatiebeveiliging en cybersecurity.
- De instelling heeft in haar configuratiemanagement database (CMDB) de vervangingstermijn opgenomen van applicaties en op basis hiervan wordt vervanging ingepland.
- Het implementeren van kritieke beveiligingspatches van applicatieleveranciers is een specifiek onderdeel van het patchmanagementproces.

20.1 Protection of security technology

Marktstandaarden* geven aan dat de instelling een proces inricht dat onder meer het volgende waarborgt:

- De instelling heeft inzicht in de voor haar relevante security technologie.[14]
- Gezien hun inherent hoge risicoprofiel, zijn voor de security technologie en de medewerkers die voor de werking van de technologie verantwoordelijk specifieke beveiligings-maatregelen van toepassing.
- Documentatie over de security technologie en beveiligings-maatregelen alsmede autorisaties voor beheerders van de ICT-infrastructuur, waaronder netwerkbeheerders, is op basis van het principle of least privilege, wat inhoudt dat toegang alleen wordt verleend tot security technologie op een 'need-to-know/need-to-have'-basis.

Let op!

Risicogebaseerd, uitbesteding en het three lines model

Good Practices hierbij zijn:

- De instelling heeft voor security technologie aanvullende beheersmaatregelen getroffen, zoals een verscherpte fysieke en logische toegangsbeveiliging, 4-ogenprincipe op beheer en onderhoud, een strikter patch regime en/of versnelde follow-up n.a.v. alerts uit het monitoring systeem, 'tamper resistant' maatregelen, etc.
- Administratieve handelingen op security systemen worden gelogd en gemonitord. Dit geldt voor alle toegangsvormen (e.g., lights-out/out-of-band management, remote). Sessie-recording vindt plaats op grond van een risicoanalyse.
- (Remote) toegang tot systemen vindt plaats over een versleuteld kanaal.
- Administratieve toegang tot systemen vindt bij voorkeur plaats via bastionhosts.
- ICT-systemen die een rol spelen in de beveiliging van de instelling zijn aangesloten op een SIEM.
- Op de security technologie van de instelling wordt gericht beveiligingsonderzoek uitgevoerd door daarin gespecialiseerde partijen.

14 Onder security technologie wordt onder meer verstaan: firewall apparatuur en programmatuur, encryptie programmatuur en apparatuur, hardware security modules (hsm) voor de opslag van certificaten en private keys, etc

21.1 Physical security measures

Marktstandaarden* geven aan dat de instelling een proces inricht dat onder meer het volgende waarborgt:

- In lijn met het risicoprofiel van de instelling zijn de fysieke beveiligingsmaatregelen vastgesteld, gedocumenteerd en uitgevoerd om gevoelige locaties zoals het terrein, de data-centra, bekabeling en (thuis)werklocaties te beschermen tegen onbevoegde fysieke toegang en (milieu)dreigingen zoals stroomstoringen, brand en waterschade.
- Passende beheersmaatregelen ter bescherming tegen bedreigingen staan in verhouding tot het belang van de gebouwen en het kritieke karakter van de werkzaamheden of ICT-systemen die in deze gebouwen gevestigd zijn.
- Fysieke toegangsbeveiligingsmaatregelen worden regelmatig onderhouden en getest.

Let op!

Risicogebaseerd, uitbesteding en het three lines model

Good Practices hierbij zijn:

- Op basis van een risicoanalyse heeft de instelling haar datacenters in klassen (tiers oftewel niveaus) ingedeeld zoals Tier I - De basis, Tier II -Redundantie van elektriciteitsproductie en koeling, Tier III – Onderhoudbaarheid of Tier IV-fouttolerantie en de daarbij behorende beheersmaatregelen getroffen.
- De instelling past fysieke zonering toe met verschillende niveaus van toegang (bijvoorbeeld: publiek, personeel en beperkt) op basis van een risicoanalyse.
- De voor de ICT kritieke gebouwen van de instelling zijn voorzien van inbraakdetectie, waarvan de werking en eventuele meldingen continu (24/7) worden gemonitord.
- De voor de bedrijfsvoering kritieke gebouwen van de instelling zijn voorzien van technische beheersmaatregelen tot het garanderen van continuïteit en het beperken van schade door bijvoorbeeld brand, bliksem, vochtigheid en temperatuur-stijgingen, zoals rookdetectors, brandmelders, blusinstallaties, bliksemafleiders, airconditioning en elektriciteit (noodstroom) voorzieningen.

21.2 Physical access

Marktstandaarden* geven aan dat de instelling een proces inricht dat onder meer het volgende waarborgt:

- Een beleid is gedefinieerd en geïmplementeerd voor de toegangsbeveiliging van gebouwen, terreinen, zones, datacenters, serverruimtes en thuiswerklocaties die van belang zijn voor het uitvoeren van de bedrijfsprocessen.
- Fysieke toegangsbeveiligingsmaatregelen zijn in lijn met het risicoprofiel van de instelling.
- Toegangsprofielen zijn door het management van de instelling geautoriseerd. De toegang tot gebouwen, gebieden, zones en serverruimtes is gebaseerd op de functie en verantwoordelijkheden van de betreffende medewerker/bezoeker.
- Regelmatig wordt de effectiviteit van fysieke toegangsbeveiligingsmaatregelen gecontroleerd en wordt gerapporteerd over de uitkomsten aan het management.
- Beoordeling van de toegekende toegangsrechten (SOLL-IST) en beoordeling van logging van het toegangsbeveiligingssysteem zijn hierbij meegenomen.
- Onnodige toegangsrechten zijn onmiddellijk ingetrokken/verwijderd en fysieke toegangsbeveiligingsmaatregelen zijn onderhouden en getest.

