Good Practice

Informatiebeveiliging 2019/2020

DeNederlandscheBank

EUROSYSTEEM

Good Practice - Informatiebeveiliging 2019/2020

Inleiding

Deze Good Practice geeft de onder toezicht van DNB staande instellingen handvatten, te weten beheersingsmaatregelen, waarmee zij kunnen voldoen aan de wettelijke bepalingen om de integriteit, voortdurende beschikbaarheid en beveiliging van de geautomatiseerde gegevensverwerking te waarborgen.

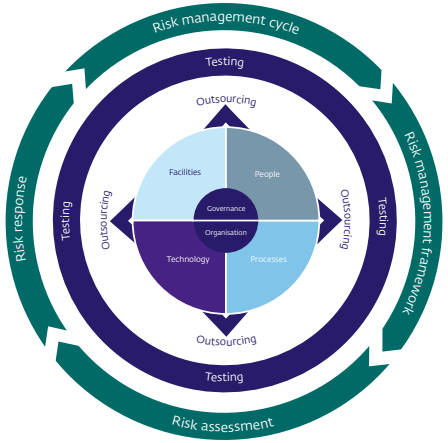
Ter beheersing van risico's op het gebied van informatiebeveiliging en cybersecurity treffen instellingen op grond van een risicoanalyse beheersingsmaatregelen die passen bij de aard, omvang en complexiteit van de risico's van de activiteiten van de instelling en de complexiteit van haar organisatiestructuur.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

Daarnaast evalueren de instellingen periodiek en aantoonbaar – als onderdeel van hun risicomanagement proces (*Riskmanagement cycle*) – in hoeverre de getroffen beheersingsmaatregelen in opzet, bestaan en werking effectief zijn om de voortdurend veranderende risico's op het gebied van informatiebeveiliging en cyberdreigingen het hoofd te bieden. Daar waar nodig worden beheersingsmaatregelen verbeterd of vervangen door betere maatregelen. De instellingen richten hun *Governance* en *Organisation* in om de aansturing hiervan te bewerkstelligen.

Tevens zorgen instellingen ervoor dat zij 'in control' zijn op het gebied van informatiebeveiliging bij uitbesteding (*Outsourcing*) en *Testen* zij in hoeverre zij weerbaar zijn tegen cyberdreigingen. In deze Good Practice is een volwassenheidsmodel 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.



Deze Good Practice kan vanuit twee verschillende invalshoeken worden gelezen:

1. de beheersingsmaatregelen per element uit het model, samengevat voor bestuurders en beleidsbepalers.
Per element vindt u een korte samenvatting van de belangrijkste beheersingsmaatregelen met voorbeelden. De beheersingsmaatregelen zijn toegespitst op respectievelijk de instelling en op de rol van het bestuur bij het implementeren van en het toezien op die beheersingsmaatregelen.

2. gedetailleerd op het niveau van de beheersingsmaatregelen zelf met aanvullende voorbeelden.
Bij elk element staan 'links' waarop kan worden doorgeklikt naar de beheersingsmaatregelen zelf. Voor de leesbaarheid is er voor gekozen elke beheersingsmaatregel slechts onder één element uit het model op te nemen. Het is echter mogelijk dat een beheersingsmaatregel bij meerdere elementen past.

Onder tabblad Inhoud kunt u op de verschillende elementen van het model klikken. Er zijn tabbladen toegevoegd die verwijzen naar de Q&A Informatie-beveiliging en naar het volwassenheidsmodel.

Aanleiding

Sinds een aantal jaren onderzoekt DNB de kwaliteit van informatiebeveiliging en cybersecurity binnen de financiële sector. DNB doet dit sinds 2010 op basis van periodieke *self assessments* bij de onder haar toezicht staande instellingen. Als handvat voor het invullen van deze *self assessments* heeft DNB tot nu toe in de 'Q&A Toetsingskader Informatiebeveiliging voor DNB onderzoek' aangegeven waar zij op let bij haar onderzoeken.

De afgelopen jaren ziet DNB in de financiële sector en daarbuiten een toename van potentieel zeer schadelijke cyberdreigingen. Daarnaast ziet DNB een financiële sector die door verschillende vormen van uitbesteding en samenwerkingsverbanden steeds meer in ketens opereert, met de daarbij behorende kansen en risico's voor informatiebeveiliging en cybersecurity. In onderzoeken is DNB verder een groot aantal goede voorbeelden tegen gekomen die de risico's voortkomend uit deze trends kunnen mitigeren.

Dit alles heeft de aanleiding gevormd om de 'Q&A Toetsingskader Informatiebeveiliging voor DNB onderzoek' te actualiseren. Cybersecurity en aandacht voor informatiebeveiliging bij uitbesteding hebben daarin een prominentere rol gekregen. Deze Good Practice en de daarbij behorende Q&A vormen een actualisering van het 'Toetsingskader Informatiebeveiliging voor DNB onderzoek'.

Wat is er gewijzigd ten opzichte van het vorige toetsingskader?

In deze Good Practice is zoveel mogelijk aangesloten op de reeds bestaande indeling van de voorgaande 'Q&A Toetsingskader Informatiebeveiliging voor DNB onderzoek',[1] maar is de directe link met Cobit losgelaten.[2] De *controls* en *points to consider* uit het vorige Toetsingskader zijn in deze Good Practice overgenomen onder beheersingsmaatregelen. Daarbij zijn cybersecurity en aandachtspunten bij uitbesteding verwerkt. Tevens zijn voorbeelden opgenomen die instellingen kunnen gebruiken bij het implementeren van de beheersingsmaatregelen.

Er zijn vier nieuwe beheersingsmaatregelen toegevoegd:

1. Employee awareness: Het actief bevorderen van bewustzijn voor cyberrisico's bij medewerkers. Zie onder element *People*, nr. 9.3
2. Vulnerability management: Het actief monitoren en oplossen van kwetsbaarheden in de IT-infrastructuur en IT-applicaties. Zie onder element *Technology*, nr. 19.2
3. Application Life cycle management: Borgen dat applicaties tijdig worden onderhouden en uitgefaseerd, opdat het gewenste informatiebeveiligingsniveau niet in gevaar komt. Zie onder element *Technology*, nr. 19.3
4. Penetration testing and ethical hacking: Testen van de weerbaarheid van de instelling tegen cyberdreigingen. Zie onder element *Testing*, nr 22.1

Nieuw is verder in deze Good Practice dat de rol van het bestuur expliciet wordt benoemd. Daarnaast wordt rond deze Good Practice samen met de sectoren invulling gegeven aan een "feedback loop" waarbij instellingen input kunnen leveren om de voorbeelden actueel te houden.

Informatiebeveiliging en cybersecurity

Onder informatiebeveiliging wordt in deze Good Practice verstaan het geheel van preventieve, detectieve, repressieve en correctieve maatregelen alsmede procedures en processen die de beschikbaarheid, exclusiviteit en integriteit van alle vormen van informatie binnen een instelling garanderen. Het doel hierbij is de continuïteit en

1 Voor de herkenbaarheid zijn de beheersingsmaatregelen in dit document voorzien van dezelfde nummering als de 'Q&A Toetsingskader Informatiebeveiliging voor DNB onderzoek' (2010-2018).

2 Bij het actualiseren van deze Good Practice en bijbehorende Q&A zijn relevante Internationale Standaarden zoals Cobit (Control Objectives for Information and related Technology) van ISACA, ISO27000 en het NIST Cybersecurity Framework meegenomen.

betrouwbaarheid van de IT, de informatie en de informatievoorziening te waarborgen en de gevolgen van eventuele beveiligingsincidenten tot een acceptabel en door de instelling vooraf bepaald niveau te beperken. Hierbij is met name van belang dat de procedures en (technische) maatregelen die vorm geven aan informatiebeveiliging passen bij de aard en doelstellingen van de instelling. DNB ziet cybersecurity als een integraal onderdeel van informatiebeveiliging.

Reikwijdte

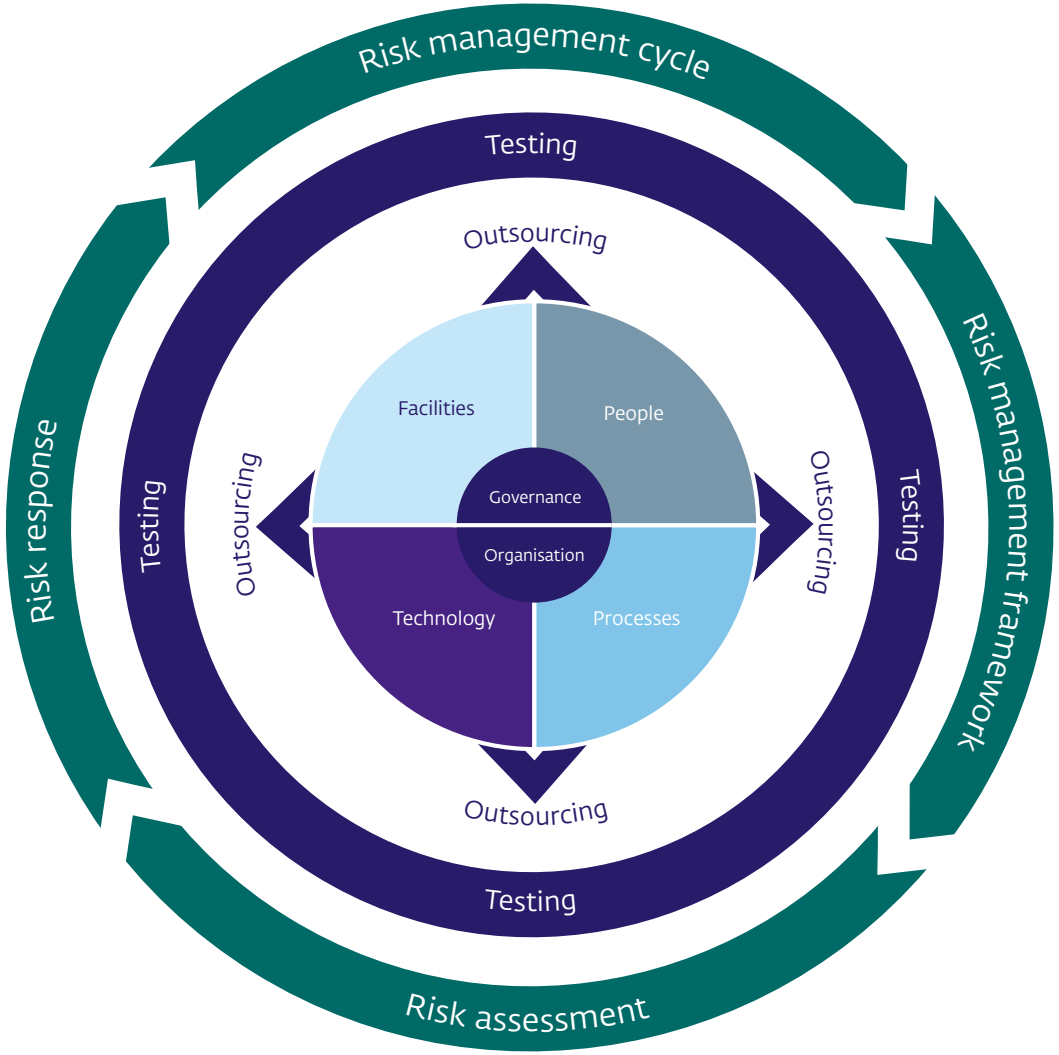
Deze Good Practice laat zien – zonder ernaar te streven compleet te zijn - wat DNB onder een juiste invulling verstaat van de regelgeving die betrekking heeft op het op een integere en beheerste wijze inrichten van informatiebeveiliging en cybersecurity. Het is aan de instellingen zelf om een beheersingsraamwerk te implementeren dat past bij de aard en omvang 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 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. De afweging over de toepassing berust bij deze instellingen zelf.

DNB Toetsingskader Informatiebeveiliging 2019-2020



Q&A Informatiebeveiliging

Zie Open Boek Toezicht, http://www.toezicht.dnb.nl/3/50-203304.jsp

Inleiding

Sinds een aantal jaren onderzoekt DNB de kwaliteit van informatiebeveiliging en cybersecurity binnen de financiële sector. DNB doet dit sinds 2010 op basis van periodieke *self assessments* bij de onder haar toezicht staande instellingen. Als handvat voor het invullen van deze *self assessments* heeft DNB tot nu toe in de 'Q&A Toetsingskader Informatiebeveiliging voor DNB onderzoek' aangegeven waar zij op let bij haar onderzoeken[3]. Deze Q&A en de Good Practice Informatiebeveiliging (waarvan de link staat onder 'Gerelateerde Downloads' op deze pagina) vormen een actualisering van het 'Toetsingskader Informatiebeveiliging voor DNB onderzoek'.

Vraag:
Hoe voldoen instellingen onder het toezicht van DNB aan de wettelijke eisen ten aanzien van de integriteit, voortdurende beschikbaarheid en beveiliging van de geautomatiseerde gegevensverwerking?

Antwoord:
Conform art. 3.17 Wet Financieel Toezicht, juncto artikel 20 Besluit prudentiële regels en de Pensioenwet (zie link onder 'Wetten en EU Richtlijnen' op deze pagina) beschikken instellingen onder toezicht van DNB over adequate procedures en maatregelen ter beheersing van IT-risico's. Het gaat hierbij onder meer om het waarborgen van de integriteit, voortdurende beschikbaarheid en de beveiliging van geautomatiseerde gegevens. Adequaat betekent in dit verband dat de procedures en maatregelen zijn gebaseerd op de aard, omvang en complexiteit van de risico's van de activiteiten van de instelling en de complexiteit van haar organisatiestructuur.

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

Daarnaast evalueren de instellingen periodiek en aantoonbaar – als onderdeel van hun risicomanagementproces (*Riskmanagement cycle*) – in hoeverre de getroffen beheersingsmaatregelen in opzet, bestaan en werking effectief zijn om de voortdurend veranderende risico's op het gebied van informatiebeveiliging en cyberdreigingen het hoofd te bieden. Daar waar nodig worden beheersingsmaatregelen verbeterd of vervangen door andere maatregelen. De instellingen richten hun *Governance* en *Organisation* in om de aansturing hiervan te bewerkstelligen.

Tevens zorgen instellingen ervoor dat zij 'in control' zijn op het gebied van informatiebeveiliging en cybersecurity bij uitbesteding (*Outsourcing*) en *Testen* zij in hoeverre zij weerbaar zijn tegen cyberdreigingen.

In de bij deze Q&A behorende Good Practice Informatiebeveiliging (waarvan de link staat onder 'Gerelateerde Downloads' op deze pagina) biedt DNB handvatten waarmee instellingen een praktische

3 https://www.toezicht.dnb.nl/3/50-203304.jsp

invulling kunnen geven aan de beheersingsmaatregelen 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 beheersingsmaatregelen) gegeven die naar het oordeel van DNB goede invulling geven aan voornoemde vereiste uit art 3.17 Wet Financieel Toezicht, juncto artikel 20 Besluit prudentiële regels en de Pensioenwet.

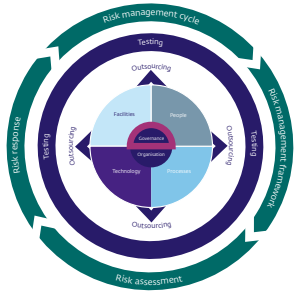
Relevante wet- en regelgeving

- 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*
- 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.

\# Relevante wet- en regelgeving vanuit EIOPA en EBA worden toegevoegd zodra deze van kracht zijn.

Governance



DNB verstaat onder dit element

Governance gaat over het geven van strategische, tactische en operationele sturing aan informatiebeveiliging en cybersecurity in overeenstemming met de strategie van de instelling, haar risicobereidheid en wet- en regelgeving. Hierbij wordt rekening gehouden met de aard, omvang en complexiteit van de instelling.

Relevante beheersingsmaatregelen voor de instelling

Bij het element *Governance* let DNB met name op het opstellen, onderhouden en uitdragen van een informatiebeveiligingsbeleid en een daaruit volgend informatiebeveiligingsplan, waarbij taken en verantwoordelijkheden zijn belegd en formele rapportagelijnen zijn ingericht. Een belangrijk aandachtspunt is dat in het beleid nadrukkelijk aandacht wordt gegeven aan de weerbaarheid tegen cyberdreigingen. Onder meer let DNB erop dat het beleid is geoperationaliseerd in zowel preventieve, detecterende, corrigerende als repressieve maatregelen. Tevens is het van belang dat de instelling relevante ontwikkelingen op het gebied van informatiebeveiliging en cybersecurity monitort. Verder let DNB erop dat bedrijfsprocessen en IT-systemen opgezet zijn volgens een door de instelling vastgestelde informatiearchitectuur. Deze architectuur maakt inzichtelijk hoe de IT-systemen en dataverzamelingen ondersteunend zijn aan de strategie van de instelling en haar processen. De instelling kan daarbij bijvoorbeeld gebruik maken van een classificatieschema op basis waarvan relevante beveiligingsmaatregelen zijn getroffen voor bijvoorbeeld toegang, versleuteling, opslag en retentie van gegevens. De instelling werkt volgens geaccepteerde (technische) standaarden op het gebied van informatiebeveiliging en cybersecurity.

Rol van het bestuur bij de implementatie van deze beheersmaatregelen

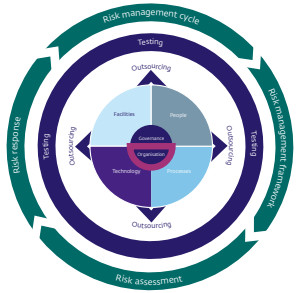
Het bestuur van de instelling is eindverantwoordelijk voor een adequate governance en ziet erop toe dat alle elementen van informatiebeveiliging en cybersecurity zijn beheerst. U kunt hierbij bijvoorbeeld denken aan de volgende aspecten:

- Het bestuur stelt periodiek een informatie-beveiligingsbeleid vast inclusief een daaruit volgend informatiebeveiligingsplan, waarbij de eisen vanuit het lijnmanagement, risk en compliance zijn vertaald naar te nemen acties.
- Vervolgens zorgt het bestuur er binnen de *Risk Management cycle* voor dat periodiek in het bestuur wordt nagegaan in hoeverre de informatie-beveiligings- en cybersecurity risico's van de instelling passen binnen de risicobereidheid van het bestuur. Hierbij kan worden afgewogen in hoeverre een effectieve mix van maatregelen – *People, Processes, Technology* en *Facilities* – is getroffen om risico's van de instelling te beheersen.
- Indien zich een substantieel incident voordoet wordt het bestuur voldoende geïnformeerd over de respons, geeft zij indien nodig sturing aan deze respons en evalueert zij achteraf het incident en neemt zij de uitkomsten van deze evaluatie mee in voornoemde risicomanagement cyclus.
- Goed opdrachtgeverschap: 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.

Beheersingsmaatregelen:

- 1.1 Information Security plan
- 1.2 IT Policies Management
- 2.1 Enterprise Information Architecture Model
- 2.2 Data classification scheme
- 3.1 Monitor future trends and regulations
- 3.2 Technology standards

Organisation



DNB verstaat onder dit element

Het is belangrijk dat taken ten aanzien van informatie-beveiliging en cybersecurity eenduidig binnen de instelling zijn belegd en dat activiteiten op dit gebied in overeenstemming zijn met de strategie van de instelling, haar risicobereidheid en met wet- en regelgeving.

Relevante beheersingsmaatregelen voor de instelling

Bij het element *Organisation* let DNB met name op het documenteren en formaliseren van de rollen en verantwoordelijkheden voor de risicobeheer- 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).

