Bestuur

1.1 (GO.01) Strategie

Risico:

Het ontbreken van een strategie kan leiden tot slechte zakelijke en beveiligingsbeslissingen of tot een niet passend antwoord op veranderingen in de bedrijfsomgeving.

Doelstelling:

Een strategie en visie op informatie- en cyber security is leidend voor alle activiteiten en maatregelen met betrekking tot informatiebeveiliging.

Volwassenheidsniveaus:

1	(a) Implementatie en uitvoering van activiteiten en maatregelen op het gebied van informatiebeveiliging en/of cyber security gebeurt ad hoc.
2	(a) Een strategie en visie is geformuleerd, maar is niet formeel vastgesteld.
3	(a) Strategie en visie zijn goedgekeurd door het senior management. (b) Strategie en missie worden actief gecommuniceerd naar medewerkers, leveranciers en business partners.
4	(a) Strategie en visie is leidend voor alle activiteiten en maatregelen met betrekking tot informatiebeveiliging en cyber security. (b) Indien van toepassing wordt vastgelegd hoe er in lijn met strategie en visie gewerkt wordt. (c) De geldigheid en uitvoerbaarheid van de strategie en visie wordt periodiek geverifieerd.
5	(a) De strategie geeft aan hoe IT de organisatie helpt haar doelstellingen te behalen. (b) Indien noodzakelijk worden strategie en visie bijgesteld om organisatiedoelstellingen en externe ontwikkelingen bij te houden.

Referenties:

Normenkader Informatie-beveiliging HO 2015 ***01 Beleid en Organisatie***	1.1 1.2
COBIT 4.1	PO1.4 ME4.2
COBIT 5	APO02.01 APO02.02 APO02.03 APO02.04 APO02.05
ISO 27K 2013	5.1 A.5.1.1
DNB 2014/2017	1.2
BIO 2019	5.1.1 5.1.1.1
NIST Cybersecurity Framework	ID.GV-3

Bestuur

1.2 (GO.02) Beleid

Risico:

Onvermogen om te voldoen aan wet- en regelgeving en/of interne informatiebeveiligingseisen, omdat het beleidskader dat de IT-strategie en informatiebeveiliging ondersteunt ineffectief is.

Doelstelling:

De organisatie heeft een (informatie)beveiligingsbeleid vastgesteld en beschreven en gecommuniceerd aan medewerkers. Indien van toepassing wordt het beleid ook actief meegedeeld aan leveranciers en contractpartners. Het beleid wordt regelmatig geëvalueerd en zo nodig geactualiseerd en goedgekeurd door het senior management.

Volwassenheidsniveaus:

1	(a) Er is geen beleid opgesteld. (b) Er zijn enkele beleidsstukken in concept.
2	(a) Er is (informatie)beveiligingsbeleid waarin de meest relevante aspecten van informatiebeveiliging zijn opgenomen.
3	(a) Informatiebeveiligingsbeleid is goedgekeurd door het senior management. (b) Beleid wordt actief gecommuniceerd naar medewerkers, leveranciers en contractpartners en is digitaal (op intranet) of in hard copy beschikbaar. (c) Het beleid maakt onderdeel uit van het security awareness programma. (d) Het voldoen aan beleid wordt op ad-hoc-basis geëvalueerd. (e*) Het informatiebeveiligingsbeleid voldoet aan best practices.
4	(a) Het (informatie)beveiligingsbeleid is ingebed in/overgenomen door de organisatie en is vertaald naar onderliggende procedures, baselines en instructies. (b) Periodiek wordt het beleid geëvalueerd, geactualiseerd en opnieuw goedgekeurd door het senior management.
5	(a) Periodiek wordt aan het senior management gerapporteerd of aan het (informatie)beveiligingsbeleid wordt voldaan.