Let op!

Risicogebaseerd, uitbesteding en het three lines model

Good Practices hierbij zijn:

- De instelling controleert dat elke toegang tot een datacentrum 24 uur van te voren is aangevraagd met een change request en bij spoed alleen onder strikte voorwaarden.
- De fysieke toegang tot gebouwen en zones wordt beheerst met behulp van toegangspasjes en -poortjes.
- Bij fysiek onderhoud aan beveiligingsapparatuur is het 4-ogen principe van toepassing.
- De instelling laat de fysieke toegangsbeveiligingsmaatregelen controleren door een “Mystery Guest”.
- ICT componenten die een rol spelen in de fysieke toegangs-beveiliging van de instelling zijn aangesloten op een SIEM (Security Information and Event Management).

22.1 Penetration testing and ethical hacking

Marktstandaarden* geven aan dat de instelling een proces inricht dat onder meer het volgende waarborgt:

- Het bestuur stelt voldoende middelen beschikbaar om een testprogramma te laten uitvoeren, bespreekt de belangrijkste uitkomsten van het testprogramma en zorgt ervoor dat er procedures zijn die erop toezien dat resultaten van de beveiligingstests gecontroleerd, geëvalueerd en geprioriteerd worden.
- Het bestuur zorgt dat geconstateerde kwetsbaarheden onverwijld gemitigeerd worden met duidelijke deadlines, rekening houdende met hoe kritiek de kwetsbaarheden en/of het getroffen ICT-systeem zijn.
- In het testprogramma dat gekoppeld is aan het (ICT-) risk management framework worden een verscheidenheid aan verschillende evaluaties, beoordelingen en tests van de informatiebeveiliging uitgevoerd om een doeltreffende identificatie van kwetsbaarheden in de ICT-systemen en diensten te waarborgen.
- De instelling bepaalt op grond van een risicoanalyse welke soorten en met welke frequentie, scope en diepgang beveiligingstests worden uitgevoerd om de robuustheid en doeltreffendheid van de informatiebeveiligingsmaatregelen te valideren.
- In de risicoanalyse is rekening gehouden met actuele cyberdreigingen, het veranderende landschap van ICT-risico's, eventuele specifieke risico's waaraan de instelling is of zou kunnen zijn blootgesteld.
- De instelling gaat na dat de interne of externe partij die de beveiligingstests uitvoert voldoende onafhankelijk en geëquipeerd is om dergelijke tests uit te voeren (juiste kennis, ervaring en referenties) en dat de tests op een veilige manier worden uitgevoerd.
- Tests van beveiligingsmaatregelen worden uitgevoerd in het geval van wijzigingen aan de infrastructuur, processen of procedures, en indien wijzigingen worden doorgevoerd wegens grote operationele of beveiligingsincidenten, of wegens de vrijgave van nieuwe of aanzienlijk gewijzigde kritieke toepassingen.

Let op!

Risicogebaseerd, uitbesteding en het three lines model

Good Practices hierbij zijn:

- De instelling neemt voor het bepalen van soorten beveiligings-tests in haar risicoanalyse actuele cyberdreigingen mee, zoals phishing, DDoS, ransomware en C-level fraude. Op basis van een risicoanalyse maakt de instelling een jaarplan voor de uit te voeren tests. Onderdeel van dit plan is het uitvoeren van pentests, ethical hacking voor alle (nieuwe en gewijzigde) kritieke ICT-applicaties en het uitvoeren van een red teaming activiteit.
- De instelling voert verschillende typen beveiligingstests uit, waaronder pentests gericht op de beveiliging van infrastructuur en applicaties, red teaming, het testen van de fysieke beveiliging, het testen van menselijk handelen in relatie tot informatiebeveiliging en cybersecurity.[15]
- De instelling maakt gebruik van een bug bounty/responsible disclosure-programma.
- De instelling laat pentests uitvoeren door gespecialiseerde partijen met juiste kennis, ervaring, certificeringen en referenties.
- De instelling wisselt regelmatig van partij die de pentests uitvoert.
- Het bestuur neemt deel aan tweejaarlijkse tabletop oefeningen.

15 Ook kan gedacht worden aan vulnerability assessments en scans, open source analyses, network security assessments, gap analyses, questionnaires en scanning software solutions, source code reviews, scenario-based tests, compatibility testing, performance testing en end-to-end testing

- De instelling betrekt haar kritieke of belangrijke dienstverleners bij haar security tests.
- De instelling sluit bij TIBER aan voor driejaarlijkse Threat Led Penetration Testing (TLPT). Deze tests hebben betrekking op de kritieke functies en diensten van een instelling en worden uitgevoerd op live productiesystemen die de kritieke functies en diensten ondersteunen. Wanneer uitbestede activiteiten binnen de scope vallen, waarborgt de financiële instelling de deelname van de betrokken dienstverlener.

De Nederlandsche Bank N.V.
Postbus 98, 1000 AB Amsterdam
020 524 91 11
dnb.nl

Volg ons op:

DeNederlandscheBank
EUROSYSTEEM