Verder let DNB erop dat het eigenaarschap van alle gegevens en informatiesystemen die de instelling gebruikt bij haar bedrijfsvoering, eenduidig is belegd. Daarnaast let DNB erop dat toegang tot gegevens en informatiesystemen door middel van toegangsrechten is 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 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. Tegelijkertijd brengen instellingen het aantal accounts met hoge rechten terug. Met een dergelijke aanpak kunnen ongewenste functievermengingen (toxic combinations) en de daarmee samenhangende risico's, worden vermeden.

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 informatiebeveiliging en cybersecurity zijn beheerst. U kunt hierbij bijvoorbeeld denken aan de volgende aspecten:

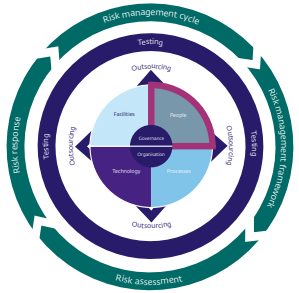
- Het bestuur heeft taken en verantwoordelijkheden op het gebied van het inrichten, beheren en controleren van informatiebeveiliging en cyber-security helder belegd.
- Het bestuur let er op dat ongewenste functie-vermengingen (toxic combinations) en de daarmee samenhangende risico's door de instelling worden vermeden.
- Op grond van het risicoprofiel van de instelling en de risicobereidheid 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.
- Goed opdrachtgeverschap: 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 informatiesystemen en functiescheiding in hun organisaties.

Beheersingsmaatregelen:

- 5.1 Responsibility for risk, security and compliance
- 5.2 Management of information security
- 6.1 Data and system ownership
- 7.1 Segregation of duties

People



DNB verstaat onder dit element

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

Relevante beheersingsmaatregelen voor de instelling

De menselijke factor is zeer bepalend voor de beheersing van de informatiebeveiliging en cyber-security risico's. Bij *People* let DNB met name op het aantrekken en behouden van medewerkers met kennis van informatiebeveiliging en cybersecurity die aansluit bij de ambitie en het risicoprofiel van de instelling. Tevens let DNB erop dat 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 IT-beheerders en informatiebeveiligings-specialisten. Met security awareness programma's besteedt de instelling expliciet aandacht aan cyberdreigingen.
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).

DNB let er verder op dat instellingen op grond van een risicoanalyse bepalen waar hun afhankelijkheid van individuen met kennis van informatiebeveiliging en cybersecurity haar risicotolerantie overschrijdt. De instelling treft maatregelen om te grote afhankelijkheid van individuen te beperken (key person risk).

Daarnaast let DNB erop dat instellingen voorafgaand aan de indiensttreding, interne- en externe medewerkers screenen afhankelijk van het risicoprofiel van de functie. Tijdens het dienstverband of langdurende inhuurperiode wordt deze screening periodiek herhaald. Bij functiewijzigingen 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.

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 beschikt ten minste over basiskennis van informatiebeveiliging en cybersecurity.
  Het bestuur heeft aantoonbaar trainingen en opleidingen gevolgd om de belangrijkste IT-risico's en beheersingsmaatregelen voor haar 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 moeten borgen (tone-at-the-top). Zogeheten 'management overrides' van bestaande processen en

procedures door het bestuur en senior management worden waar mogelijk vermeden.

- Goed opdrachtgeverschap: 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.

Beheersingsmaatregelen:

8.1 Personnel recruitment and retention

8.2 Personnel competencies

8.3 Dependence upon individuals

8.4 Personnel clearance procedures

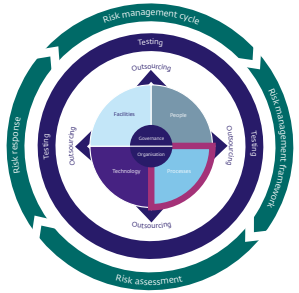
8.5 Job change and termination

9.1 Knowledge transfer to end users

9.2 Knowledge transfer to operations and support staff

9.3 Employee awareness

Processes



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.

Relevante beheersingsmaatregelen voor de instelling

Bij het onderdeel *Processes* is het van belang dat de instelling een IT-continuïteitsplan 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 cyberaanvallen te bevorderen. DNB let er op hoe de instelling omgaat met beveiligingsincidenten, waaronder cybersecurity incidenten met als doel de hieruit volgende schade zoveel mogelijk te beperken en herhaling te voorkomen. Hierbij let DNB erop dat de instelling beschikt over een geformaliseerd beleid voor incidentbeheer, waarin een escalatieprocedure en escalatiecriteria zijn opgenomen. Cybersecurity incidenten worden daarbij conform geldende regels gerapporteerd aan de autoriteiten. Oplossingen voor incidenten worden regelmatig geanalyseerd om processen en IT-systemen te verbeteren. Een voorbeeld hierbij is het oprichten van een Computer Emergency Response Team (CERT) binnen de instelling.

DNB let er verder op dat instellingen op beheerste wijze wijzigingen doorvoeren met als doel om te voorkomen dat deze wijzigingen (bedoeld of onbedoeld) leiden tot een lager informatiebeveiligingsniveau of leiden tot verstoringen in de bedrijfsprocessen en/of de data-integriteit negatief beïnvloeden. Daarbij let DNB erop dat wijzigingen in IT-applicaties, IT-infrastructuur, IT-processen en kritische systeeminstellingen een gestandaardiseerd en gecontroleerd pad volgen, waarbij wijzigingen worden geregistreerd (audit trail) geaccordeerd en geëvalueerd.

Tevens let DNB erop dat criteria voor het beschermen van testgegevens zijn opgesteld en worden onderhouden, waarbij test- en productiegegevens goed van elkaar worden gescheiden. Wijzigingen worden getest volgens een testplan waarin acceptatiecriteria zijn opgenomen; ook voor beveiliging en IT-performance.

Daarnaast heeft DNB aandacht voor de manier waarop de instelling de kwaliteit van de IT-beheerprocessen heeft geborgd. Daarbij let DNB erop dat de instelling procedures implementeert en onderhoudt met betrekking tot onder meer:

- configuratie (het bijhouden van de IT-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.

Tevens let DNB erop dat de instelling periodiek onafhankelijke assurance verkrijgt over het functioneren van de beheersingsmaatregelen.

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 beheersingsmaatregelen gedurende een bepaalde periode.

Rol van het bestuur bij de implementatie van deze beheersmaatregelen

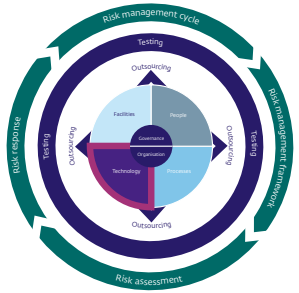
Het bestuur van de instelling is eindverantwoordelijk voor het zorgdragen en/of controleren dat de strategie en het overall IT-security plan in lijn is met de richtlijnen van het bestuur en de overige bedrijfsprocedures. U kunt hierbij bijvoorbeeld denken aan de volgende aspecten:

- Het bestuur controleert jaarlijks of het IT-continuïteitsplan nog aansluit op aan de IT-omgeving door haar medewerkers hiertoe opdracht te geven en over de resultaten te laten rapporteren aan het bestuur.
- Het bestuur neemt actief deel aan de continuïteitstesten en let er op dat ook actuele cyberdreigingen in de contrinuiteitsplannen (scenario's) zijn opgenomen.

Beheersingsmaatregelen:

- 10.1 Change standards and procedures
- 10.2 Impact assessment, prioritisation and authorization
- 10.3 Test environment
- 10.4 Testing of changes
- 10.5 Promotion to Production
- 11.1 IT Continuity plans
- 11.2 Testing of the IT Continuity plan
- 11.3 Offsite backup storage
- 11.4 Backup and 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 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 Management
- 17.2 User account management

Technology



DNB verstaat onder dit element

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

Relevante beheersingsmaatregelen voor de instelling

Bij het element *Technology* let DNB er met name op dat technische beheersingsmaatregelen zodanig zijn ingericht dat zij een hoog niveau van beschikbaarheid, exclusiviteit en integriteit waarborgen. Daarbij houden risicoanalyses van de instelling rekening met actuele cyberdreigingen. Voorbeeld hierbij zijn de SANS[4] Top 20, dreigingsanalyses van het NCSC[5] en ENISA[6] en uitkomsten van penetration testing en ethical hacking. Daarbij let DNB erop dat het onderhoud aan de IT-infrastructuur en IT-applicaties planmatig en gestructureerd verloopt, in lijn met de change management procedures en het life-cyclemanagementproces van de instelling.

De instelling let er bijvoorbeeld op dat de technologische veroudering van haar IT-infrastructuur en IT-applicaties binnen haar risicotolerantiegrenzen blijft en dat security updates worden toegepast. Daarnaast let DNB er op dat instellingen in beeld hebben van welke IT-infrastructuur en IT-applicaties hun bedrijfsprocessen afhankelijk zijn en in hoeverre de IT-systemen kwetsbaar zijn voor cyberaanvallen. Bijvoorbeeld kan de instelling op basis van een risicoanalyse en threat intelligence regelmatig vulnerability scans uitvoeren op haar IT-infrastructuur en IT-applicaties.

De instelling heeft zowel preventieve, detecterende als corrigerende maatregelen geïmplementeerd om IT-systemen te beschermen tegen cyberaanvallen, zoals virussen, malware, cryptoware, spyware en DDoS aanvallen. Wat betreft de preventieve maatregelen let DNB erop dat de instelling up-to-date technische beveiligingsmaatregelen toe past (zoals firewalls, netwerksegmentatie en intrusion detection) en daarbij behorende beheerprocedures heeft ingericht om de toegang tot de IT-infrastructuur te beperken tot geautoriseerde personen. De instelling past daartoe bijvoorbeeld moderne firewall technologie toe die in lijn zijn met standaarden zoals GovCert, ISO/IEC[7], ITSEC[8]. De instelling heeft daarnaast beleid geformuleerd ten aanzien van het delen van vertrouwelijke informatie. 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. Daarbij let DNB er ook op dat het beheer van cryptografische sleutels op beheerste wijze plaatsvindt.

4 System Administration, Networking, and Security Institute. Zie https://www.sans.org/

5 Nationaal cybersecurity Centrum. Zie https://ncsc.nl

6 European Union Agency for Network and Information Security. Zie https://www.enisa.europa.eu/

7 International Standards Organisation, Zie https://www.iso.org

8 Information Technology Security Evaluation Criteria. Zie https://www.itsec.org

DNB let er op dat een verhoogde focus bij de instellingen 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

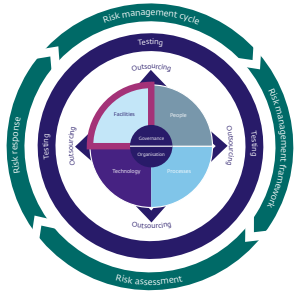
Het bestuur van de instelling is eindverantwoordelijk voor het uitzetten en implementeren van de IT-strategie. U kunt hierbij bijvoorbeeld denken aan de volgende aspecten:

- Het bestuur zorgt dat zij zich periodiek laat informeren over de risico's op het gebied van informatiebeveiliging en cybersecurity 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 Riskmanagement Cycle zie daartoe ook het betreffende element in het model.

Beheersingsmaatregelen:

- 18.1 Infrastructure resource protection and availability
- 18.2 Infrastructure maintenance
- 18.3 Cryptographic key management
- 18.4 Network Security
- 18.5 Exchange of sensitive data
- 19.1 Malicious software prevention, detection and correction
- 19.2 Vulnerability assessment
- 19.3 Application Life cycle management
- 20.1 Protection of security technology

Facilities



DNB verstaat onder dit element

Onder dit element verstaat DNB onder andere dat toegang tot informatie ook fysiek is beveiligd, denk hierbij aan maatregelen die de toegang tot kantoorgebouwen en datacenters beperken.

Relevante beheersingsmaatregelen voor de instelling

Bij het onderdeel *Facilities* let DNB er met name op dat de instelling een beleid heeft gedefinieerd en geïmplementeerd, dat regelmatig wordt geactualiseerd en in lijn is met het risicoprofiel van de instelling, ten aanzien van:

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

Een voorbeeld hierbij is dat de instelling ook maatregelen treft om de beveiligingssystemen zelf te beschermen. Hierbij kan worden gedacht aan aanvullende fysieke toegangsbeveiliging, strikte netwerksegmentering, een strikter patch regime en/of snellere follow-up na alerts of incidenten met die beveiligingssystemen.

DNB let er verder op dat de instelling regelmatig de effectiviteit van fysieke toegangs-beveiligings-maatregelen controleert 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:

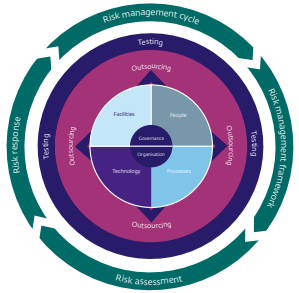
- Het bestuur laat zien belang te hechten aan afdoende fysieke toegangsbeveiliging en implementeert de benodigde maatregelen op basis van het risicoprofiel van iedere locatie.
- Het bestuur laat zich hierover informeren en spreekt de organisatie erop aan als er hiaten zijn (tone at the top).

Beheersingsmaatregelen:

21.1 Physical security measures

21.2 Physical access

Outsourcing



DNB verstaat onder dit element

DNB ziet dat instellingen in toenemende mate belangrijke bedrijfsprocessen zoals ICT, vermogens-beheer, 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 cybersecurity is dat bijvoorbeeld de ongewenste omgang van de dienstverlener met vertrouwelijke gegevens van de instelling. Ook bestaat het risico dat de beveiliging van vertrouwelijke gegevens niet in overeenstemming is met het interne beleid als gevolg van onder uitbesteding door de dienstverlener.

Relevante beheersingsmaatregelen voor de instelling

Voor alle beheersingsmaatregelen uit deze Good Practice geldt dat bij uitbesteding van activiteiten/systemen de instelling eindverantwoordelijk blijft voor informatiebeveiliging en cybersecurity. Dit betekent dat DNB erop let dat de instelling een proces heeft ingericht dat ten minste het volgende waarborgt:

- De instelling heeft afspraken gemaakt met de dienstverlener ten aanzien van het naleven van het informatiebeveiligingsbeleid en indien van toepassing de uitvoering van het informatiebeveiligingsplan van de onderneming. Deze werken door naar eventuele onderaannemers.
- De instelling ontvangt Service Level Rapportages (SLR) en/of assurance-rapportages met de juiste scope en diepgang aan de hand waarvan die afspraken kunnen worden gemonitord.
- De instelling stuurt bij wanneer haar risicotoleranties worden overschreden (zie daartoe ook de Risk Management cycle).

Om verder handvatten te geven aan waar DNB op let bij uitbesteding in het kader van informatiebeveiliging en cybersecurity zijn drie specifieke beheersings-maatregelen 14.1, 14.2 en 16.3 in deze Good Practice opgenomen.

Uit deze drie beheersingsmaatregelen komt naar voren dat DNB erop let dat de instelling specifieke prestatie criteria overeenkomt met haar dienstverleners, dat deze afspraken worden gemonitord en dat daarover wordt gerapporteerd aan belanghebbenden. Verantwoordingsrapportages van de dienstverleners worden door de instelling geanalyseerd om trends en ontwikkelingen te identificeren en eventueel de dienstverlening bij te sturen.

Van belang is daarnaast dat in de contractvoor-bereidingsfase aandacht wordt besteed 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 dienstverleners een risicoanalyse op en bepaalt hoe zij met eventuele restrisico's omgaat. Bij deze analyse zijn risico's bij partijen waaraan diensten zijn onder-uitbesteed 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. Onder-uitbesteding is hierbij in scope.

Verder zijn bij een aantal beheersingsmaatregelen uit deze Good Practice voorbeelden opgenomen over hoe de instelling de uitbesteding kan beheersen.

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 evalueert periodiek maar minimaal jaarlijks 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.

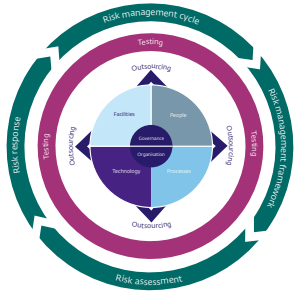
Beheersingsmaatregelen:

14.1 Monitoring and reporting of Service Level Achievements

14.2 Supplier risk management

16.3 Internal control at third parties

Testing



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 belangrijke uitbestedingen meenemen.

Relevante beheersingsmaatregelen voor de instelling

DNB let erop dat de instelling op grond van een risicoanalyse en actuele cyberdreigingen bepaalt welke soorten beveiligingstests worden uitgevoerd alsmede de scope en diepgang van die tests. Daarbij is de aard en frequentie van deze testen afhankelijk van het risicoprofiel van de instelling. 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 extern ingehuurde partijen.

Daarnaast let DNB erop dat de instelling na gaat dat de partij die de beveiligingstests uitvoert voldoende geëquipeerd is om dergelijke tests uit te voeren (hebben zij de juiste kennis en 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.

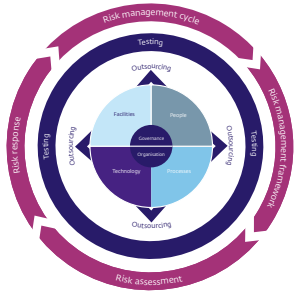
U kunt hierbij bijvoorbeeld denken aan de volgende aspecten:

- Het bestuur stelt voldoende middelen beschikbaar om periodiek security tests te laten uitvoeren.
- Het bestuur houdt in het oog dat de scope van security tests de verschillende elementen uit het model van deze Good Practice omvat en daarbij rekening houdt bij het laten uitvoeren van de tests.
- Het bestuur zorgt ervoor dat in de RvB vergadering de uitkomsten van security tests worden besproken. Verder zorgt het bestuur ervoor dat met passende maatregelen opvolging wordt gegeven aan de constateerde risico's.

Beheersingsmaatregelen:

22.1 Penetration testing and ethical hacking

Risk management cycle



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 maatregelen om risico's te beperken en accepteert (tijdelijk) eventuele restrisico's. Geaccepteerde restrisico's worden periodiek opnieuw geëvalueerd en opnieuw ter acceptatie aangeboden.

Relevante beheersingsmaatregelen voor de instelling

Bij het element *Risk Management cycle* let DNB er met name op dat de instelling de beheersing van risico's ten aanzien van informatiebeveiliging en cybersecurity heeft geborgd door de implementatie van een IT Risk Management framework. Dit raamwerk is gebaseerd op een Plan-do-check-act cyclus, waarover regelmatig wordt gerapporteerd aan het bestuur. DNB let erop dat de instelling in haar *IT Risk management framework* eenduidige definities voor informatiebeveiliging en cybersecurity hanteert, die zijn ontleend aan markt standaarden zoals bijvoorbeeld NIST, ISO en Cobit en consistent worden toegepast binnen alle documenten en rapportages. Een voorbeeld hierbij is dat actuele cyberdreigingen zoals malware, cryptoware, DDoS aanvallen en phishing deel uitmaken van het IT Risk Management framework van de instelling.

Daarnaast let DNB erop dat de instelling periodiek Risk assessments uitvoert op basis van kwalitatieve en kwantitatieve methoden en waarin actuele cyberdreigingen zijn geanalyseerd en geprioriteerd. Een voorbeeld hierbij is dat de instelling haar 'kroonjuwelen' in kaart brengt, deze periodiek evalueert en relateert aan actuele cyberdreigingen. Daar waar nodig treft de instelling aanvullende beheersingsmaatregelen. Daarnaast maakt de instelling expliciet welke risico's formeel worden geaccepteerd. Maatregelen die niet (meer) effectief werken worden aangepast, vervangen door andere maatregelen of uitgefaseerd.