Referenties:

Normenkader Informatie-beveiliging HO 2015 ***01 Beleid en Organisatie***	1.1 1.2 1.3 1.4 2.2 6.9
COBIT 4.1	PO6.3 PO6.4 PO6.5
COBIT 5	APO01.03 APO01.04 APO01.06 APO01.07 APO01.08
ISO 27K 2013	5.2 A.5.1.1 A.5.1.2 A.6.1.1 A.7.2.2 A.18.2.2
DNB 2014/2017	1.2
BIO 2019	5.1.1 5.1.1.1 5.1.2 5.1.2.1 6.1.1.1 6.1.1.2 6.1.1.3 6.1.1.4
NIST Cybersecurity Framework	ID.GV-3

Bestuur

1.3 (GO.03) Planning / Roadmap

Risico:

De organisatie voorziet niet in richtlijnen of ondersteuning om informatiebeveiliging in overeenstemming te brengen met bedrijfsdoelstellingen, risico's en compliance eisen.

Doelstelling:

Bedrijfsdoelstellingen, risico's en compliance eisen worden vertaald in een algemeen informatiebeveiligingsplan en/of cyber security plan, rekening houdend met de IT-infrastructuur en de veiligheidscultuur.

Volwassenheidsniveaus:

1	(a) Er is geen informatiebeveiligings- of cyber security plan of roadmap opgesteld. (b) Er lopen enkele projecten op het gebied van IT-beveiliging of deze zijn gepland.
2	(a) Er is een informatiebeveiligings- en/of cybersecurity plan of roadmap opgesteld. Dit plan bestrijkt alle relevante organisatiedoelstellingen, risico's en eisen op het gebied van wet- en regelgeving.
3	(a) Het plan of roadmap is goedgekeurd door het senior management. (b) Het plan is uitgewerkt in (informatie)beveiligingsbeleid en -procedures, tezamen met passende investeringen op het gebied van diensten, personeel, software en hardware. (c) Gerelateerd beleid en -procedures worden gecommuniceerd naar gebruikers en stakeholders.
4	(a) Het informatiebeveiligings- en/of cyber security plan is geïmplementeerd en wordt ondersteund door het afdwingen van security policies, procedures, diensten, personeel, software en hardware. (b) Het informatiebeveiligings- en/of cyber security plan wordt periodiek geëvalueerd, geactualiseerd en goedgekeurd op een passend managementniveau. (c*) Er is gedocumenteerd hoe medewerkers blijvend geïnformeerd worden over informatiebeveiliging en privacy en hun eigen rol daarin.
5	(a) Het informatiebeveiligings- en/of cyber security plan en daaraan gerelateerd projectportfolio worden periodiek gemonitord op bijvoorbeeld voortgang, bedreigingen, haalbaarheid en mate waarin aan business requirements wordt voldaan. (b) Hierover wordt gerapporteerd aan het senior management.

Referenties:

Normenkader Informatie-beveiliging HO 2015 *01 Beleid en Organisatie*	1.1 1.2 1.3 1.6 1.9 1.10 1.12 1.19 1.20 2.2 3.1 5.1
COBIT 4.1	DS5.2
COBIT 5	APO02.05 APO13.02
ISO 27K 2013	5.2 A.5.1.1 A.5.1.2 A.6.2.1 A.6.2.2 A.7.2.2 A.9.1.1 A.10.1.1 A.13.2.1 A.18.1.1 A.18.1.2 A.18.1.3 A.18.1.4 A.18.1.5
DNB 2014/2017	1.1
BIO 2019	5.1.1 5.1.1.1 5.1.2 5.1.2.1 6.2.1 6.2.1.1 6.2.1.2 6.2.2 7.2.2 7.2.2.1 7.2.2.2 7.2.2.3 9.1.1 10.1.1 10.1.1.1 10.1.1.2 13.2.1 18.1.1 18.1.2 18.1.3 18.1.3.1 18.1.4 18.1.5
NIST Cybersecurity Framework	ID.BE-1 ID.GV-1 ID.GV-2 ID.GV-3

Bestuur

1.4 (GO.04) Architectuur

Risico:

Onvolledig overzicht van huidige en beoogde architectuur kan leiden tot toename in kosten, complexiteit en onvermogen om tijdig te reageren op problemen die voortkomen uit zakelijke of juridische veranderingen of (externe) dreigingen.

Doelstelling:

Er is een enterprise information architecture model (EIAM) opgesteld en toegepast om applicatieontwikkeling en beslissingsondersteunende activiteiten mogelijk te maken, conform informatie- of IT-plannen. Dit model moet het mogelijk maken om effectief, veilig en op een robuuste manier informatie te creëren, gebruiken en te delen zoals wordt vereist door bedrijfsdoelstellingen en wettelijke voorschriften.