Verder let DNB erop dat de instelling voor niet geaccepteerde risico's een 'risk action plan' opstelt 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 maatregelen noodzakelijk zijn.

DNB let erop dat zowel de 1e, 2e en 3e lijn actief betrokken zijn bij de totstandkoming, uitvoering en het onderhoud van de risk management cycle.

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 maatregelen die voortkomen uit de Risk management cycle. U kunt hierbij bijvoorbeeld denken aan de volgende aspecten:

- Het bestuur heeft een risicomanagementcyclus ingericht en wordt regelmatig geïnformeerd over informatiebeveiligingsrisico's en cyberdreigingen.
- Het bestuur evalueert periodiek het riskmanagement framework en de effectiviteit

van de daarin opgenomen informatiebeveiligings-maatregelen. Hierbij wordt rekening gehouden met actuele ontwikkelingen en risico's. Verzekeraars verwerken risico's in de ORSA, pensioenfondsen in de ERB en banken in de ICAAP.

- Het bestuur stelt voldoende middelen beschikbaar om effectieve maatregelen 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.
- Het bestuur weegt periodiek af in hoeverre een effectieve 'mix' van maatregelen – 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).

Beheersingsmaatregelen:

4.1 IT Risk Management framework

4.2 Risk assessment

4.3 Maintenance and monitoring of a risk action plan

Volwassenheidsmodel

Zoals aangegeven in de inleiding bij deze Good Practice onderzoekt DNB sinds een groot aantal jaren de kwaliteit van informatiebeveiliging als thema binnen de financiële sector. Onderdeel van dit thema zijn periodieke *self assessments*, die DNB bij de onder haar toezicht staande instellingen uitzet. In deze self assessments zijn "Operational Maturity Levels", volwassenheidsniveaus opgenomen.

Het doel van de self assessments is vast te stellen in hoeverre de beheersing van informatiebeveiliging en cybersecurity bij de instellingen op het vereiste niveau is. Om dit niveau te kunnen vaststellen, hanteert DNB een volwassenheidsmodel. DNB veronderstelt dat financiële instellingen aantoonbaar 'in control' zijn. In het door DNB gehanteerde model met 58 beheersingsmaatregelen komt dat overeen met ten minste een volwassenheidsniveau van '3': aantoonbare werking gedurende een langere periode voor 55 beheersingsmaatregelen. Voor de overige 3 beheersingsmaatregelen verwacht DNB een hoger volwassenheidsniveau van '4' . Dit betreffen de controls #4.1, #4.2 en #4.3 in de Risk Management cycle.[9]

Bij het invullen van het self assesement houdt de instelling bij het toekennen van de volwassen-heidsniveaus, 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.

Het verschil tussen volwassenheidsniveau "3" en "4" is dat niveau "3" ziet op implementatie en werking van de beheersingsmaatregel; niveau "4" past aanvullend bij een aantoonbare evaluatie van de effectiviteit van de beheersingsmaatregel en de beoogde herstelacties die hieruit mogelijk voortvloeien.

9 De definities van de volwassenheidsniveaus sluiten 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 beheersingsmaatregel is geen aandacht besteed.	
1	**Initieel** – De beheersingsmaatregel is (gedeeltelijk) gedefinieerd maar wordt op inconsistente wijze uitgevoerd. Er is een grote afhankelijkheid van individuen bij de uitvoering van de beheersingsmaatregel.	■ Geen of beperkte beheersingsmaatregel geïmplementeerd. ■ Niet of ad-hoc uitgevoerd. ■ Niet /deels gedocumenteerd. ■ Wijze van uitvoering afhankelijk van individu (niet gestandaardiseerd)
2	**Herhaalbaar maar informeel** – De beheersingsmaatregel is aanwezig en wordt op consistente en gestructureerde, maar op informele wijze uitgevoerd.	■ De uitvoering van de beheersingsmaatregel is gebaseerd op een informele maar wel gestandaardiseerde werkwijze. Deze werkwijze is niet volledig gedocumenteerd.
3	**Gedefinieerd** – De opzet van de beheersingsmaatregel is gedocumenteerd en wordt op gestructureerde en geformaliseer-de wijze uitgevoerd. De vereiste effectiviteit van de beheersing-smaatregel is aantoonbaar en wordt getoetst.	■ Beheersingsmaatregel is gedefinieerd o.b.v. risico assessment. ■ Gedocumenteerd en geformaliseerd. ■ Verantwoordelijkheden en taken zijn eenduidig toegewezen. ■ Opzet, bestaan en effectieve werking zijn aantoonbaar. ■ Effectieve werking van controls wordt periodiek getoetst. ■ De toetsing vindt risicogebaseerd plaats en toont aan dat de control effectief is over een langere periode (>6 maanden). ■ De uitvoering van de beheersingsmaatregel wordt aan het management gerapporteerd.
4	**Beheerst en meetbaar** – De effectiviteit van de beheersings-maatregel wordt periodiek geëvalueerd. Daar waar nodig wordt de beheersingsmaatregel verbeterd of vervangen door andere beheersingsmaatregel(en). De evaluatie wordt vastgelegd.	Criteria voor niveau 3 plus de volgende onderscheidende criteria: ■ Periodieke (control) evaluatie en opvolging vindt plaats. ■ Evaluatie is gedocumenteerd. ■ Taken en verantwoordelijkheden voor het evalueren zijn geformaliseerd. ■ Frequentie waarop wordt geëvalueerd is gebaseerd op het risicoprofiel van de instelling en is minimaal jaarlijks. ■ In de evaluatie worden (operationele) incidenten meegenomen. ■ De uitkomsten van de evaluatie wordt aan het management gerapporteerd.
5	**Continu verbeteren** – De beheersingsmaatregelen zijn verankerd in het integrale risicomanagement raamwerk, waarbij continu gezocht wordt naar verbetering van de effectiviteit van de maatregelen. Hierbij wordt gebruik gemaakt van externe data en benchmarking. Medewerkers zijn pro-actief betrokken bij de verbetering van de beheersingsmaatregelen	Criteria voor niveau 4 plus de volgende onderscheidende criteria: ■ Continu evalueren van de beheersingsmaatregelen om de effectiviteit van beheersmaatregelen voortdurend te verbeteren. ■ Gebruik makend van resultaten uit self-assessments, gap en root cause analyses. ■ De getroffen beheersingsmaatregelen worden gebenchmarkt op basis van externe data en zijn 'Best Practice' in vergelijking met andere organisaties.

1.1 Information Security Plan

Good Practices

De instelling heeft een proces ingericht dat onder meer het volgende waarborgt:

- Eisen op het gebied van beschikbaarheid, integriteit en vertrouwelijkheid van informatie zijn vanuit bedrijfsdoelstellingen, bedrijfsprocessen, risk en compliance gesteld en vertaald in een informatiebeveiligingsbeleid en een daaruit volgend informatiebeveiligingsplan.
- Het informatiebeveiligingsbeleid en -plan hebben een relatie met de bedrijfsstrategie en de aard en omvang van de instelling (proportionaliteit).
- In het informatiebeveiligingsbeleid is aandacht gegeven aan de weerbaarheid van de instelling tegen cyberdreigingen.
- Het informatiebeveiligingsbeleid wordt periodiek geactualiseerd en gecommuniceerd naar in- en externe belanghebbenden.
- De uitvoering van het informatiebeveiligingsplan wordt gemonitord.
- Taken en verantwoordelijkheden op bovenstaande onderdelen zijn belegd in 1e, 2e, en 3e lijnfuncties; formele rapportagelijnen zijn ingericht.

De instelling let op de volgende punten bij uitbesteding:

Bij uitbesteding van activiteiten/systemen blijft de instelling eindverantwoordelijk voor het opstellen en naleven van het informatiebeveiligingsbeleid en -plan. De instelling heeft een proces dat ten minste het volgende waarborgt (zie ook de door DNB gepubliceerde Good Practice uitbesteding):[10]

- De instelling heeft afspraken gemaakt met de dienstverlener ten aanzien van het naleven van het informatiebeveiligingsbeleid en indien van toepassing de uitvoering van het informatiebeveiligingsplan van de instelling. Deze werken door naar eventuele onderaannemers.
- De instelling ontvangt Service Level Rapportages (SLR) en/of assurance rapportages met de juiste scope en diepgang aan de hand waarvan die afspraken kunnen worden gemonitord.
- De instelling stuurt bij wanneer haar risicotoleranties worden overschreden (zie Risk Management cycle).

Voorbeelden 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 maatregelen. 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 (IT) technische maatregelen als procedurele maatregelen in de bedrijfsprocessen.
- De instelling actualiseert het informatiebeveiligingsbeleid met een vaste periodiciteit die past bij de aard en omvang van de instelling (bijvoorbeeld tweejaarlijks) 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 het informatiebeveiligingsbeleid en kennen hun rol en verantwoordelijkheden in dat verband.

10 Zie http://www.toezicht.dnb.nl/2/50-237170.jsp

1.2 IT Policies Management

Good Practices

De instelling heeft een proces ingericht dat onder meer het volgende waarborgt:

- Maatregelen die voortkomen uit het Informatiebeveiligingsbeleid en –plan maken deel uit van gestandaardiseerde en voorspelbare (IT) werkprocessen (beheerste en integere bedrijfsvoering).
- (IT) werkprocessen en procedures zien toe op een beheerste IT-systeemontwikkeling, verwerving van veilige hard- en software uit onbetwiste bron, verwerking en opslag van gegevens, IT-systeemonderhoud en IT-support.
- Noodprocedures zijn opgesteld voor situaties waarin de standaardprocedures niet voorzien.
- Taken en verantwoordelijkheden op bovenstaande onderdelen zijn belegd in 1e, 2e, en 3e lijnfuncties; formele rapportagelijnen zijn ingericht.

De instelling let op de volgende punten bij uitbesteding:

Bij uitbesteding van activiteiten/systemen blijft de instelling eindverantwoordelijk voor de beheerste uitvoering van (IT) werkprocessen en procedures.
De instelling heeft een proces ingericht dat ten minste het volgende waarborgt (zie ook de Good Practice uitbesteding):

- De instelling heeft afspraken gemaakt met de dienstverlener ten aanzien van de beheerste uitvoering van (IT) werkprocessen en procedures conform het beleid van de instelling. Deze werken door naar eventuele onderaannemers.
- De instelling ontvangt SLR en/of assurance rapportages met de juiste scope en diepgang aan de hand waarvan die afspraken kunnen worden gemonitord.
- De instelling stuurt bij wanneer haar risicotoleranties worden overschreden (zie Risk Management cycle).

Voorbeelden hierbij zijn:

- De instelling heeft (IT) werkprocessen en procedures beschreven en/of ingericht in workflow tooling die een beheerste uitvoering van die (IT) werkprocessen en procedures waarborgen. De workflow tooling dwingt bijvoorbeeld het 4-ogen principe af bij het aanpassen van kritische IT-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 (IT) werkprocessen en procedures met een vaste periodiciteit (bijvoorbeeld tweejaarlijks) en met een hogere frequentie wanneer daartoe aanleiding bestaat, bijvoorbeeld bij fusies en overnames, uitbesteding van de (IT) werkprocessen of incidenten in de uitvoering.
  Bij nieuwe of in intensiteit toenemende vormen van cyberdreigingen, bekijkt de instelling of (IT) werkprocessen en procedures dienen te worden aangescherpt.
- De instelling stelt vast in hoeverre haar medewerkers, inhuurkrachten en dienstverleners zich houden aan de vastgestelde (IT) werkwijzen en zich ervan bewust zijn dat een beheerste uitvoering van hun werkzaamheden bijdraagt aan informatiebeveiliging en weerbaarheid tegen cyberdreigingen.

2.1 Enterprise Information Architecture Model

Good Practices

De instelling heeft een proces ingericht dat onder meer het volgende waarborgt:

- Bedrijfsprocessen en IT-systemen zijn opgezet volgens een door de instelling vastgestelde informatiearchitectuur waarin onder meer is geadresseerd:
  - Visie op de informatievoorziening;
  - Doelarchitectuur van IT-systemen en processen;
  - Cybersecurity- en privacy vereisten;
  - Systeem- en dataclassificatie;
  - Rationalisatie van huidige IT-systemen; het uitfaseren van legacy IT-systemen en IT-systemen die kwetsbaar zijn voor cyberdreigingen.
- Taken en verantwoordelijkheden op bovenstaande onderdelen zijn belegd in 1e, 2e, en 3e lijnfuncties; formele rapportagelijnen zijn ingericht.

De instelling let op de volgende punten bij uitbesteding:

Bij uitbesteding van activiteiten/systemen blijft de instelling eindverantwoordelijk voor het opstellen en bewaken van haar informatiearchitectuur. De instelling heeft een proces ingericht dat ten minste het volgende waarborgt (zie de Good Practice uitbesteding):

- De instelling heeft afspraken gemaakt met de dienstverlener ten aanzien van het navolgen van haar informatiearchitectuur. Deze werken door naar eventuele onderaannemers.
- De instelling ontvangt SLR en/of assurance rapportages met de juiste scope en diepgang aan de hand waarvan die afspraken kunnen worden gemonitord.
- De instelling stuurt bij wanneer haar risicotoleranties worden overschreden (zie Risk Management cycle).

Voorbeelden hierbij zijn:

- De instelling werkt volgens een (informatie) architectuur waarin inzichtelijk is gemaakt hoe de IT-systemen en dataverzamelingen de bedrijfsstrategie en bedrijfsprocessen ondersteunen.
- De informatiearchitectuur is gebaseerd op internationaal geaccepteerde standaarden zoals TOGAF en DYA.
- De instelling heeft een visie ontwikkeld waaruit blijkt hoe de IT-systemen en organisatiestructuur zullen evolueren om de bedrijfsstrategie op (midden)lange termijn te ondersteunen; belangrijke afhankelijkheden van derden / partners zijn daarbij in kaart gebracht.
- 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

Good Practices

De instelling heeft een proces ingericht dat onder meer het volgende waarborgt:

- Het eigenaarschap van systemen en data is door het management van de organisatie vastgesteld.
- De instelling heeft een classificatiebeleid vastgesteld.
- IT-systemen en data zijn op een basis van een risicoanalyse ingedeeld in categorieën die de mate van beschikbaarheid, integriteit en vertrouwelijkheid (BIV) aangeeft.
- De instelling maakt gebruik van een classificatie-schema, op basis waarvan relevante beveiligings-maatregelen zijn getroffen met betrekking tot toegang, versleuteling, opslag, retentie, schoning, etc.
- De instelling controleert periodiek of medewerkers het classificatiebeleid naleven.
- Taken en verantwoordelijkheden op bovenstaande onderdelen zijn belegd in 1e, 2e, en 3e lijnfuncties; formele rapportagelijnen zijn ingericht.

De instelling let op de volgende punten bij uitbesteding
Bij uitbesteding van activiteiten/systemen blijft de instelling eindverantwoordelijk voor het opstellen en naleven van het classificatiebeleid. De instelling heeft een proces ingericht dat ten minste het volgende waarborgt (zie de Good Practice uitbesteding):

- De instelling heeft afspraken gemaakt met de dienstverlener ten aanzien van het navolgen van haar classificatiebeleid. Deze werken door naar eventuele onderaannemers.
- De instelling ontvangt SLR- en/of assurance rapportages met de juiste scope en diepgang aan de hand waarvan die afspraken kunnen worden gemonitord.
- De instelling stuurt bij wanneer haar risicotoleranties worden overschreden (zie Risk Management cycle).

Voorbeelden hierbij zijn:

- De instelling heeft een dataclassificatieschema (BIV) opgesteld dat gebaseerd is op de risico's aan de hand waarvan alle IT-systemen en data worden ingedeeld in bijvoorbeeld Hoog/Midden/Laag en Publiek/Vertrouwelijk/Geheim
- Op basis van de classificatie treft de instelling maatregelen, 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-software in hoeverre gevoelige data vanuit het bedrijfsnetwerk naar buiten wordt verzonden en of dat in overeenstemming is met de dataclassificatie.

3.1 Monitor future trends and regulations

Good Practices

De instelling heeft een proces ingericht dat onder meer het volgende waarborgt:

- Ontwikkelingen in de sector worden gemonitord, onder meer op het gebied van cybersecurity.
- De instelling wordt tijdig geïnformeerd over (cyber) dreigingen (Threat Intelligence).
- De potentiële impact van deze ontwikkelingen/ dreigingen wordt gewogen, indien van toepassing worden passende maatregelen getroffen om risico's te mitigeren.
- Taken en verantwoordelijkheden op bovenstaande onderdelen zijn belegd in 1e, 2e, en 3e lijnfuncties; formele rapportagelijnen zijn ingericht.

De instelling let op de volgende punten bij uitbesteding:

Bij uitbesteding van activiteiten/systemen blijft de instelling eindverantwoordelijk voor het monitoren van relevante wet- en regelgeving, trends en ontwikkelingen. De instelling heeft een proces ingericht dat ten minste het volgende waarborgt (zie de Good Practice uitbesteding):

- De instelling heeft afspraken gemaakt met de dienstverlener ten aanzien van het monitoren van relevante wet- en regelgeving en ontwikkelingen op het gebied van cyberdreigingen en cybersecurity conform het beleid van de instelling. Deze werken door naar eventuele onderaannemers.
- De instelling ontvangt SLR en/of assurance rapportages met de juiste scope en diepgang aan de hand waarvan die afspraken kunnen worden gemonitord.
- De instelling stuurt bij wanneer haar risicotoleranties worden overschreden (zie Risk Management cycle).

Voorbeelden 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 heeft contractuele afspraken gemaakt met belangrijke uitbestedingspartners over samenwerking en informatie uitwisseling op het gebied van informatiebeveiliging en cybersecurity.

3.2 Technology standards

Good Practices

De instelling heeft een proces ingericht 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 en omvang van de instelling.
- Het werken volgens standaarden is naar medewerkers gecommuniceerd; zij zijn bekend met de voor hun werkzaamheden relevante standaarden.
- Nieuwe IT-systemen en wijzigingen in IT-systemen voldoen aan op de vastgestelde standaarden.
- De instelling gaat na dat volgens de vastgestelde standaarden wordt gewerkt.
- Taken en verantwoordelijkheden op bovenstaande onderdelen zijn belegd in 1e, 2e, en 3e lijnfuncties; formele rapportagelijnen zijn ingericht.

De instelling let op de volgende punten bij uitbesteding:

Bij uitbesteding van activiteiten/systemen blijft de instelling eindverantwoordelijk dat wordt gewerkt volgens (technische) standaarden. De instelling heeft een proces ingericht dat ten minste het volgende waarborgt (zie de Good Practice uitbesteding):

- De instelling heeft afspraken gemaakt met de dienstverlener ten aanzien van het werken volgens de (technische) standaarden conform het beleid van de instelling. Deze werken door naar eventuele onderaannemers.
- De instelling ontvangt SLR en/of assurance rapportages met de juiste scope en diepgang aan de hand waarvan die afspraken kunnen worden gemonitord.
- De instelling stuurt bij wanneer haar risicotoleranties worden overschreden (zie Risk Management cycle).

Voorbeelden hierbij zijn:

- De instelling werkt volgens internationaal geaccepteerde standaarden voor informatiebeveiliging en cybersecurity, zoals bijvoorbeeld ISO27001/2, NIST cybersecurity framework en/of SANS.
- De standaarden zijn gecommuniceerd en bekend bij intern en ingehuurd personeel, zoals IT-security officers, IT-architecten, projectmanagers, software ontwikkelaars, functioneel- en technisch beheerders, IT-riskmanagers en IT-auditors.
- De IT-security officer van de instelling beoordeelt nieuwe standaarden op het gebied van informatiebeveiliging en cybersecurity en doet voorstellen hoe deze de informatiebeveiliging en cybersecurity maatregelen van de instelling kunen versterken.
- De door de instelling geformaliseerde IT-Architectuur en standaarden zijn van toepassing verklaard op de dienstverleners van de instelling. Periodiek wordt vastgesteld dat de dienstverleners haar IT-omgeving conform deze standaarden heeft ingericht.
- De IT-infrastructuur en het IT-applicatielandschap wordt jaarlijks getoetst aan de meest actuele security baselines en marktstandaarden.

4.1 IT Risk Management framework

Good Practices

De instelling heeft een proces ingericht dat onder meer het volgende waarborgt:

- De instelling ontwikkelt en onderhoudt een IT risk management framework.
- Het IT-risk management framework sluit aan op het risk management raamwerk van de instelling.
- De instelling adresseert risico's op het gebied van informatiebeveiliging en cybersecurity in het IT-risk management raamwerk.
- De risicotoleranties ten aanzien van informatiebeveiliging en cybersecurity zijn bepaald en vastgelegd.
- Taken en verantwoordelijkheden op bovenstaande onderdelen zijn belegd in 1e, 2e, en 3e lijnfuncties; formele rapportagelijnen zijn ingericht.

De instelling let op de volgende punten bij uitbesteding:

Bij uitbesteding van activiteiten/systemen blijft de instelling ervoor verantwoordelijk dat (IT) risico's met betrekking tot de uitbestede activiteiten/systemen zijn beheerst. De instelling heeft een proces ingericht dat ten minste het volgende waarborgt (zie de Good Practice uitbesteding):

- De instelling heeft afspraken gemaakt met de dienstverlener ten aanzien van de beheersing van (IT) risico's conform het beleid en risicotoleranties van de instelling. Deze afspraken werken door naar eventuele onderaannemers.
- De instelling ontvangt SLR en/of assurance rapportages met de juiste scope en diepgang aan de hand waarvan die afspraken kunnen worden gemonitord.
- De instelling stuurt bij wanneer haar risicotoleranties worden overschreden.

Voorbeelden hierbij zijn:

- De instelling hanteert in haar IT-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 IT risk management framework gehanteerd.
- Actuele cyberdreigingen zoals malware, cryptoware, DDoS aanvallen en phishing maken deel uit van het risk management raamwerk.
- In de keten van uitbestede diensten werken partijen in overeenstemming met het IT risk management framework van de instelling.
- De instelling beoordeelt periodiek in hoeverre partijen aan wie activiteiten/systemen zijn uitbesteed, werken in overeenstemming met het IT-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 op het gebied van informatiebeveiliging en cybersecurity.

4.2 Risk assessment

Good Practices

De instelling heeft een proces ingericht dat onder meer het volgende waarborgt:

- De instelling voert periodiek IT-risicoanalyses uit op basis van kwalitatieve en kwantitatieve methoden.
- De kans en impact van inherente risico's op het gebied van informatiebeveiliging en van restrisico's worden hierbij in kaart te gebracht.
- Actuele cyberdreigingen worden meegenomen in de IT-risicoanalyses.
- 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.
- Taken en verantwoordelijkheden op bovenstaande onderdelen zijn belegd in 1e, 2e, en 3e lijnfuncties; formele rapportagelijnen zijn ingericht.

De instelling let op de volgende punten bij uitbesteding:

Bij uitbesteding van activiteiten/systemen blijft de instelling eindverantwoordelijk voor de analyse van risico's op het gebied van informatiebeveiliging en cybersecurity met betrekking tot de uitbestede activiteiten/systemen. De instelling heeft een proces ingericht dat ten minste het volgende waarborgt (zie de Good Practice uitbesteding):

- De instelling heeft afspraken gemaakt met de dienstverlener ten aanzien van het uitvoeren van risicoanalyses conform het risicoraamwerk van de instelling. Deze afspraken werken door naar eventuele onderaannemers.
- De instelling ontvangt SLR en/of assurance rapportages met de juiste scope en diepgang aan de hand waarvan die afspraken kunnen worden gemonitord.
- De instelling stuurt bij wanneer haar risicotoleranties worden overschreden (zie Risk Management cycle).

Voorbeelden hierbij zijn:

- De instelling voert jaarlijks een IT-risicoanalyse uit met alle voor de analyse relevante stakeholders binnen de instelling. Op basis hiervan worden actuele cyberdreigingen gewogen en geprioriteerd.
- De instelling brengt haar 'kroonjuwelen' in kaart, evalueert deze periodiek en relateert deze aan actuele cyberdreigingen en getroffen beheersingsmaatregelen. Daar waar nodig treft de instelling aanvullende beheersingsmaatregelen. Maatregelen die niet (meer) effectief werken worden aangepast, vervangen door andere maatregelen 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.

4.3 Maintenance and monitoring of a risk action plan

Good Practices

De instelling heeft een proces ingericht 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 rest risico's en compenserende maatregelen opgenomen.
- 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 en omvang van het restrisico's.
- Het risk action plan is actueel; opvolging van de acties wordt bewaakt.
- Taken en verantwoordelijkheden op bovenstaande onderdelen zijn belegd in 1e, 2e, en 3e lijnfuncties; formele rapportagelijnen zijn ingericht.

De instelling let op de volgende punten bij uitbesteding:

Bij uitbesteding van activiteiten/systemen blijft de instelling eindverantwoordelijk dat niet geaccepteerde restrisico's op het gebied van informatiebeveiliging en cybersecurity met betrekking tot de uitbestede activiteiten/systemen, worden gemitigeerd. De instelling heeft een proces ingericht dat ten minste het volgende waarborgt (zie de Good Practice uitbesteding):

- De instelling heeft afspraken gemaakt met de dienstverlener ten aanzien van het uitvoeren van risicoanalyses conform het risicoraamwerk van de instelling. Deze afspraken werken door naar eventuele onderaannemers.
- De instelling ontvangt SLR en/of assurance rapportages met de juiste scope en diepgang aan de hand waarvan die afspraken kunnen worden gemonitord.
- De instelling stuurt bij wanneer haar risicotoleranties worden overschreden (zie Risk Management cycle).

Voorbeelden hierbij zijn:

- De instelling heeft voor actuele cyberdreigingen expliciet gemaakt welke risico's formeel worden geaccepteerd en voor welke restrisico's aanvullende maatregelen 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 senior management.

De instelling laat het lijnmanagement jaarlijks een 'in control' statement (ICS) opstellen.

- 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.

5.1 Responsibility for risk, security and compliance

Good Practices

De instelling heeft een proces ingericht dat onder meer het volgende waarborgt:

- De eindverantwoordelijkheid voor de beheersing van informatiebeveiligingsrisico's (inclusief cybersecurity risico's) is belegd op het hoogste management niveau binnen de instelling.
- Taken en verantwoordelijkheden voor de risicobeheer- en informatiebeveiligingsfunctie zijn geformaliseerd en gedocumenteerd.
- Binnen de instelling heerst een bewustzijnscultuur met betrekking tot de verantwoordelijkheid van de medewerkers om beveiligingsprocessen en -procedures na te leven en te onderhouden.
- Taken en verantwoordelijkheden op bovenstaande onderdelen zijn belegd in 1e, 2e, en 3e lijnfuncties; formele rapportagelijnen zijn ingericht.

De instelling let op de volgende punten bij uitbesteding:

Bij uitbesteding van activiteiten/systemen ziet de instelling erop toe dat de verantwoordelijkheid voor informatiebeveiliging en cybersecurity ook bij dienstverleners in de uitbestedingsketen is belegd. De instelling heeft een proces ingericht dat ten minste het volgende waarborgt (zie de Good Practice uitbesteding):

- De instelling heeft afspraken gemaakt met de dienstverlener ten aanzien van de verantwoordelijkheid voor informatiebeveiliging en cybersecurity conform het beleid van de instelling. Deze werken door naar eventuele onderaannemers.
- De instelling ontvangt SLR en/of assurance rapportages met de juiste scope en diepgang aan de hand waarvan die afspraken kunnen worden gemonitord.
- De instelling stuurt bij wanneer haar risicotoleranties worden overschreden (zie Risk Management cycle).

Voorbeelden 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 hoogste management.
- Specifieke verantwoordelijkheden op het gebied van informatiebeveiliging en cybersecurity maatregelen zijn belegd bij een Computer Emergency Response Team (CERT) of Security Operations Center (SOC).
- De instelling gaat zowel bij het aangaan van kritische uitbestedingsrelaties als bij het monitoren van die relaties na dat bovenstaande punten van toepassing zijn bij haar ketenpartners.

5.2 Management of information security

Good Practices

De instelling heeft een proces ingericht dat onder meer het volgende waarborgt:

- De instelling heeft een Plan-do-check-act cyclus voor de beheersing van de risico's t.a.v. informatiebeveiliging en cybersecurity ingericht.
- De uitvoering van de cyclus vindt risico gebaseerd plaats en is afgestemd op de doelstellingen van de instelling en in overeenstemming met de risicotolerantie van de instelling.
- Zowel de 1e, 2e en 3e lijn zijn actief betrokken bij de totstandkoming en het onderhoud van Plan-do-check-act cyclus voor de beheersing van informatiebeveiliging en cybersecurity; formele rapportagelijnen zijn ingericht.

De instelling let op de volgende punten bij uitbesteding:

Bij uitbesteding van activiteiten/systemen blijft de instelling eindverantwoordelijk voor de uitvoering van een plan-do-check-act cyclus voor de beheersing van informatiebeveiliging en cybersecurity. De instelling heeft een proces ingericht dat ten minste het volgende waarborgt (zie de Good Practice uitbesteding):

- De instelling heeft afspraken gemaakt met de dienstverlener ten aanzien van de rol van de dienstverlener in de Plan-do-check-act cyclus conform het beleid van de instelling. Deze werken door naar eventuele onderaannemers.
- De instelling ontvangt SLR en/of assurance rapportages met de juiste scope en diepgang aan de hand waarvan die afspraken kunnen worden gemonitord.
- De instelling stuurt bij wanneer haar risicotoleranties worden overschreden (zie Risk Management cycle).

Voorbeelden hierbij zijn:

- 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 lijn, 2e als 3e lijn. Dit komt tot uitdrukking in organisatieschema's en functiebeschrijvingen.
- De instelling voert regelmatig overleg met haar dienstverleners over de beheersing van risico's op het gebied van informatiebeveiliging en cybersecurity. Hierin wordt nagegaan op welke punten in de keten verbeteringen noodzakelijk zijn (PDCA cyclus).
- 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 verantwoording afgelegd aan het bestuur/directie van de instelling.

6.1 Data and system ownership

Good Practices

De instelling heeft een proces ingericht 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. Beheersingsmaatregelen zijn in overeenstemming met deze classificatie bepaald. Zie beheersings-maatregel 2.2.
- Taken en verantwoordelijkheden op bovenstaande onderdelen zijn belegd in 1e, 2e, en 3e lijnfuncties; formele rapportagelijnen zijn ingericht.

De instelling let op de volgende punten bij uitbesteding:

Bij uitbesteding van activiteiten/systemen blijft de instelling eindverantwoordelijk dat het eigenschap van gegevens en informatiesystemen is belegd. De instelling heeft een proces ingericht dat ten minste het volgende waarborgt (zie de Good Practice uitbesteding):

- De instelling heeft afspraken gemaakt met de dienstverlener ten aanzien van eigenaarschap van gegevens en informatiesystemen conform het beleid van de instelling. Deze werken door naar eventuele onderaannemers.
- De instelling ontvangt SLR en/of assurance rapportages met de juiste scope en diepgang aan de hand waarvan die afspraken kunnen worden gemonitord.
- De instelling stuurt bij wanneer haar risicotoleranties worden overschreden (zie Risk Management cycle).

Voorbeelden hierbij zijn:

- De instelling heef 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 informatiesystemen, gegevens en de daarvoor verantwoordelijke eigenaren.
- De instelling heeft voor uitbestede IT-systemen en clouddiensten 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.

7.1 Segregation of duties

Good Practices

De instelling heeft een proces ingericht dat onder meer het volgende waarborgt:

- 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.
- Taken en verantwoordelijkheden op bovenstaande onderdelen zijn belegd in 1e, 2e, en 3e lijnfuncties; formele rapportagelijnen zijn ingericht.

De instelling let op de volgende punten bij uitbesteding

Bij uitbesteding van activiteiten/systemen blijft de instelling eindverantwoordelijk. De instelling heeft een proces ingericht dat ten minste het volgende waarborgt (zie de Good Practice uitbesteding):

- De instelling heeft afspraken gemaakt met de dienstverlener ten aanzien van functiescheidingen. Deze werken door naar eventuele onderaannemers.
- De instelling ontvangt SLR en/of assurance rapportages met de juiste scope en diepgang aan de hand waarvan die afspraken kunnen worden gemonitord.
- De instelling stuurt bij wanneer haar risico-toleranties worden overschreden (zie Risk Management cycle).

Voorbeelden 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 IT-systemen (ist) zijn afgedwongen (soll-ist vergelijking).
- De implementatie van functiescheidingen in IT-systemen wordt periodiek beoordeeld. Nadat majeure wijzigingen in IT-systemen zijn aangebracht vindt een tussentijdse beoordeling plaats.
- De instelling heeft op basis van een risico gebaseerde 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 proces-niveau 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

Good Practices

De instelling heeft een proces ingericht dat onder meer het volgende waarborgt:

- De instelling trekt medewerkers aan met 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.
- Taken en verantwoordelijkheden op bovenstaande onderdelen zijn belegd in 1e, 2e, en 3e lijnfuncties; formele rapportagelijnen zijn ingericht.

De instelling let op de volgende punten bij uitbesteding:

Bij uitbesteding van activiteiten/systemen blijft de instelling ervoor verantwoordelijk dat de werkzaamheden worden uitgevoerd door voldoende deskundig personeel. De instelling heeft een proces ingericht dat ten minste het volgende waarborgt (zie de Good Practice uitbesteding):

- De instelling heeft afspraken gemaakt met de dienstverlener ten aanzien van het waarborgen dat voldoende mensen met kennis van informatie-beveiliging en cybersecurity in de context van de instelling beschikbaar zijn. Deze werken door naar eventuele onderaannemers.
- De instelling heeft bepaald welke kennis 'in huis' noodzakelijk is om uitbestede activiteiten te kunnen beoordelen en te sturen.
- De instelling ontvangt SLR- en/of assurance rapportages met de juiste scope en diepgang aan de hand waarvan die afspraken kunnen worden gemonitord.
- De instelling stuurt bij wanneer haar risicotoleranties worden overschreden (zie Risk Management cycle).

Voorbeelden 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.

8.2 Personnel competencies

Good Practices

De instelling heeft een proces ingericht dat onder meer het volgende waarborgt:

- Kennis en competenties van medewerkers en beleidsbepalers op het gebied van informatiebeveiliging en cybersecurity sluiten aan bij de (digitale) ambities van de instelling.
- Periodiek wordt nagegaan 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.
- Taken en verantwoordelijkheden op bovenstaande onderdelen zijn belegd in 1e, 2e, en 3e lijnfuncties; formele rapportagelijnen zijn ingericht.

De instelling let op de volgende punten bij uitbesteding:

Bij uitbesteding van activiteiten/systemen blijft de instelling eindverantwoordelijk dat de werkzaamheden worden uitgevoerd door voldoende deskundig personeel. De instelling heeft een proces ingericht dat ten minste het volgende waarborgt (zie de Good Practice uitbesteding):

- De instelling heeft afspraken gemaakt met de dienstverlener ten aanzien van de uitvoering van de werkzaamheden door ter zake deskundig personeel conform het beleid van de instelling. Deze werken door naar eventuele onderaannemers.
- De instelling ontvangt SLR en/of assurance rapportages met de juiste scope en diepgang aan de hand waarvan die afspraken kunnen worden gemonitord.
- De instelling stuurt bij wanneer haar risico-toleranties worden overschreden (zie Risk Management cycle).

Voorbeelden 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 IT-risico's en beheersingsmaatregelen voor hun instelling te kunnen begrijpen.
- In functiebeschrijvingen is opgenomen welke kennis en competenties van medewerkers ten aanzien van informatiebeveiliging 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.

8.3 Dependence upon individuals

Good Practices

De instelling heeft een proces ingericht dat onder meer het volgende waarborgt:

- De instelling heeft geïnventariseerd op welke voor de uitoefening van haar bedrijf kritische processen/ activiteiten zij afhankelijk is van een beperkt aantal medewerkers.
- Op grond van een risicoanalyse heeft de instelling bepaald waar de afhankelijkheid van individuen haar risicotolerantie overschrijdt.
- De instelling heeft maatregelen getroffen te grote afhankelijkheid van individuen te beperken binnen haar risicotolerantiegrenzen.
- Taken en verantwoordelijkheden op bovenstaande onderdelen zijn belegd in 1e, 2e, en 3e lijnfuncties; formele rapportagelijnen zijn ingericht.

De instelling let op de volgende punten bij uitbesteding:

Bij uitbesteding van activiteiten/systemen blijft de instelling eindverantwoordelijk voor de continuïteit van de werkzaamheden. De instelling heeft een proces ingericht dat ten minste het volgende waarborgt (zie de Good Practice uitbesteding):

- De instelling heeft afspraken gemaakt met de dienstverlener ten aanzien van het identificeren en reduceren van de afhankelijkheid van enkele individuen (key person risk) conform het beleid van de instelling. Deze werken door naar eventuele onderaannemers.
- De instelling ontvangt SLR en/of assurance rapportages met de juiste scope en diepgang aan de hand waarvan die afspraken kunnen worden gemonitord.
- De instelling stuurt bij wanneer haar risicotoleranties worden overschreden (zie Risk Management cycle).

Voorbeelden 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 kritische functies binnen de instelling.

8.4 Personnel clearance procedures

Good Practices

De instelling heeft een proces ingericht dat onder meer het volgende waarborgt:

- Voorafgaand aan de indiensttreding wordt personeel gescreend afhankelijk van het risicoprofiel van de functie.
- Tijdens het dienstverband wordt de screening periodiek herhaald.
- Bovenstaand is van toepassing op zowel eigen medewerkers als op ingehuurde medewerkers.
- Taken en verantwoordelijkheden op bovenstaande onderdelen zijn belegd in 1e, 2e, en 3e lijnfuncties; formele rapportagelijnen zijn ingericht.

De instelling let op de volgende punten bij uitbesteding:

Bij uitbesteding van activiteiten/systemen blijft de instelling eindverantwoordelijk dat werkzaamheden door betrouwbare en integere medewerkers worden uitgevoerd. De instelling heeft een proces ingericht dat ten minste het volgende waarborgt (zie de Good Practice uitbesteding):

- De instelling heeft afspraken gemaakt met de dienstverlener ten aanzien van het screenen van medewerkers conform het beleid van de instelling. Deze werken door naar eventuele onderaannemers.
- De instelling ontvangt SLR en/of assurance rapportages met de juiste scope en diepgang aan de hand waarvan die afspraken kunnen worden gemonitord.
- De instelling stuurt bij wanneer haar risicotoleranties worden overschreden (zie Risk Management cycle).