Volwassenheidsniveaus:

1	(a) Geen enterprise information architecture model (EIAM) gedefinieerd.
2	(a) De baseline architectuur (IST) is gedefinieerd. (b) Er zijn EIAM-specifieke processen opgezet om de ontwikkeling van systemen en/of toepassingen mogelijk te maken.
3	(a) Er is een baseline voor de huidige (IST) en de beoogde architectuur (SOLL) gedefinieerd. (b) De beoogde architectuur is in overeenstemming met de organisatiebrede doelstellingen (inclusief de naleving van wettelijke voorschriften) en de organisatorische verantwoordelijkheden. (c) Het EIAM en de relevante processen zijn gedefinieerd en worden toegepast om applicatieontwikkeling en beslissingsondersteunende activiteiten in overeenstemming met de informatie- of IT-plannen mogelijk te maken. (d) Het EIAM is goedgekeurd door het (senior) management.
4	Aanvullend: (a) Het model moet, op een veilige en robuuste manier, het creëren, gebruiken en delen van informatie effectief ondersteunen in lijn met de instellingsdoelstellingen, met inbegrip van innovaties. (b) De beoogde architectuur is gericht op de prioriteiten en performancedoelstellingen die in het businessplan van de organisatie zijn vastgesteld. (c) Het EIAM en de relevante processen worden periodiek geëvalueerd.
5	Aanvullend: (a) Het EIAM moet het effectief creëren, het gebruik en het delen van informatie vergemakkelijken op een wijze die de integriteit verbetert (of ten minste handhaaft) en die flexibel, functioneel, kosteneffectief en tijdig is.

Referenties:

Normenkader Informatie-beveiliging HO 2015 ***01 Beleid en Organisatie***	1.4
COBIT 4.1	PO4.8 DS5.1
COBIT 5	APO01.01 APO01.02 APO01.03 APO13.01 APO13.03
ISO 27K 2013	5.3 A.6.1.1 A.7.2.1
DNB 2014/2017	5.1 5.2
BIO 2019	6.1.1 6.1.1.1 6.1.1.2 6.1.1.3 6.1.1.4 7.2.1 7.2.1.1 Supplement BIG: 3.1
NIST Cybersecurity Framework	ID.GV-2 DE.DP-1 RS.CO-1 RC.CO-3

Bestuur

1.5 (GO.05) Onafhankelijke assurance

Risico:

Naleving van wet- en regelgeving en prestaties worden niet beoordeeld en bevestigd door een onafhankelijke partij, waardoor onbekende en ongeadresseerde afwijkingen in naleving en/of prestaties kunnen optreden.

Doelstelling:

Onafhankelijke assurance (intern of extern) wordt verkregen om te bepalen in hoeverre de informatievoorziening (inclusief IT) voldoet aan relevante wet- en regelgeving; het beleid van de organisatie, de normen en procedures van de organisatie; algemeen aanvaarde werkwijzen; en effectieve en efficiënte prestaties van IT.

Volwassenheidsniveaus:

1	(a) Er vindt geen onafhankelijke assurance plaats.
2	(a) De internal auditfunctie is gedefinieerd en bestaat o.a. uit toetsing op naleving van relevante wet- en regelgeving, IT- of informatiebeleid, standaarden en procedures binnen de organisatie.
3	(a) Onafhankelijke assurance (intern of extern) wordt verkregen ten aanzien van het voldoen van de informatievoorziening (inclusief IT) aan relevante wet- en regelgeving, beleid, standaarden, procedures binnen de organisatie en algemeen aanvaarde werkwerkwijzen. (b) De assurance activiteiten zijn beschreven in een Auditplan dat is goedgekeurd door het (senior) management en een auditcommissie. (c) De resultaten van deze assurance activiteiten worden gerapporteerd aan het (senior) management en de auditcommissie. (d*) Ingevulde checklists die worden gebruikt bij de controle zijn beschikbaar.
4	Aanvullend: (a) De performance van de onafhankelijke assurance wordt periodiek geëvalueerd door de auditcommissie. (b) Het ontwerp van de onafhankelijke assurance functie wordt periodiek geëvalueerd door een externe partij.
5	Aanvullend: (a) Onafhankelijke assurance (intern of extern) omvat ook de effectiviteit en de efficiëntie van de informatieverwerking (inclusief IT).