Voorbeelden 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 vraagt een verklaring omtrent gedrag (VOG) op voor functies met een gemiddeld of hoog risicoprofiel en trekt referenties na.
- Risico gebaseerd wordt periodiek een in-employment screening uitgevoerd voor gemiddeld en hoog risico functies.

8.5 Job change and termination

Good Practices

De instelling heeft een proces ingericht dat onder meer het volgende waarborgt:

- Bij functiewijzigingen worden rechten in IT-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.
- Bij uitdiensttreding worden rechten in systemen en processen per direct ingetrokken. 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.
- Taken en verantwoordelijkheden op bovenstaande onderdelen zijn belegd in 1e, 2e, en 3e lijnfuncties; formele rapportagelijnen zijn ingericht.

De instelling let op de volgende punten bij uitbesteding:

Bij uitbesteding van activiteiten/systemen blijft de instelling eindverantwoordelijk voor het tijdig intrekken van toegangsrechten in IT-systemen bij functiewijziging en bij uitdiensttreding van medewerkers. De instelling heeft een proces ingericht dat ten minste het volgende waarborgt (zie de Good Practice uitbesteding):

- De instelling heeft afspraken gemaakt met de dienstverlener ten aanzien van het tijdig intrekken van toegangsrechten conform het beleid van de instelling. Deze werken door naar eventuele onderaannemers.
- De instelling ontvangt SLR en/of assurance rapportages met de juiste scope en diepgang aan de hand waarvan die afspraken kunnen worden gemonitord.
- De instelling stuurt bij wanneer haar risicotoleranties worden overschreden (zie Risk Management cycle).

Voorbeelden hierbij zijn:

- De instelling maakt gebruik van User Provisioning, waarbij toegangsrechten in IT-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 beheersingsmaatregelen 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

Good Practices

De instelling heeft een proces ingericht dat onder meer het volgende waarborgt:

- Medewerkers beschikken over de kennis en vaardigheden om correct gebruik te maken van IT-applicaties en IT-systemen in overeenstemming met procedures en werkinstructies van de instelling.
- Medewerkers weten hoe informatietechnologie hun kritische 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.
- Taken en verantwoordelijkheden op bovenstaande onderdelen zijn belegd in 1e, 2e, en 3e lijnfuncties; formele rapportagelijnen zijn ingericht.

De instelling let op de volgende punten bij uitbesteding:

Bij uitbesteding van activiteiten/systemen blijft de instelling eindverantwoordelijk voor kennisdeling in de gehele keten van uitbesteding. De instelling heeft een proces ingericht dat ten minste het volgende waarborgt (zie de Good Practice uitbesteding):

- De instelling heeft afspraken gemaakt met de dienstverlener ten aanzien van kennisdeling conform het beleid van de instelling. Deze werken door naar eventuele onderaannemers.
- De instelling ontvangt SLR en/of assurance rapportages met de juiste scope en diepgang aan de hand waarvan die afspraken kunnen worden gemonitord.
- De instelling stuurt bij wanneer haar risico-toleranties worden overschreden (zie Risk Management cycle).

Voorbeelden hierbij zijn:

- Medewerkers ontvangen periodiek functionele trainingen over het correct gebruik van IT-applicaties en IT-infrastructuur, waarbij tevens aandacht wordt geschonken aan informatiebeveiligings- en cybersecurity aspecten.
- Werkinstructies voor het correct gebruik van IT-applicaties en IT-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

Good Practices

De instelling heeft een proces ingericht dat onder meer het volgende waarborgt:

- IT-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.
- IT-medewerkers weten hoe informatietechnologie hun kritische bedrijfsprocessen ondersteunt en kennen de met die technologie verband houdende risico's ten aanzien van informatiebeveiliging en cybersecurity. IT-medewerkers passen die kennis toe in hun dagelijkse operationele werkzaamheden.
- IT-medewerkers zetten hun specialistische kennis actief in om informatiebeveiligingsrisico's en cyberdreigingen te herkennen en met passende maatregelen te beheersen.
- Taken en verantwoordelijkheden op bovenstaande onderdelen zijn belegd in 1e, 2e, en 3e lijnfuncties; formele rapportagelijnen zijn ingericht.

De instelling let op de volgende punten bij uitbesteding:

Bij uitbesteding van activiteiten/systemen blijft de instelling eindverantwoordelijk dat IT-specialisten in de gehele keten van uitbesteding voldoende kennis hebben van informatiebeveiliging en cybersecurity. De instelling heeft een proces ingericht dat ten minste het volgende waarborgt (zie de Good Practice uitbesteding):

- De instelling heeft afspraken gemaakt met de dienstverlener ten aanzien van het borgen van specialistische kennis van informatiebeveiliging en cybersecurity conform het beleid van de instelling. Deze werken door naar eventuele onderaannemers.
- De instelling ontvangt SLR en/of assurance rapportages met de juiste scope en diepgang aan de hand waarvan die afspraken kunnen worden gemonitord.
- De instelling stuurt bij wanneer haar risicotoleranties worden overschreden (zie Risk Management cycle).

Voorbeelden hierbij zijn:

- Gerichte security trainingen voor specifieke doelgroepen, zoals IT-systeemontwikkelaars, helpdeskmedewerkers, IT-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

Good Practices

De instelling heeft een proces ingericht dat onder meer het volgende waarborgt:

- 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 programma is geïmplementeerd. Hierin wordt expliciet aandacht besteed aan cybersecurity risico's.
- Basiskennis van informatiebeveiliging en cyberdreigingen wordt breed binnen de instelling en het bestuur gedeeld.
- Management en medewerkers weten hoe te handelen wanneer zij vermoeden of signaleren dat risico's op het gebied van informatiebeveiliging en cybersecurity zich voordoen.
- Taken en verantwoordelijkheden op bovenstaande onderdelen zijn belegd in 1e, 2e, en 3e lijnfuncties; formele rapportagelijnen zijn ingericht.

De instelling let op de volgende punten bij uitbesteding:

Bij uitbesteding van activiteiten/systemen blijft de instelling eindverantwoordelijk voor *security awareness* in de gehele keten van uitbesteding. De instelling heeft een proces ingericht dat ten minste het volgende waarborgt (zie de Good Practice uitbesteding):

- De instelling heeft afspraken gemaakt met de dienstverlener ten aanzien van security awareness van management en personeel conform het beleid van de instelling. Deze werken door naar eventuele onderaannemers.
- De instelling ontvangt SLR en/of assurance rapportages met de juiste scope en diepgang aan de hand waarvan die afspraken kunnen worden gemonitord.
- De instelling stuurt bij wanneer haar risico-toleranties worden overschreden (zie Risk Management cycle).

Voorbeelden 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 informatiebeveiligingsbeleid 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.
- De instelling onderneemt initiatieven om samen met uitbestedingspartners bewustwording op het gebied van cybersecurity te vergroten.
- De instelling participeert in gremia waarin cybersecurity dreigingen en aanvallen vertrouwelijk worden gedeeld (zoals de sectorale ISAC's).
- De instelling onderhoudt nauwe contacten met overheidsinstanties, die zich richten op cybersecurity zoals het NCSC of het Digital Trust Center.

10.1 Change standards and procedures

Good Practices

De instelling heeft een proces ingericht dat onder meer het volgende waarborgt:

- Wijzigingen in IT-applicaties, IT-infrastructuur, IT-processen en kritische systeeminstellingen volgen een gestandaardiseerd en gecontroleerd pad.
- Taken en verantwoordelijkheden met betrekking tot het controleren en goedkeuren van wijzigings-verzoeken zijn belegd.
- Wijzigingen (inclusief security patches) worden geprioriteerd.
- De impact en risico's van wijzigingen op informatie-beveiliging en cybersecurity worden ingeschat voordat de wijziging wordt geïmplementeerd.
- Security experts zijn betrokken bij wijzigingen die de informatiebeveiligingsmaatregelen raken.
- Wijzigingen in kritische systemen en infrastructuur worden niet door één en dezelfde persoon aangevraagd, goedgekeurd en geïmplementeerd (functiescheiding).
- Wijzigingen worden geregistreerd (audit trail) en geëvalueerd.
- Taken en verantwoordelijkheden op bovenstaande onderdelen zijn belegd in 1e, 2e, en 3e lijnfuncties; formele rapportagelijnen zijn ingericht.

De instelling let op de volgende punten bij uitbesteding:

Bij uitbesteding van activiteiten/systemen blijft de instelling eindverantwoordelijk voor het proces change management. De instelling heeft een proces ingericht dat ten minste het volgende waarborgt (zie de Good Practice uitbesteding):

- De instelling heeft afspraken gemaakt met de dienstverlener ten aanzien van change standaarden en procedures conform het beleid van de instelling. Deze werken door naar eventuele onderaannemers.
- De instelling ontvangt SLR en/of assurance rapportages met de juiste scope en diepgang aan de hand waarvan die afspraken kunnen worden gemonitord.
- De instelling stuurt bij wanneer haar risico-toleranties worden overschreden (zie Risk Management cycle).

Voorbeelden hierbij zijn:

- Het changemanagementproces is gebaseerd op internationale standaarden en werkwijzen, zoals ITIL, Agile, Scrum.
- De instelling gebruikt een workflow systeem dat het gehele proces van wijzigingsverzoek tot en met implementatie ondersteunt, inclusief logging en documentatie.
- 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 door verschillende disciplines zoals business, IT en IT-Risk/IT Security wordt besloten over wijzigingen.

10.2 Impact assessment, prioritisation and authorisation

Good Practices

De instelling heeft een proces ingericht dat onder meer het volgende waarborgt:

- De impact van wijzigingsverzoeken op operationele IT-systemen wordt beoordeeld.
- In deze beoordeling worden de gevolgen voor informatiebeveiliging en cybersecurity meegenomen en meegewogen in de besluitvorming over het wijzigingsverzoek.
- Taken en verantwoordelijkheden op bovenstaande onderdelen zijn belegd in 1e, 2e, en 3e lijnfuncties; formele rapportagelijnen zijn ingericht.

De instelling let op de volgende punten bij uitbesteding:

Bij uitbesteding van activiteiten/systemen blijft de instelling eindverantwoordelijk voor het proces change management. De instelling heeft een proces ingericht dat ten minste het volgende waarborgt (zie de Good Practice uitbesteding):

- De instelling heeft afspraken gemaakt met de dienstverlener ten aanzien van impact assessment, prioritering en autorisatie van wijzigingen conform het beleid van de instelling. Deze werken door naar eventuele onderaannemers.
- De instelling ontvangt SLR en/of assurance rapportages met de juiste scope en diepgang aan de hand waarvan die afspraken kunnen worden gemonitord.
- De instelling stuurt bij wanneer haar risicotoleranties worden overschreden (zie Risk Management cycle).

Voorbeelden hierbij zijn:

- De informatiebeveiligingsrol binnen de instelling is betrokken bij de beoordeling van de impact van wijzigingsverzoeken op de maatregelen die in het kader van informatiebeveiliging en cybersecurity zijn getroffen.
- Bij het bepalen van de impact en prioriteit van wijzigingsverzoeken worden informatiebeveiligings-aspecten van de wijzigingen expliciet meegewogen.

10.3 Test environment

Good Practices

De instelling heeft een proces ingericht dat onder meer het volgende waarborgt:

- Criteria voor het beschermen van testgegevens zijn opgesteld en worden onderhouden.
- Toegang tot test- en productie IT-systemen is strikt gescheiden; test- en productiegegevens worden niet vermengd.
- De instelling heeft een omgeving beschikbaar waarin zij de effectiviteit van security maatregelen test.
- Taken en verantwoordelijkheden op bovenstaande onderdelen zijn belegd in 1e, 2e, en 3e lijnfuncties; formele rapportagelijnen zijn ingericht.

De instelling let op de volgende punten bij uitbesteding:

Bij uitbesteding van activiteiten/systemen blijft de instelling eindverantwoordelijk voor het proces change management. De instelling heeft een proces ingericht dat ten minste het volgende waarborgt (zie de Good Practice uitbesteding):

- De instelling heeft afspraken gemaakt met de dienstverlener ten aanzien van de test omgeving conform het beleid van de instelling. Deze werken door naar eventuele onderaannemers.
- De instelling ontvangt SLR en/of assurance rapportages met de juiste scope en diepgang aan de hand waarvan die afspraken kunnen worden gemonitord.
- De instelling stuurt bij wanneer haar risico-toleranties worden overschreden (zie Risk Management cycle).

Voorbeelden hierbij zijn:

- 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 (het OTAP model wordt gehanteerd).
- 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

Good Practices

De instelling heeft een proces ingericht dat onder meer het volgende waarborgt:

- Wijzigingen in de IT-infrastructuur n IT-applicaties worden getest voordat zij in gebruik (productie) worden genomen.
- De tests worden uitgevoerd volgens een testplan waarin ook acceptatiecriteria voor informatiebeveiliging en IT-performance zijn opgenomen.
- Op grond van een risico inschatting worden gewijzigde IT-systemen gescand op kwetsbaarheden voor cyberdreigingen.
- Taken en verantwoordelijkheden op bovenstaande onderdelen zijn belegd in 1e, 2e, en 3e lijnfuncties; formele rapportagelijnen zijn ingericht.

De instelling let op de volgende punten bij uitbesteding:

Bij uitbesteding van activiteiten/systemen blijft de instelling eindverantwoordelijk voor het proces change management. De instelling heeft een proces ingericht dat ten minste het volgende waarborgt (zie de Good Practice uitbesteding):

- De instelling heeft afspraken gemaakt met de dienstverlener ten aanzien van het testen van wijzigingen conform het beleid van de instelling. Deze werken door naar eventuele onderaannemers.
- De instelling ontvangt SLR en/of assurance rapportages met de juiste scope en diepgang aan de hand waarvan die afspraken kunnen worden gemonitord.
- De instelling stuurt bij wanneer haar risicotoleranties worden overschreden (zie Risk Management cycle).

Voorbeelden hierbij zijn:

- De instelling voert verschillende tests uit (zoals een systeemtest, gebruikers acceptatietest, regressietest en integratietest). De effectiviteit van beveiligingsmaatregelen in gewijzigde applicaties en infrastructuur vast te stellen. Bij een agile werkwijze wordt software getest op grond van acceptatiecriteria (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, kritische handelingen worden gelogd en de systeemperformance voldoet aan de gestelde eisen.
- Bij het testen van wijzigingen worden maatregelen van informatiebeveiliging en cybersecurity expliciet meegenomen, bijvoorbeeld door middel van security & vulnerability scanning en source code reviews.
- In geval van uitbesteding van IT-applicaties stelt de instelling risicogebaseerd vast dat de belangrijkste functionaliteit en beveiligingsmaatregelen werken conform specificaties.

10.5 Promotion to production

Good Practices

De instelling heeft een proces ingericht dat onder meer het volgende waarborgt:

- Beheerste overdracht van wijzigingen in productie systemen vindt plaats.
- De belangrijkste belanghebbenden bij systeem-wijzigingen, zoals gebruikers, systeemeigenaar, functioneel en technisch beheerders zijn betrokken bij het goedkeuringsproces.
- Op grond van een risicoanalyse bepaalt de instelling of een nieuw of aangepast IT-systeem parallel naast het oude systeem gebruikt wordt. Bij risicovolle aanpassingen heeft de instelling voorzien in een fall-back plan.
- Taken en verantwoordelijkheden op bovenstaande onderdelen zijn belegd in 1e, 2e, en 3e lijnfuncties; formele rapportagelijnen zijn ingericht.

De instelling let op de volgende punten bij uitbesteding

Bij uitbesteding van activiteiten/systemen blijft de instelling eindverantwoordelijk voor het proces change management.

De instelling heeft een proces ingericht dat ten minste het volgende waarborgt (zie de Good Practice uitbesteding):

- De instelling heeft afspraken gemaakt met de dienstverlener ten aanzien van gecontroleerde overdracht naar productie omgeving, conform het beleid van de instelling. Deze afspraken werken door naar eventuele onderaannemers.
- De instelling ontvangt SLR en/of assurance rapportages met de juiste scope en diepgang aan de hand waarvan die afspraken kunnen worden gemonitord.
- De instelling stuurt bij wanneer haar risicotoleranties worden overschreden (zie Risk Management cycle).

Voorbeelden hierbij zijn:

- Voor het in gebruik nemen wijzigingen in de IT-infrastructuur en IT-applicaties zijn overdrachtsprocedures vastgesteld.
- De instelling gebruikt een workflow systeem ten behoeve van de gecontroleerde overdracht en registratie van wijzigingen in de productie omgeving.
- Wijzigingen in kritische systemen en wijziging van beveiligingsparameters vinden plaats onder het 4-ogen principe.
- Alle wijzigingen in de productieomgeving worden gelogd. Op basis hiervan wordt periodiek nagegaan dat geen ongeautoriseerde wijzigen hebben plaatsgevonden.

11.1 IT Continuity plans

Good Practices

De instelling heeft een proces ingericht dat onder meer het volgende waarborgt:

- De instelling heeft een continuïteitsplan uitgewerkt om de impact van een grote verstoring op de belangrijkste bedrijfsfuncties en -processen te beperken.
- Alternatieve verwerkings- en herstelmogelijkheden voor alle kritieke IT-services zijn voorhanden.
- In het IT-continuïteitsplan is rekening gehouden met de continuïteit van cybersecurity maatregelen en de ongestoorde voortzetting van informatiebeveiligingsfuncties tijdens verstoringen en cyberaanvallen.
- Het IT-continuïteitsplan adresseert de weerbaarheid tegen DDoS aanvallen.
- Crisismanagement is ingericht, inclusief de daarbij behorende communicatieprotocollen.
- Taken en verantwoordelijkheden op bovenstaande onderdelen zijn belegd in 1e, 2e, en 3e lijnfuncties; formele rapportagelijnen zijn ingericht.

De instelling let op de volgende punten bij uitbesteding:

Bij uitbesteding van activiteiten/systemen blijft de instelling eindverantwoordelijk voor de continuïteit bedrijfsvoering. De instelling heeft een proces ingericht dat ten minste het volgende waarborgt (zie de Good Practice uitbesteding):

- De instelling heeft afspraken gemaakt met de dienstverleners ten aanzien van de continuïteit van IT-systemen en daarbij behorende dienstverlening conform het beleid van de instelling. Deze werken door naar eventuele onderaannemers.
- De instelling ontvangt SLR en/of assurance rapportages met de juiste scope en diepgang aan de hand waarvan die afspraken kunnen worden gemonitord.
- De instelling stuurt bij wanneer haar risicotoleranties worden overschreden (zie Risk Management cycle).

Voorbeelden hierbij zijn:

- Belangrijke wijzigingen in IT systemen of dienstverlening worden direct in het continuïteitsplan verwerkt.
- De instelling controleert daarnaast jaarlijks of het continuïteitsplan toereikend is.
- De instelling test periodiek of het IT-continuïteits-plan werkt. De uitkomsten van de testen worden verwerkt en vervolgacties worden genomen.
- Bij het implementeren van een nieuw systeem of applicatie neemt de instelling deze op in een vernieuwde versie van het IT-continuïteitsplan en bijbehorende testcyclus.

11.2 Testing of the IT Continuity plan

Good Practices

De instelling heeft een proces ingericht dat onder meer het volgende waarborgt:

- Het IT-continuïteitsplan wordt periodiek getest om ervoor te zorgen dat IT-systemen effectief kunnen worden hersteld, tekortkomingen worden opgelost en het plan relevant blijft.
- De weerbaarheid tegen (D)DoS aanvallen en andere cyberaanvallen met een impact op de beschikbarheid wordt getest.
- Het testen van de continuïteitsmaatregelen dekt de gehele keten van systemen en applicaties af die de kritische bedrijfsprocessen ondersteunen.
- Taken en verantwoordelijkheden op bovenstaande onderdelen zijn belegd in 1e, 2e, en 3e lijnfuncties; formele rapportagelijnen zijn ingericht.

De instelling let op de volgende punten bij uitbesteding:

Bij uitbesteding van activiteiten/systemen blijft de instelling eindverantwoordelijk dat continuïteits-maatregelen worden getest. De instelling heeft een proces ingericht dat ten minste het volgende waarborgt (zie de Good Practice uitbesteding):

- De instelling heeft afspraken gemaakt met de dienstverleners ten aanzien van het testen van continuïteitsmaatregelen van IT-systemen en daarbij behorende dienstverlening conform het beleid van de instelling. Deze werken door naar eventuele onderaannemers.
- De instelling ontvangt SLR en/of assurance rapportages met de juiste scope en diepgang aan de hand waarvan die afspraken kunnen worden gemonitord.
- De instelling stuurt bij wanneer haar risicotoleranties worden overschreden (zie Risk Management cycle).

Voorbeelden hierbij zijn:

- De instelling bereidt het testen van het IT-continuïteitsplan zorgvuldig voor en rapporteert over de testresultaten, zorgt voor opvolging van actiepunten en voert kort na de eerste test een hertest uit om vast te stellen dat de actiepunten tot het gewenste resultaat leiden.
- 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 IT-continuïteitsplan en bijbehorende testcyclus.
- In haar testscenario's neemt de instelling expliciet cybersecurity dreigingen zoals (D)DoS en Advanced Persistent Threats (APT's) op.

11.3 Offsite backup storage

Good Practices

De instelling heeft een proces ingericht 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.
- Het risicoprofiel van de locaties moet zodanig zijn dat een calamiteit niet de locaties tegelijkertijd kan treffen.
- De inhoud van de back-up wordt door de eigenaars van de bedrijfsprocessen en het IT-personeel bepaald.
- De instelling beoordeelt periodiek in hoeverre de backup data volledig en juist is.
- Het beheer van de data op de verschillende locaties (backup / 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 te testen en te vernieuwen is verzekerd.
- Taken en verantwoordelijkheden op bovenstaande onderdelen zijn belegd in 1e, 2e, en 3e lijnfuncties; formele rapportagelijnen zijn ingericht.

De instelling let op de volgende punten bij uitbesteding:

Bij uitbesteding van activiteiten/systemen blijft de instelling eindverantwoordelijk dat backups op een externe locatie wordt bewaard. De instelling heeft een proces ingericht dat ten minste het volgende waarborgt (zie de Good Practice uitbesteding):

- De instelling heeft afspraken gemaakt met de dienstverleners ten aanzien van het bewaren van backups op een externe opslagfaciliteit conform het beleid van de instelling. Deze afspraken werken door naar eventuele onderaannemers.
- De instelling ontvangt SLR en/of assurance rapportages met de juiste scope en diepgang aan de hand waarvan die afspraken kunnen worden gemonitord.
- De instelling stuurt bij wanneer haar risicotoleranties worden overschreden (zie Risk Management cycle).

Voorbeelden hierbij zijn:

- De instelling heeft op grond van een risicoanalyse bepaald op welke externe locatie de backups worden bewaard.
- De instelling gaat periodiek na of de off-site backup bruikbaar is door deze terug te zetten in een testomgeving. Eindgebruikers zijn hierbij nauw betrokken.
- De instelling heeft afspraken gemaakt met haar dienstverleners over Recovery Point Objectives (RPO's) en Recovery Time Objectives (RTO's) en het testen daarvan.

11.4 Backup and restoration

Good Practices

De instelling heeft een proces ingericht dat onder meer het volgende waarborgt:

- De instelling heeft procedures opgesteld en geïmplementeerd voor back-up en herstel van IT-systemen, IT-applicaties, gegevens en documentatie.
- De instelling heeft maatregelen getroffen om cyberdreigingen die gericht zijn op het beschadigen van backups te voorkomen, te detecteren en te mitigeren.
- Taken en verantwoordelijkheden op bovenstaande onderdelen zijn belegd in 1e, 2e, en 3e lijnfuncties; formele rapportagelijnen zijn ingericht.

De instelling let op de volgende punten bij uitbesteding:

Bij uitbesteding van activiteiten/systemen blijft de instelling eindverantwoordelijk dat backups worden gemaakt en teruggezet kunnen worden. De instelling heeft een proces ingericht dat ten minste het volgende waarborgt (zie de Good Practice uitbesteding):

- De instelling heeft afspraken gemaakt met de dienstverleners ten aanzien van het maken en terugzetten van backups conform het beleid van de instelling. Deze werken door naar eventuele onderaannemers.
- De instelling ontvangt SLR en/of assurance rapportages met de juiste scope en diepgang aan de hand waarvan die afspraken kunnen worden gemonitord.
- De instelling stuurt bij wanneer haar risico-toleranties worden overschreden (zie Risk Management cycle).

Voorbeelden hierbij zijn:

- Na een storing of majeure systeemuitval kan de instelling met behulp van backups of “snapshots” haar data en IT-systemen binnen de gestelde tijdslimiet herstellen zodat haar kritische bedrijfs-processen 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* van haar kritische processen bepaald en vastgesteld op basis van realistische tests dat herstelwerkzaamheden (bijvoorbeeld: het terugzetten van backups) binnen deze maximale downtime haalbaar is.
- De instelling heeft een recovery scenario opgesteld voor het geval zich cybersecurity incidenten voordoen.
- De instelling heeft diverse maatregelen getroffen om de toegang tot backups te bewaken en te monitoren: offline backup, netwerkzonering, detectie van afwijkende backup/restore activiteiten.

12.1 Storage and retention arrangements

Good Practices

De instelling heeft een proces ingericht 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.
- Bij de opslag van data wordt rekening gehouden met de wettelijke vereisten ten aanzien van bewaartermijnen.
- Taken en verantwoordelijkheden op bovenstaande onderdelen zijn belegd in 1e, 2e, en 3e lijnfuncties; formele rapportagelijnen zijn ingericht.

De instelling let op de volgende punten bij uitbesteding:

Bij uitbesteding van activiteiten/systemen blijft de instelling eindverantwoordelijk dat dataopslag voldoet aan de wettelijke vereisten en in lijn is met de bedrijfsdoelstellingen. De instelling heeft een proces ingericht dat ten minste het volgende waarborgt (zie de Good Practice uitbesteding):

- 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 ontvangt SLR en/of assurance rapportages met de juiste scope en diepgang aan de hand waarvan die afspraken kunnen worden gemonitord.
- De instelling stuurt bij wanneer haar risicotoleranties worden overschreden (zie Risk Management cycle).

Voorbeelden hierbij zijn:

- De instelling houdt een vervalkalender bij van opgeslagen data op grond waarvan gegevens worden vernietigd.
- De instelling gaat periodiek na in hoeverre de dienstverleners zich houden aan de afgesproken bewaartermijnen.
- De instelling beoordeelt periodiek of dienstverleners en onderaannemers voldoen aan de eisen van de instelling op het gebied van gegevensopslag, archivering en retentie.

12.2 Disposal

Good Practices

De instelling heeft een proces ingericht 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.
- Taken en verantwoordelijkheden op bovenstaande onderdelen zijn belegd in 1e, 2e, en 3e lijnfuncties; formele rapportagelijnen zijn ingericht.

De instelling let op de volgende punten bij uitbesteding:

Bij uitbesteding van activiteiten/systemen blijft de instelling eindverantwoordelijk voor het vernietigen van gevoelige gegevens. De instelling heeft een proces ingericht dat ten minste het volgende waarborgt (zie de Good Practice uitbesteding):

- De instelling heeft afspraken gemaakt met de dienstverlener ten aanzien van het vernietigen van gegevens conform het beleid van de instelling. Deze werken door naar eventuele onderaannemers.
- De instelling ontvangt SLR en/of assurance rapportages met de juiste scope en diepgang aan de hand waarvan die afspraken kunnen worden gemonitord.
- De instelling stuurt bij wanneer haar risico-toleranties worden overschreden (zie Risk Management cycle).

Voorbeelden hierbij zijn:

- De instelling heeft vernietigingsprotocollen voor documenten en elektronische gegevensdragers zoals disk drives, 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

Good Practices

De instelling heeft een proces ingericht 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.
- Taken en verantwoordelijkheden op bovenstaande onderdelen zijn belegd in 1e, 2e, en 3e lijnfuncties; formele rapportagelijnen zijn ingericht.

De instelling let op de volgende punten bij uitbesteding:

Bij uitbesteding van activiteiten/systemen blijft de instelling eindverantwoordelijk voor veilig ontvangen, verwerken, opslaan en verstrekken van data. De instelling heeft een proces ingericht dat ten minste het volgende waarborgt (zie de Good Practice uitbesteding):

- De instelling heeft afspraken gemaakt met de dienstverlener ten aanzien van het veilig ontvangen, verwerken, opslaan en verstrekken van data. Deze werken door naar eventuele onderaannemers.
- De instelling ontvangt SLR en/of assurance rapportages met de juiste scope en diepgang aan de hand waarvan die afspraken kunnen worden gemonitord.
- De instelling stuurt bij wanneer haar risicotoleranties worden overschreden (zie Risk Management cycle).

Voorbeelden hierbij zijn:

- De instelling neemt in haar informatiebeveiligings-beleid op hoe medewerkers met gevoelige informatie moeten omgaan op basis van haar dataclassificatie (zie beheersingsmaatregel 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

Good Practices

De instelling heeft een proces ingericht dat onder meer het volgende waarborgt:

- De instelling heeft integraal inzicht in de IT-assets waarvan haar bedrijfsprocessen afhankelijk zijn.
- De instelling heeft inzicht in de configuratie(parameters) van die IT-assets.
- De instelling evalueert aanbevelingen van leveranciers voor een veilige inrichting van IT-infrastructuur en IT-applicaties en legt vast hoe zij haar IT-assets 'veilig' configureert (baselines).
- Taken en verantwoordelijkheden op bovenstaande onderdelen zijn belegd in 1e, 2e, en 3e lijnfuncties; formele rapportagelijnen zijn ingericht.

De instelling let op de volgende punten bij uitbesteding:

Bij uitbesteding van activiteiten/systemen blijft de instelling eindverantwoordelijk dat de dienstverlener inzicht heeft in de IT-assets. De instelling heeft een proces ingericht dat ten minste het volgende waarborgt (zie de Good Practice uitbesteding):

- De instelling heeft afspraken gemaakt met de dienstverlener ten aanzien van het registreren van IT-assets ten behoeve van het tijdig kunnen onderkennen van de impact van kwetsbaarheden in die IT-assets. Deze werken door naar eventuele onderaannemers.
- De instelling ontvangt SLR en/of assurance rapportages met de juiste scope en diepgang aan de hand waarvan die afspraken kunnen worden gemonitord.
- De instelling stuurt bij wanneer haar risico-toleranties worden overschreden (zie Risk Management cycle).

Voorbeelden hierbij zijn:

- De instelling heeft haar IT-assets geïnventariseerd en vastgelegd in centrale repository zoals een Configuration Management Database (CMDB).
- De instelling gebruikt de CMDB om te bepalen in hoeverre IT-assets zijn geïnstalleerd conform een veilige uitgangssituatie (baseline).
- De instelling gebruikt de CMDB ter verificatie van de werkelijk aanwezige IT-assets. Verschillen worden geanalyseerd.
- De instelling gebruikt de CMDB om te bepalen in hoeverre IT-assets zijn verouderd en in hoeverre zij worden ondersteund met security updates.

13.2 Identification and Maintenance of Configuration Items

Good Practices

De instelling heeft een proces ingericht dat onder meer het volgende waarborgt:

- Wijzigingen in de configuratie management database (zie beheersingsmaatregel 13.1) vinden gecontroleerd plaats. Dat wil zeggen dat wijzigingen zijn geaccordeerd en worden gelogd. De instelling heeft de configuratiemanagementprocedure beschreven
- De configuratiemanagementprocedure is geïntegreerd met procedures voor wijzigingsbeheer, incidentbeheer en probleembeheer.
- Taken en verantwoordelijkheden op bovenstaande onderdelen zijn belegd in 1e, 2e, en 3e lijnfuncties; formele rapportagelijnen zijn ingericht.

De instelling let op de volgende punten bij uitbesteding:

Bij uitbesteding van activiteiten/systemen blijft de instelling eindverantwoordelijk voor het proces configuratie management. De instelling heeft een proces ingericht dat ten minste het volgende waarborgt (zie de Good Practice uitbesteding):

- De instelling heeft afspraken gemaakt met de dienstverlener ten aanzien van de identificatie en onderhoud van configuratie items conform het beleid van de instelling. Deze werken door naar eventuele onderaannemers.
- De instelling ontvangt SLR en/of assurance rapportages met de juiste scope en diepgang aan de hand waarvan die afspraken kunnen worden gemonitord.
- De instelling stuurt bij wanneer haar risico-toleranties worden overschreden (zie Risk Management cycle).

Voorbeelden hierbij zijn:

- De configuratiemanagementprocedures zijn gebaseerd op internationale standaarden zoals ITIL.
- Periodiek wordt door de instelling geautomatiseerde inventarisatie scans uitgevoerd op de IT-infrastructuur. De uitkomst van deze scans wordt vergeleken met de inhoud van de CMDB en indien hierin afwijkingen voorkomen worden deze geanalyseerd en actie op ondernomen.
- De instelling stelt op grond van assurance rapportages vast dat haar dienstverleners hun configuratie management beheersen.

14.1 Monitoring and reporting of Service Level Achievements

Good Practices

De instelling heeft een proces ingericht dat onder meer het volgende waarborgt:

- De instelling is specifieke kwantitatieve en kwalitatieve prestatie criteria overeengekomen met haar dienstverleners die daarover rapporteren aan de instelling.
- Rapportages van dienstverleners worden geanalyseerd om zowel positieve als negatieve trends en ontwikkelingen te identificeren voor zowel instelling specifieke als generieke diensten. Hierover wordt het daarvoor verantwoordelijk lijnmanagement geïnformeerd.
- Taken en verantwoordelijkheden op bovenstaande onderdelen zijn belegd in 1e, 2e, en 3e lijnfuncties; formele rapportagelijnen zijn ingericht.

De instelling let op de volgende punten bij onder-uitbesteding:

Zowel bij uitbesteding als bij onder-uitbesteding van activiteiten/systemen is de instelling verantwoordelijk voor het monitoren van prestaties die door de dienstverlener zijn geleverd conform afspraken in de service level agreement.

De instelling heeft een proces ingericht dat ten minste het volgende waarborgt (zie de Good Practice uitbesteding):

- De instelling heeft afspraken gemaakt met de dienstverlener ten aanzien van het rapporteren over gemaakte afspraken. Deze werken door naar eventuele onderaannemers.
- De instelling ontvangt SLR en/of assurance rapportages met de juiste scope en diepgang aan de hand waarvan die afspraken kunnen worden gemonitord.
- De instelling stuurt bij wanneer haar risico-toleranties worden overschreden (zie Risk Management cycle).

Voorbeelden hierbij zijn:

- De instelling ontvangt periodiek een rapportage 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 IT-dienstverlener 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.

14.2 Supplier risk management

Good Practices

De instelling heeft een proces ingericht dat onder meer het volgende waarborgt:

- Risico's met betrekking tot de continue en betrouwbare dienstverlening door dienstverleners zijn geïdentificeerd en gemitigeerd.
- Contracten zijn opgesteld volgens industrie standaarden en zijn in overeenstemming met wettelijke bepalingen.
- Risicomanagement van de instelling beoordeelt de continue beschikbaarheid van kritieke of belangrijke dienstverlening door de dienstverleners, fall back mogelijkheden om de dienstverlening door dienstverleners op een alternatieve wijze voort te zetten en conformiteit met standaards op het gebied van informatiebeveiliging en cybersecurity.
- Taken en verantwoordelijkheden op bovenstaande onderdelen zijn belegd in 1e, 2e, en 3e lijnfuncties; formele rapportagelijnen zijn ingericht.

De instelling let op de volgende punten bij uitbesteding

Zowel bij uitbesteding als bij onder-uitbesteding van activiteiten/systemen blijft de instelling eindverantwoordelijk voor het risicobeheer door dienstverleners. De instelling heeft een proces ingericht dat ten minste het volgende waarborgt (zie de Good Practice uitbesteding):

- De instelling heeft afspraken gemaakt met de dienstverlener ten aanzien van het risicobeheer conform het beleid van de instelling. Deze werken door naar eventuele onderaannemers.
- De instelling ontvangt SLR en/of assurance rapportages met de juiste scope en diepgang aan de hand waarvan die afspraken kunnen worden gemonitord.
- De instelling stuurt bij wanneer haar risico-toleranties worden overschreden (zie Risk Management cycle).

Voorbeelden hierbij zijn:

- De instelling heeft samen met haar dienstverleners een risicoanalyse met betrekking tot de continuïteit en betrouwbaarheid van de dienstverlening opgesteld. Risico's bij partijen waaraan diensten zijn onder-uitbesteed zijn meegenomen in de risicoanalyse.
- 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 (backup) data van de instelling na de exit. Onder-uitbesteding is in scope van de exit plannen.
- De instelling heeft maatregelen 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. De instelling gaat voor kritieke of belangrijke systemen na in hoeverre deze afspraken in de overeenkomsten zijn nageleefd.
- De instelling beschikt over een standaard geheimhoudingsverklaring 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 van haar kritische dienstverleners en neemt waar nodig actie.

15.1 Security incident definition

Good Practices

De instelling heeft een proces ingericht dat onder meer het volgende waarborgt:

- De instelling hanteert een eenduidige definitie voor beveiligingsincidenten die bij alle belanghebbenden bij de instelling bekend is.
- In het incidentmanagement proces zijn (cyber) beveiligingsincidenten afzonderlijk geclassificeerd en vastgelegd met als doel dat op dergelijke incidenten snel en met de juiste expertise wordt gereageerd.
- De instelling heeft procedures vastgesteld met betrekking tot het melden van cybersecurity incidenten, het reageren op (cyber)beveiligings-incidenten, het beperken van schade als gevolg van die incidenten en het uitvoeren van herstelwerkzaamheden.
- (Cyber)security incidenten worden conform geldende regels gerapporteerd aan de autoriteiten.
- Taken en verantwoordelijkheden op bovenstaande onderdelen zijn belegd in 1e, 2e, en 3e lijnfuncties; formele rapportagelijnen zijn ingericht.

De instelling let op de volgende punten bij uitbesteding:

Bij uitbesteding van activiteiten/systemen blijft de instelling eindverantwoordelijk dat cybersecurity incidenten snel worden geïdentificeerd, gemitigeerd en gerapporteerd. De instelling heeft een proces ingericht dat ten minste het volgende waarborgt (zie de Good Practice uitbesteding):

- De instelling heeft afspraken gemaakt met de dienstverlener ten aanzien van de het identificeren, mitigeren en rapporteren van beveiligingsincidenten conform het beleid van de instelling. Deze werken door naar eventuele onderaannemers.
- De instelling ontvangt SLR en/of assurance rapportages met de juiste scope en diepgang aan de hand waarvan die afspraken kunnen worden gemonitord.
- De instelling stuurt bij wanneer haar risico-toleranties worden overschreden (zie Risk Management cycle).