Referenties:

Normenkader Informatie-beveiliging HO 2015 *06 Controle en Logging*	1.1 1.2 1.4 4.14 6.9
COBIT 4.1	PO6.2 PO9.1
COBIT 5	EDM03.01 EDM03.02 APO01.03 APO12.01 APO12.03
ISO 27K 2013	4.4, 6.1.1 6.1.2 A.5.1.1 A.17.1.1 A.17.1.2 A.18.2.2
DNB 2014/2017	4.1
BIO 2019	5.1.1 5.1.1.1 17.1.1 17.1.2 18.2.2 18.2.2.1
NIST Cybersecurity Framework	ID.GV-1 ID.GV-4 ID.RA-1 ID.RA-2 ID.RA-3 ID.RA-4 ID.RA-5 ID.RA-6 ID.RM-2 RS.IM-1 RS.IM-2

Organisatie

2.1 (OR.01) Eigenaarschap, rollen, verantwoording en verantwoordelijkheid

Risico:

Onduidelijke of dubbelzinnige toewijzing van eigenaarschap, rollen, verantwoordelijkheden of aansprakelijkheid kunnen effectieve besluitvorming, management en rapportage over informatiebeveiliging met betrekking tot bedrijfsvereisten/bedrijfsrisico's in gevaar brengen.

Doelstelling:

Informatiebeveiliging wordt gemanaged op alle toepasselijke organisatieniveaus en Security (of Information Risk) Management wordt gemanaged in overeenstemming met business requirements/risico's. Eigenaarschap, rollen, verantwoordelijkheden en aansprakelijkheid zijn formeel toegewezen en ingebed in de organisatie.

Volwassenheidsniveaus:

1	(a) Eigenaarschap, rollen en verantwoordelijkheden zijn niet toegewezen. (b) Er zijn enkele rollen te onderscheiden die informeel worden uitgevoerd.
2	(a) Rollen die cruciaal zijn voor het managen van informatierisico's zijn benoemd en toegewezen, inclusief specifieke verantwoordelijkheid en aansprakelijkheid voor informatiebeveiliging en/of cyber security, fysieke veiligheid en het voldoen aan wet- en regelgeving.
3	(a) Alle rollen op het gebied van het managen van informatierisico's zijn vastgesteld en toegewezen. (b) De verantwoordelijkheid (en aansprakelijkheid) voor Information Risk en Security Management is op organisatieniveau vastgesteld en behandelt organisatiebrede kwesties. (c) Er is een intentieverklaring van het senior management, die de doelen en uitgangspunten van informatiebeveiliging en Information Risk Management ondersteunen en deze is in overeenstemming met de strategie en de organisatiedoelstellingen. (d*) De governancestructuur is gedocumenteerd met daarin opgenomen de verantwoordelijkheden en rapportagestructuur.
4	(a) Eigenaarschap, verantwoordelijkheid en aansprakelijkheid voor IT-gerelateerde risico's zijn in de organisatie op senior management niveau ingebed. (b) Bijkomende verantwoordelijkheden voor (Information) Security Management kunnen op een systeemspecifiek niveau worden toegewezen (het juiste niveau kan worden bepaald met bijvoorbeeld een RACI matrix). (c) Eigenaarschap, rollen, verantwoordelijkheden en aansprakelijkheid worden periodiek geëvalueerd. (d*) Informatie waaruit de verantwoordelijkheden en bevoegdheden van de beveiligingsfunctionarissen blijkt.
5	Aanvullend: (a) Het senior management bepaalt formeel de risicobereidheid voor informatierisico's en de acceptatie van restrisico's.