Voorbeelden hierbij zijn:

- De instelling heeft een proces ingericht dat waarborgt dat alle (potentiele) beveiligings-incidenten centraal worden gemeld en worden geregistreerd.
- De Security Officer beoordeelt (ten minste) dagelijks de geregistreerde beveiligingsincidenten en bepaalt de impact en opvolging 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 IT-infrastructuur. De instelling heeft hiervoor een Security Operations Center (SOC) ingericht.
- De instelling maakt gebruik van tooling zoals een SIEM om IT-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.
- Indien zich een substantieel incident voordoet wordt het bestuur voldoende geïnformeerd over de respons. 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.

15.2 Incident escalation

Good Practices

De instelling heeft een proces ingericht dat onder meer het volgende waarborgt:

- De instelling beschikt over een geformaliseerd beleid voor incident management, waarin een escalatieprocedure en escalatiecriteria zijn opgenomen.
- De escalatieprocedure is gebaseerd op overeengekomen serviceniveaus voor incidenten die niet onmiddellijk kunnen worden opgelost.
- Categorisering en prioritering gebeurt op basis van impactanalyse, gedefinieerde criteria en serviceniveaus.
- Het reageren op informatiebeveiliging en cybersecurity incidenten wordt getraind.
- Incidenten zijn toegewezen aan een eigenaar.
- Significante incidenten worden gerapporteerd aan het management.
- Escalatieprocedures zijn binnen de instelling bekend en worden nageleefd.
- Oplossingen voor incidenten worden regelmatig geanalyseerd om processen en IT-systemen te verbeteren.
- Taken en verantwoordelijkheden op bovenstaande onderdelen zijn belegd in 1e, 2e, en 3e lijnfuncties; formele rapportagelijnen zijn ingericht.

De instelling let op de volgende punten bij uitbesteding

Bij uitbesteding van activiteiten/systemen blijft de instelling eindverantwoordelijk voor het inzicht geven in incidenten op het juiste managementniveau. De instelling heeft een proces ingericht dat ten minste het volgende waarborgt (zie de Good Practice uitbesteding):

- De instelling heeft afspraken gemaakt met de dienstverlener ten aanzien van het escaleren van incidenten conform het beleid van de instelling. Deze werken door naar eventuele onderaannemers.
- De instelling ontvangt SLR en/of assurance rapportages met de juiste scope en diepgang aan de hand waarvan die afspraken kunnen worden gemonitord.
- De instelling stuurt bij wanneer haar risicotoleranties worden overschreden (zie Risk Management cycle).

Voorbeelden hierbij zijn:

- Naast het hiervoor genoemde beleid en escalatieprocedures, heeft de instelling een Computer Emergency Response Team (CERT) opgericht, bestaande uit gespecialiseerde ICT-professionals, dat in staat is snel te handelen in het geval van een informatiebeveiligings- of cybersecurity incident. Het CERT heeft als doel schade te reduceren en snel herstel van de dienstverlening te bevorderen.
- Het CERT van de instelling richt zich ook op de preventie van cybersecurity incidenten en de voorbereiding van de instelling op dergelijke incidenten.

16.1 Security testing, surveillance and monitoring

Good Practices

De instelling heeft een proces ingericht dat onder meer het volgende waarborgt:

- De instelling heeft de beveiligingsmaatregelen getroffen en vastgelegd. Deze maatregelen worden getest en periodiek geëvalueerd zodat deze blijven voldoen aan vastgestelde security baselines.
- Monitoring van ongebruikelijke activiteiten in IT-systemen vindt plaats, uitzonderingen worden gesignaleerd en opgevolgd.
- Taken en verantwoordelijkheden op bovenstaande onderdelen zijn belegd in 1e, 2e, en 3e lijnfuncties; formele rapportagelijnen zijn ingericht.

De instelling let op de volgende punten bij uitbesteding:

Bij uitbesteding van activiteiten/systemen blijft de instelling eindverantwoordelijk voor het testen, monitoren en bewaken van de kwaliteit van informatiebeveiliging. De instelling heeft een proces ingericht dat ten minste het volgende waarborgt (zie de Good Practice uitbesteding):

- De instelling heeft afspraken gemaakt met de dienstverlener ten aanzien van het testen, monitoren en bewaken van IT-security conform het beleid van de instelling. Deze werken door naar eventuele onderaannemers.
- De instelling ontvangt SLR en/of assurance rapportages met de juiste scope en diepgang aan de hand waarvan die afspraken kunnen worden gemonitord.
- De instelling stuurt bij wanneer haar risico-toleranties worden overschreden (zie Risk Management cycle).

Voorbeelden hierbij zijn:

- 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.

16.2 Monitoring of internal control framework

Good Practices

De instelling heeft een proces ingericht dat onder meer het volgende waarborgt:

- De instelling beheerst haar IT risico's en risico's op het gebied van informatiebeveiliging en cybersecurity. Hiertoe heeft de instelling een IT-beheersingsraamwerk (internal control framework) opgesteld waarin onder meer een informatiebeveiligingsbeleid, standaarden, procedures, (key) controls en IT 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.
- Taken en verantwoordelijkheden op bovenstaande onderdelen zijn belegd in 1e, 2e, en 3e lijnfuncties; formele rapportagelijnen zijn ingericht.

De instelling let op de volgende punten bij uitbesteding:

Bij uitbesteding van activiteiten/systemen blijft de instelling eindverantwoordelijk voor het monitoren van de dienstverlening. De instelling heeft een proces ingericht dat ten minste het volgende waarborgt (zie de Good Practice uitbesteding):

- De instelling heeft afspraken gemaakt met de dienstverlener ten aanzien van het monitoren van de dienstverlening conform het beleid van de instelling. Deze werken door naar eventuele onderaannemers.
- De instelling ontvangt SLR en/of assurance rapportages met de juiste scope en diepgang aan de hand waarvan die afspraken kunnen worden gemonitord.
- De instelling stuurt bij wanneer haar risico-toleranties worden overschreden (zie Risk Management cycle).

Voorbeelden hierbij zijn:

- De risicomanagementfunctie, interne auditor en externe accountant rapporteren regelmatig hun oordeel, bevindingen en aanbevelingen over de opzet, bestaan en werking van het IT-beheersingsraamwerk.
- De opvolging van aanbevelingen wordt gemonitord.
- De instelling vergelijkt Service Level rapportages van 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

Good Practices

De instelling heeft een proces ingericht dat onder meer het volgende waarborgt:

- 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 beheersingsmaatregelen 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.
- Taken en verantwoordelijkheden op bovenstaande onderdelen zijn belegd in 1e, 2e, en 3e lijnfuncties; formele rapportagelijnen zijn ingericht.

De instelling let op de volgende punten bij uitbesteding:

Bij zowel uitbesteding als onder-uitbesteding van activiteiten/systemen blijft de instelling eind-verantwoordelijk voor de interne beheersing bij de dienstverlener. De instelling heeft een proces ingericht dat ten minste het volgende waarborgt (zie de Good Practice uitbesteding):

- De instelling heeft afspraken gemaakt met de dienstverlener ten aanzien van de interne beheersing bij de dienstverlener conform het beleid van de instelling. Deze werken door naar eventuele onderaannemers.
- De instelling ontvangt SLR en/of assurance rapportages met de juiste scope en diepgang aan de hand waarvan die afspraken kunnen worden gemonitord.
- De instelling stuurt bij wanneer haar risicotoleranties worden overschreden (zie Risk Management cycle).

Voorbeelden hierbij zijn:

- De instelling heeft haar “right-to-audit” bij de dienstverlener en de onderaannemers contractueel vastgelegd.
- De instelling neemt in het contract op dat de dienstverlener de instelling in kennis stelt 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 maatregelen kan nemen of de exitclausule in werking 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 rapportages van de dienstverlener over de werking van de getroffen interne beheersingsmaatregelen bij de dienstverlener.
- De instelling ontvangt en beoordeelt een onafhankelijke assurance rapportage over de beheersing van risico’s op het gebied van informatiebeveiliging en cybersecurity bij de dienstverlener die aansluit bij de afgesproken dienstverlening.
- De instelling bespreekt afwijkingen/uitzonderingen met de dienstverlener. Deze worden door de dienstverlener tijdig en effectief geadresseerd. De instelling bewaakt de afloop.
- De dienstverlener geeft jaarlijks aan de instelling een assurance verklaring af over de IT-beheersing zoals een SOC 2 rapport type II. Maatregelen op het gebied van informatiebeveiliging en cybersecurity maken deel uit van de scope van de assurance verklaring.

16.4 Evaluation of compliance with external requirements

Good Practices

De instelling heeft een proces ingericht dat onder meer het volgende waarborgt:

- De instelling beoordeelt periodiek in hoeverre haar IT-beleid en procedures in lijn zijn met wet- en regelgeving.
- Taken en verantwoordelijkheden op bovenstaande onderdelen zijn belegd in 1e, 2e, en 3e lijnfuncties; formele rapportagelijnen zijn ingericht.

De instelling let op de volgende punten bij uitbesteding:

Bij uitbesteding van activiteiten/systemen blijft de instelling eindverantwoordelijk voor de evaluatie van de naleving van wet- en regelgeving. De instelling heeft een proces ingericht dat ten minste het volgende waarborgt (zie de Good Practice uitbesteding):

- De instelling heeft afspraken gemaakt met de dienstverlener ten aanzien van de evaluatie van de naleving van wet- en regelgeving conform het beleid van de instelling. Deze werken door naar eventuele onderaannemers.
- De instelling ontvangt SLR en/of assurance rapportages met de juiste scope en diepgang aan de hand waarvan die afspraken kunnen worden gemonitord.
- De instelling stuurt bij wanneer haar risicotoleranties worden overschreden (zie Risk Management cycle).

Voorbeelden hierbij zijn:

- De compliance officer van de instelling beoordeelt jaarlijks in hoeverre de IT-policies 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 wordt proactief geïnformeerd bij wijzigingen op het gebied van relevante externe regelgeving.

16.5 Independent assurance

Good Practices

De instelling heeft een proces ingericht dat onder meer het volgende waarborgt:

- De instelling verkrijgt periodiek onafhankelijke assurance over het functioneren van de IT-beheersing van de instelling. Dit omvat ondermeer assurance over de effectiviteit van de getroffen beheersingsmaatregelen op het gebied van informatiebeveiliging en cybersecurity.
- De resultaten van de onafhankelijke beoordeling worden voorgelegd aan het management van de instelling.
- Taken en verantwoordelijkheden op bovenstaande onderdelen zijn belegd in 1e, 2e, en 3e lijnfuncties; formele rapportagelijnen zijn ingericht.

De instelling let op de volgende punten bij uitbesteding:

Bij uitbesteding van activiteiten/systemen blijft de instelling verantwoordelijk voor het verkrijgen van assurance over de IT-beheersing. De instelling heeft een proces ingericht dat ten minste het volgende waarborgt (zie de Good Practice uitbesteding):

- De instelling heeft afspraken gemaakt met de dienstverlener ten aanzien van het verkrijgen van onafhankelijke assurance over de IT-beheersing. Dit omvat ondermeer assurance over de effectiviteit van de getroffen beheersingsmaatregelen op het gebied van informatiebeveiliging en cybersecurity. Deze werken door naar eventuele onderaannemers.
- De instelling ontvangt SLR en/of assurance rapportages met de juiste scope en diepgang aan de hand waarvan die afspraken kunnen worden gemonitord.
- De instelling stuurt bij wanneer haar risico-toleranties worden overschreden (zie Risk Management cycle).

Voorbeelden hierbij zijn:

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

17.1 Identity & Access Management

Good Practices

De instelling heeft een proces ingericht dat onder meer het volgende waarborgt:

- Toegang tot informatiesystemen en data van de instelling is te herleiden naar uniek te identificeren personen (intern, extern en inhuur) of naar IT-services (bijv. scripts en batch jobs) met een uniek te identificeren eigenaar.
- 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 beheersingsmaatregel 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 IT-infrastructuur en in IT-applicaties, conform de geaccordeerde SOLL autorisatie matrices.
- Toegangsrechten in IT-systemen (IST) worden regelmatig vergeleken met de SOLL autorisatie matrices.
- Taken en verantwoordelijkheden op bovenstaande onderdelen zijn belegd in 1e, 2e, en 3e lijnfuncties; formele rapportagelijnen zijn ingericht.

De instelling let op de volgende punten bij uitbesteding:

Bij uitbesteding van activiteiten/systemen blijft de instelling eindverantwoordelijk voor de beheersing van toegang tot de informatiesystemen en data. De instelling heeft een proces ingericht dat ten minste het volgende waarborgt (zie de Good Practice uitbesteding):

- De instelling heeft afspraken gemaakt met de dienstverlener ten aanzien van de beheersing van toegang tot informatiesystemen en data conform het beleid van de instelling. Deze werken door naar eventuele onderaannemers.
- De instelling ontvangt SLR en/of assurance rapportages met de juiste scope en diepgang aan de hand waarvan die afspraken kunnen worden gemonitord.
- De instelling stuurt bij wanneer haar risicotoleranties worden overschreden (zie Risk Management cycle).

Voorbeelden hierbij zijn:

- De instelling kent unieke user-id's toe aan alle personen met toegang tot de IT-systemen en data. Gebruikersidentiteiten en toegangsrechten worden bijgehouden in een centrale repository.
- De instelling past het principe van 'Role based access' toe.
- Toegang tot IT-systemen en data wordt verleend op basis van 'need-to-know' en 'least privilege' principes. De naleving van deze principes wordt periodiek geëvalueerd.
- De instelling gebruikt een Identity & Access Management (IAM) tool ter ondersteuning van de inrichting van de toegangsbeveiliging en de controle daarop door bedrijfsproceseigenaren en IT-systeembeheerders.
- 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.

17.2 User account management

Good Practices

De instelling heeft een proces ingericht 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.
- Taken en verantwoordelijkheden op bovenstaande onderdelen zijn belegd in 1e, 2e, en 3e lijnfuncties; formele rapportagelijnen zijn ingericht.

De instelling let op de volgende punten bij uitbesteding:

Bij uitbesteding van activiteiten/systemen blijft de instelling eindverantwoordelijk dat toegangsrechten tot informatiesystemen en data op gecontroleerde wijze worden verleend, gewijzigd en verwijderd. De instelling heeft een proces ingericht dat ten minste het volgende waarborgt (zie de Good Practice uitbesteding):

- De instelling heeft afspraken gemaakt met de dienstverlener ten aanzien van het verlenen, wijzigen en intrekken toegang tot informatiesystemen en data conform het beleid van de instelling. Deze werken door naar eventuele onderaannemers.
- De instelling ontvangt SLR en/of assurance rapportages met de juiste scope en diepgang aan de hand waarvan die afspraken kunnen worden gemonitord.
- De instelling stuurt bij wanneer haar risico-toleranties worden overschreden (zie Risk Management cycle).

Voorbeelden hierbij zijn:

- De instelling maakt gebruik van User Provisioning, waarbij user accounts in de IT-infrastructuur en business IT-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.

18.1 Infrastructure resource protection and availability

Good Practices

De instelling heeft een proces ingericht dat onder meer het volgende waarborgt:

- De beheersingsmaatregelen in de IT-infrastructuur componenten zijn zodanig ingericht dat zij een hoog niveau van beschikbaarheid, exclusiviteit en integriteit van informatie waarborgen.
- De verantwoordelijkheid voor het ontwerpen en implementeren van deze beheersingsmaatregelen is duidelijk belegd.
- Het ontwerp en de implementatie van deze beheersingsmaatregelen wordt gemonitord en geëvalueerd.
- Taken en verantwoordelijkheden op bovenstaande onderdelen zijn belegd in 1e, 2e, en 3e lijnfuncties; formele rapportagelijnen zijn ingericht.

De instelling let op de volgende punten bij uitbesteding:

Bij uitbesteding van activiteiten/systemen blijft de instelling eindverantwoordelijk voor de beschik-baarheid en integriteit van de IT-infrastructuur.
De instelling heeft een proces ingericht dat ten minste het volgende waarborgt (zie de Good Practice uitbesteding):

- De instelling heeft afspraken gemaakt met de dienstverlener ten aanzien van de beschikbaarheid en integriteit van de IT-infrastructuur conform het beleid van de instelling. Deze werken door naar eventuele onderaannemers.
- De instelling ontvangt SLR en/of assurance rapportages met de juiste scope en diepgang aan de hand waarvan die afspraken kunnen worden gemonitord.
- De instelling stuurt bij wanneer haar risico-toleranties worden overschreden (zie Risk Management cycle).

Voorbeelden hierbij zijn:

- Risicoanalyses voor infrastructuur componenten houden rekening met actuele cyberdreigingen, zoals bijvoorbeeld vastgelegd in de SANS Top 20, 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.
- Het gebruik van 'scrubbing services' (omleiden van de aanval naar een anti-DDoS omgeving) voor het mitigeren van DDoS aanvallen. 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 en een onderbouwde afweging gemaakt op welke interne of externe locatie sleutels en wachtwoorden worden opgeslagen.
- De beveiliging en beschikbaarheid van de IT-infrastructuur is een vast agendapunt in de relevante gremia in de eerste, tweede en derde lijn van de instelling.

18.2 Infrastructure maintenance

Good Practices:

De instelling heeft een proces ingericht dat onder meer het volgende waarborgt:

- Onderhoud aan de IT-infrastructuur verloopt planmatig, gestructureerd en in lijn met de change management procedures van de instelling.
- De instelling heeft de infrastructuurcomponenten geclassificeerd, waarbij onderscheid is gemaakt tussen kritische en minder kritische componenten.
- In de prioritering en uitvoering van onderhoud aan de IT-infrastructuur houdt de instelling rekening met de classificatie van infrastructuur componenten.
- Oplossingen voor kwetsbaarheden in de IT-infrastructuur zoals patches hebben invloed op de prioritering van onderhoudswerkzaamheden aan de IT-infrastructuur.
- Hierbij worden change management processen gevolgd, waarbij rekening wordt gehouden met patchmanagement voor kritisch en minder kritische kwetsbaarheden. Dit is gebaseerd op risicoanalyses die onderdeel uitmaken van het changemanagement proces (change risk assessments (cra's)).
- Bij de cra's wordt expliciet aandacht besteed aan cyberdreigingen. Deze zijn van invloed op prioritering van implementatie van de changes.
- Een verhoogde focus bij de instelling op klant-beleving en time-to-market leidt er niet toe dat de implementatie van infrastructurele (beveiligings) maatregelen en investeringen in technologische ontwikkelingen (te) lang worden uitgesteld.
- Taken en verantwoordelijkheden op bovenstaande onderdelen zijn belegd in 1e, 2e, en 3e lijnfuncties; formele rapportagelijnen zijn ingericht.

De instelling let op de volgende punten bij uitbesteding:

Bij uitbesteding van activiteiten/systemen blijft de instelling eindverantwoordelijk dat onderhoud van de IT-infrastructuur plaatsvindt. De instelling heeft een proces ingericht dat ten minste het volgende waarborgt (zie de Good Practice uitbesteding):

- De instelling heeft afspraken gemaakt met de dienstverlener ten aanzien van het onderhoud van de IT-infrastructuur conform het beleid van de instelling. Deze werken door naar eventuele onderaannemers.
- De instelling ontvangt SLR en/of assurance rapportages met de juiste scope en diepgang aan de hand waarvan die afspraken kunnen worden gemonitord.
- De instelling stuurt bij wanneer haar risico-toleranties worden overschreden (zie Risk Management cycle).

Voorbeelden hierbij zijn:

- Implementeren van kritische beveiligingspatches is een specifiek onderdeel van het patch-managementproces.
- De status van de IT-infrastructuur inclusief de kwetsbaarheid voor cyberdreigingen wordt periodiek met behulp van tools geïnventariseerd, hierover wordt gerapporteerd en actie op achterstallig onderhoud wordt genomen.

18.3 Cryptographic key management

Good Practices:

De instelling heeft een proces ingericht dat onder meer het volgende waarborgt:

- Het beheer van cryptografische sleutels vindt op beheerste 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 maatregelen zijn getroffen.
- De instelling heeft de risico's van cyberaanvallen gericht op het modificeren en onderscheppen van de cryptografische sleutels onderkend en met passende maatregelen beheerst.
- Taken en verantwoordelijkheden op bovenstaande onderdelen zijn belegd in 1e, 2e, en 3e lijnfuncties; formele rapportagelijnen zijn ingericht.

De instelling let op de volgende punten bij uitbesteding:

Bij uitbesteding van activiteiten/systemen blijft de instelling eindverantwoordelijk voor het beheer van cryptografische sleutels. De instelling heeft een proces ingericht dat ten minste het volgende waarborgt (zie de Good Practice uitbesteding):

- De instelling heeft afspraken gemaakt met de dienstverlener ten aanzien van het beheer van cryptografische sleutels conform het beleid van de instelling. Deze werken door naar eventuele onderaannemers.
- De instelling ontvangt SLR en/of assurance rapportages met de juiste scope en diepgang aan de hand waarvan die afspraken kunnen worden gemonitord.
- De instelling stuurt bij wanneer haar risico-toleranties worden overschreden (zie Risk Management cycle).

Voorbeelden 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 beschermen.
- De beschikbaarheid van cryptografische sleutels is meegenomen in de continuïteitsplannen van de instelling.

18.4 Network Security

Good Practices:

De instelling heeft een proces ingericht dat onder meer het volgende waarborgt:

- De instelling past up-to-date technische beveiligingsmaatregelen toe (zoals firewalls, netwerksegmentatie en intrusion detection) en daarbij behorende beheerprocedures om de toegang tot de IT-infrastructuur te beperken tot geautoriseerde personen, IT-services en informatie-uitwisseling tussen netwerken.
- Autorisaties voor beheerders van de IT-infrastructuur, waaronder netwerkbeheerders, is op degelijke wijze ingericht (zie beheersingsmaatregels 17.1 en 17.2)
- Taken en verantwoordelijkheden op bovenstaande onderdelen zijn belegd in 1e, 2e, en 3e lijnfuncties; formele rapportagelijnen zijn ingericht.

De instelling let op de volgende punten bij uitbesteding:

Bij uitbesteding van activiteiten/systemen blijft de instelling eindverantwoordelijk voor netwerk beveiliging. De instelling heeft een proces ingericht dat ten minste het volgende waarborgt (zie de Good Practice uitbesteding):

- De instelling heeft afspraken gemaakt met de dienstverlener ten aanzien van netwerk beveiliging conform het beleid van de instelling. Deze werken door naar eventuele onderaannemers.
- De instelling ontvangt SLR en/of assurance rapportages met de juiste scope en diepgang aan de hand waarvan die afspraken kunnen worden gemonitord.
- De instelling stuurt bij wanneer haar risicotoleranties worden overschreden (zie Risk Management cycle).

Voorbeelden hierbij zijn:

- De instelling past moderne firewall technologie toe in haar netwerk infrastructuur die in lijn is met best practices zoals GovCert, ISO/IEC en ITSec.
- Meldingen van cyberaanvallen op de IT-infrastructuur worden gelogd en de logging wordt geautomatiseerd geanalyseerd waarop de instelling passende acties neemt.
- De beschikbaarheid van de netwerkinfrastructuur (percentages voor ‘uptime’ en ‘downtime’) wordt geregistreerd en gemonitord. De instelling stelt gericht onderzoek in bij downtime als gevolg van beveiligingsincidenten.
- De instelling maakt gebruik van tooling die in de netwerkinfrastructuur actief speurt naar ongeautoriseerde apparatuur zoals laptops, routers en WiFi access points.
- De instelling past endpoint security toe op laptops, tablets en werkstations.

18.5 Exchange of sensitive data

Good Practices

De instelling heeft een proces ingericht dat onder meer het volgende waarborgt:

- De instelling heeft beleid geformuleerd ten aanzien van het delen van vertrouwelijke informatie.
- De instelling beschikt over faciliteiten die de uitwisseling van vertrouwelijke informatie via beveiligde kanalen mogelijk maakt.
- Taken en verantwoordelijkheden op bovenstaande onderdelen zijn belegd in 1e, 2e, en 3e lijnfuncties; formele rapportagelijnen zijn ingericht.

De instelling let op de volgende punten bij uitbesteding:

Bij uitbesteding van activiteiten/systemen blijft de instelling eindverantwoordelijk dat gevoelige data uitsluitend via beveiligde kanalen plaatsvindt. De instelling heeft een proces ingericht dat ten minste het volgende waarborgt (zie de Good Practice uitbesteding):

- De instelling heeft afspraken gemaakt met de dienstverlener ten aanzien van het uitwisselen van gevoelige data conform het beleid van de instelling. Deze werken door naar eventuele onderaannemers.
- De instelling ontvangt SLR en/of assurance rapportages met de juiste scope en diepgang aan de hand waarvan die afspraken kunnen worden gemonitord.
- De instelling stuurt bij wanneer haar risico-toleranties worden overschreden (zie Risk Management cycle).

Voorbeelden 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 van de integriteit van berichten waarborgt, alsook de bevestiging van verzending, van ontvangst en identiteit van de afzender en ontvanger van vertrouwelijke gegevens.
- Vertrouwelijke gegevens worden versleuteld vastgelegd op laptops, harde schijven, USB sticks en andere informatiedragers.
- De instelling past Data Loss Prevention software toe ter controle van uitgaande berichten.
- De instelling hanteert protocollen voor het schonen en vernietigen van media waar vertrouwelijke gegevens op kunnen staan, zoals harde schijven, USB sticks en SSD's.

19.1 Malicious software prevention, detection and correction

Good Practices

De instelling heeft een proces ingericht dat onder meer het volgende waarborgt:

- De instelling heeft zowel preventieve, detecterende als corrigerende maatregelen geïmplementeerd om IT-systemen en applicaties te beveiligen tegen cyberdreigingen, zoals virussen, wormen, malware, cryptoware, cryptojacking en spyware.
- Taken en verantwoordelijkheden op bovenstaande onderdelen zijn belegd in 1e, 2e, en 3e lijnfuncties; formele rapportagelijnen zijn ingericht.

De instelling let op de volgende punten bij uitbesteding:

Bij uitbesteding van activiteiten/systemen blijft de instelling eindverantwoordelijk voor preventie, detectie en correctie van kwaadaardige software. De instelling heeft een proces ingericht dat ten minste het volgende waarborgt (zie de Good Practice uitbesteding):

- De instelling heeft afspraken gemaakt met de dienstverlener ten aanzien van preventie, detectie en correctie van kwaadaardige software conform het beleid van de instelling. Deze werken door naar eventuele onderaannemers.
- De instelling ontvangt SLR en/of assurance rapportages met de juiste scope en diepgang aan de hand waarvan die afspraken kunnen worden gemonitord.
- De instelling stuurt bij wanneer haar risico-toleranties worden overschreden (zie Risk Management cycle).

Voorbeelden hierbij zijn:

- De instelling heeft tools geïmplementeerd voor de automatische detectie en blokkade van virussen, wormen, malware en spyware zoals moderne firewall technologie, virusscanners, Intrusion Detection Systems (IDS) en Intrusion Prevention Systems (IPS).
- Logfiles uit voornoemde systemen worden naar een Security Incident and Event Monitoring (SIEM) systeem gestuurd ten behoeve van analyse en (re) actie.
- De instelling past segmentering van haar netwerk toe om de impact van een geslaagde malware aanval zo veel mogelijk te beperken.
- 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.

19.2 Vulnerability management

Good Practices

De instelling heeft een proces ingericht dat onder meer het volgende waarborgt:

- De belangrijkste IT-assets zijn op basis van een risicoanalyse geïdentificeerd.
- Periodiek worden aan de IT-assets gerelateerde (cyber)kwetsbaarheden mede op basis van threat intelligence en vulnerability scans vastgesteld en de impact op de (bedrijfs)processen van de instelling bepaald.
- Op basis van de impact worden risicomitigerende acties bepaald voor bedreigingen die buiten de risicotolerantie van de instelling vallen.
- Taken en verantwoordelijkheden op bovenstaande onderdelen zijn belegd in 1e, 2e, en 3e lijnfuncties; formele rapportagelijnen zijn ingericht.

De instelling let op de volgende punten bij uitbesteding:

Bij uitbesteding van activiteiten/systemen blijft de instelling eindverantwoordelijk voor vulnerability management. De instelling heeft een proces ingericht dat ten minste het volgende waarborgt (zie de Good Practice uitbesteding):

- De instelling heeft afspraken gemaakt met de dienstverlener ten aanzien van vulnerability assessments conform het beleid van de instelling. Deze werken door naar eventuele onderaannemers.
- De instelling ontvangt SLR en/of assurance rapportages met de juiste scope en diepgang aan de hand waarvan die afspraken kunnen worden gemonitord.
- De instelling stuurt bij wanneer haar risico-toleranties worden overschreden (zie Risk Management cycle).

Voorbeelden hierbij zijn:

- De instelling inventariseert regelmatig van welke IT-assets de bedrijfsprocessen gebruik maken.
- De instelling inventariseert frequent (dagelijks) kwetsbaarheden op basis van Threat Intelligence.
- De instelling gebruikt tools om kwetsbaarheden geautomatiseerd te inventariseren (vulnerability scanning).
- De instelling bepaalt structureel en risicogebaseerd, wat de impact van deze kwetsbaarheden op de eigen IT-assets is.
- De instelling bepaalt een risk response op basis van haar risicotoleranties en monitort de opvolging van de risk response aan de hand van gedefinieerde KPI's.
- De instelling bespreekt met haar dienstverleners regelmatig rapportages / dashboards omtrent de resultaten van uitgevoerde vulnerability scans.

19.3 Application life-cycle management

Good Practices

De instelling heeft een proces ingericht dat onder meer het volgende waarborgt:

- Onderhoud aan applicaties verloopt planmatig, gestructureerd en in lijn met de change management procedures van de instelling.
- De instelling bewaakt dat de IT-infrastructuur en IT-applicaties die zij gebruikt, worden ondersteund door de ontwikkelaar/leverancier en dat beveiligingsupdates (patches) beschikbaar worden gesteld.
- Oplossingen voor kwetsbaarheden in applicaties zoals patches hebben invloed op de prioritering van reguliere onderhoudswerkzaamheden aan IT-applicaties.
- Taken en verantwoordelijkheden op bovenstaande onderdelen zijn belegd in 1e, 2e, en 3e lijnfuncties; formele rapportagelijnen zijn ingericht.

De instelling let op de volgende punten bij uitbesteding:

Bij uitbesteding van activiteiten/systemen blijft de instelling eindverantwoordelijk voor application life-cycle management. De instelling heeft een proces ingericht dat ten minste het volgende waarborgt (zie de Good Practice uitbesteding):

- De instelling heeft afspraken gemaakt met de dienstverlener ten aanzien van application life-cycle management conform het beleid van de instelling. Deze werken door naar eventuele onderaannemers.
- De instelling ontvangt SLR en/of assurance rapportages met de juiste scope en diepgang aan de hand waarvan die afspraken kunnen worden gemonitord.
- De instelling stuurt bij wanneer haar risico-toleranties worden overschreden (zie Risk Management cycle).

Voorbeelden hierbij zijn:

- De instelling hanteert bij de ontwikkeling en aanschaf van IT-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.

20.1 Protection of security technology

Good Practices

De instelling heeft een proces ingericht dat onder meer het volgende waarborgt:

- De instelling heeft inzicht in de voor haar relevante security technologie[11]
- Gezien hun inherent hoge risicoprofiel, zijn op de security technologie specifieke beveiligings-maatregelen van toepassing.
- Documentatie over de security technologie en beveiligingsmaatregelen is alleen op basis van het 'need-to-know' principe beschikbaar.
- Taken en verantwoordelijkheden op bovenstaande onderdelen zijn belegd in 1e, 2e, en 3e lijnfuncties; formele rapportagelijnen zijn ingericht.

De instelling let op de volgende punten bij uitbesteding:

Bij uitbesteding van activiteiten/systemen blijft de instelling eindverantwoordelijk voor de security gerelateerde technologie. De instelling heeft een proces ingericht dat ten minste het volgende waarborgt (zie de Good Practice uitbesteding):

- De instelling heeft afspraken gemaakt met de dienstverlener ten aanzien van de beheersing van security technologie conform het beleid van de instelling (die doorwerken naar eventuele onderaannemers)
- De instelling ontvangt SLR en/of assurance rapportages met de juiste scope en diepgang aan de hand waarvan die afspraken kunnen worden gemonitord.
- De instelling stuurt bij wanneer haar risicotoleranties worden overschreden (zie Risk Management cycle).

Voorbeelden hierbij zijn:

- Voor deze componenten gelden aanvullende maatregelen 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.
- IT-systemen die een rol spelen in de beveiliging van de instelling zijn aangesloten op een SIEM.
- Op de IT-security componenten van de instelling wordt gericht beveiligingsonderzoek uitgevoerd door een daarin gespecialiseerde partijen.

11 Onder security gerelateerde 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

Good Practices

De instelling heeft een proces ingericht dat onder meer het volgende waarborgt:

- De instelling heeft een beleid gedefinieerd en geïmplementeerd ten aanzien van de fysieke beveiliging van kantoorgebouwen, terreinen en IT-infrastructuur locaties (datacenters, serverruimten).
- Fysieke toegangsbeveiligingsmaatregelen zijn in lijn met het risicoprofiel van de instelling.
- Fysieke toegangsbeveiligingsmaatregelen worden regelmatig onderhouden en getest.
- Taken en verantwoordelijkheden op bovenstaande onderdelen zijn belegd in 1e, 2e, en 3e lijnfuncties; formele rapportagelijnen zijn ingericht.

De instelling let op de volgende punten bij uitbesteding:

Bij uitbesteding van activiteiten/systemen blijft de instelling eindverantwoordelijk voor fysieke beveiliging van (IT) assets. De instelling heeft een proces ingericht dat ten minste het volgende waarborgt (zie de Good Practice uitbesteding):

- De instelling heeft afspraken gemaakt met de dienstverlener ten aanzien van de fysieke beveiliging van (IT) assets conform het beleid van de instelling. Deze werken door naar eventuele onderaannemers.
- De instelling ontvangt SLR en/of assurance rapportages met de juiste scope en diepgang aan de hand waarvan die afspraken kunnen worden gemonitord.
- De instelling stuurt bij wanneer haar risicotoleranties worden overschreden (zie Risk Management cycle).

Voorbeelden hierbij zijn:

- Op basis van een risicoanalyse heeft de instelling bepaald dat een fysieke zonering is aangebracht met verschillende niveaus van toegang (bijvoorbeeld: publiek, personeel en beperkt).
- Bij fysiek onderhoud aan beveiligingsapparatuur is het 4-ogen principe van toepassing.
- De instelling laat de fysieke beveiligingsmaatregelen jaarlijks controleren door een “Mystery Guest”.

21.2 Physical access

Good Practices

De instelling heeft een proces ingericht dat onder meer het volgende waarborgt:

- De instelling heeft een beleid gedefinieerd en geïmplementeerd voor de beveiliging gebouwen, terreinen, zones, datacenters en serverruimtes die van belang zijn voor het uitvoeren van de bedrijfsprocessen.
- 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.
- De instelling controleert regelmatig de effectiviteit van fysieke toegangsbeveiligingsmaatregelen en rapporteert over de uitkomsten aan het management. Beoordeling van de toegekende toegangsrechten (SOLL-IST) en beoordeling van logging van het toegangsbeveiligingssysteem worden hierbij meegenomen.
- Taken en verantwoordelijkheden op bovenstaande onderdelen zijn belegd in 1e, 2e, en 3e lijnfuncties; formele rapportagelijnen zijn ingericht.

De instelling let op de volgende punten bij uitbesteding:

Bij uitbesteding van activiteiten/systemen blijft de instelling eindverantwoordelijk voor fysieke toegang. De instelling heeft een proces ingericht dat ten minste het volgende waarborgt (zie de Good Practice uitbesteding):

- De instelling heeft afspraken gemaakt met de dienstverlener ten aanzien van fysieke toegang conform het beleid van de instelling. Deze werken door naar eventuele onderaannemers.
- De instelling ontvangt SLR en/of assurance rapportages met de juiste scope en diepgang aan de hand waarvan die afspraken kunnen worden gemonitord.
- De instelling stuurt bij wanneer haar risico-toleranties worden overschreden (zie Risk Management cycle).

Voorbeelden hierbij zijn:

- De fysieke toegang tot gebouwen en zones wordt beheerst met behulp van toegangspasjes en -poortjes.
- De instelling laat de fysieke toegangsbeveiligingsmaatregelen controleren door een “Mystery Guest”. IT componenten die een rol spelen in de fysieke toegangsbeveiliging van de instelling zijn aangesloten op een SIEM (Security Information and Event Management).

22.1 Penetration testing and ethical hacking

Good Practices

De instelling heeft een proces ingericht dat onder meer het volgende waarborgt:

- De instelling bepaalt op grond van een risicoanalyse en actuele cyberdreigingen welke soorten beveiligingstests worden uitgevoerd alsmede de scope en diepgang van die tests.
- De aard en frequentie van deze tests zijn afhankelijk van het risicoprofiel van de instelling. Onder meer kan gedacht worden aan de volgende soorten beveiligingstests: pentesting, ethical hacking en/of red teaming.
- De instelling gaat na dat de partij die de beveiligingstests uitvoert voldoende geëquipeerd is om dergelijke tests uit te voeren (juiste kennis en ervaring, certificeringen en referenties).
- Taken en verantwoordelijkheden op bovenstaande onderdelen zijn belegd in 1e, 2e, en 3e lijnfuncties; formele rapportagelijnen zijn ingericht.

De instelling let op de volgende punten bij uitbesteding:

Bij uitbesteding van activiteiten/systemen blijft de instelling eindverantwoordelijk voor het testen van informatiebeveiliging en cybersecurity. De instelling heeft een proces ingericht dat ten minste het volgende waarborgt (zie de Good Practice uitbesteding):

- De instelling heeft afspraken gemaakt met de dienstverlener ten aanzien van het testen van informatiebeveiliging en cybersecurity conform het beleid van de instelling. Deze werken door naar eventuele onderaannemers.
- De instelling ontvangt SLR en/of assurance rapportages met de juiste scope en diepgang aan de hand waarvan die afspraken kunnen worden gemonitord.
- De instelling stuurt bij wanneer haar risicotoleranties worden overschreden (zie Risk Management cycle).

Voorbeelden hierbij zijn:

- De instelling neemt voor het bepalen van soorten beveiligingstests in haar risicoanalyse actuele cyberdreigingen mee, zoals phishing, DDoS, cryptoware en CEO 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 voor alle (nieuwe en gewijzigde) kritische IT-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 en het testen van menselijk handelen in relatie tot informatiebeveiliging en cybersecurity.
- De instelling laat pentests uitvoeren door daarin gespecialiseerde partijen.
- De instelling wisselt regelmatig van partij die de pentests uitvoert.
- De instelling betrekt haar kritische dienstverleners bij haar security tests.