Referenties:

Normenkader Informatie-beveiliging HO 2015 ***01 Beleid en Organisatie***	1.3 1.5 6.9
COBIT 4.1	PO9.4
COBIT 5	APO12.02 APO12.04
ISO 27K 2013	4.4 6.1.2 6.1.3 A.5.1.2 A.6.1.5 A.17.1.1 A.18.2.2
DNB 2014/2017	4.2
BIO 2019	5.1.2 5.1.2.1 6.1.5 17.1.1 18.2.2 18.2.2.1 18.2.2.2
NIST Cybersecurity Framework	ID.GV-1 ID.GV-4 ID.RA-1 ID.RA-2 ID.RA-3 ID.RA-4 ID.RA-5 ID.RA-6 ID.RM-2 RS.IM-1 RS.IM-2 RS.MI-3 RC.CO-1 RC.CO-2

Organisatie

2.2 (OR.02) Functiescheiding

Risico:

Acties van eenlingen (bijvoorbeeld ongeautoriseerde toegang tot gegevens) kunnen zich voordoen in belangrijke (IT-)processen, wat kan resulteren in een negatieve impact op bedrijfsprocessen, bijvoorbeeld het risico van nalatig of opzettelijk misbruik van het systeem.

Doelstelling:

Rollen en verantwoordelijkheden zijn gescheiden om de kans te verkleinen dat individuele personen kritieke processen in gevaar brengen. Het personeel voert alleen geautoriseerde taken uit die bij hun respectievelijke functies en rol horen.

Volwassenheidsniveaus:

1	(a) Er vindt geen of nagenoeg geen functiescheiding plaats.
2	(a) Rollen en verantwoordelijkheden zijn gescheiden. (b) Hoe deze rollen en verantwoordelijkheden worden gescheiden is niet formeel vastgelegd en/of afgestemd met het (senior) management.
3	(a) De scheiding van rollen en verantwoordelijkheden is gedefinieerd en grotendeels geïmplementeerd, wat de kans verkleint dat individuen essentiële processen kunnen compromitteren. (b) De scheiding van verantwoordelijkheden is goedgekeurd door het (senior) management. (c) Vastgestelde functiescheiding is geïmplementeerd zodat personeel alleen geautoriseerde handelingen kan verrichten die behoren bij hun werkzaamheden.
4	(a) Een functiescheiding conflict matrix is gedefinieerd en wordt periodiek (d.m.v. GRC tooling) getoetst aan de werkelijke implementatie van systemen en processen. (b) Deze functiescheiding conflict matrix wordt op zijn minst geëvalueerd na grote wijzigingen in processen of systemen. (c) De implementatie en uitvoering van relevante procedures worden periodiek geëvalueerd.
5	Aanvullend: (a) Periodiek worden er database checks uitgevoerd om de huidige processen te toetsen in relatie tot de functiescheidingsmatrix, waarbij er gekeken wordt naar ongebruikelijk transacties/gebieden voor verbetering (bijv. d.m.v. process mining technieken).

Referenties:

Normenkader Informatie-beveiliging HO 2015 ***01 Beleid en Organisatie***	1.5 1.6 1.14 1.16 3.1 3.9 3.13 4.2 4.8 4.11
COBIT 4.1	PO9.6
COBIT 5	APO12.04 APO12.05 APO12.06
ISO 27K 2013	6.1.3 A.6.2.1 A.6.1.5 A.8.1.3 A.11.2.1 A.11.2.6 A.12.1.4 A.12.6.1 A.14.1.1 A.15.1.1 A.15.1.3 A.15.2.2
DNB 2014/2017	4.3
BIO 2019	6.2.1 6.2.1.1 6.2.1.2 6.1.5 8.1.3 8.1.3.1 8.1.3.2 11.2.1 11.2.6 12.1.4 12.1.4.1 12.1.4.2 12.6.1 12.6.1.1 14.1.1 14.1.1.1 15.1.1 15.1.1.1 15.1.1.2 15.1.1.3 15.1.3 15.1.3.1 15.2.2
NIST Cybersecurity Framework	ID.GV-1 ID.GV-4 ID.RA-1 ID.RA-2 ID.RA-3 ID.RA-4 ID.RA-5 ID.RA-6 ID.RM-2 RS.IM-1 RS.IM-2

Risk Management

3.1 (RM.01) Framework voor Information Risk Management

Risico:

Het framework voor Information Risk en Control Management is niet in lijn met het organisatiebrede model voor risicomanagement, resulterend in verkeerde interpretaties van risico's en/of het niet voldoen aan bedrijfs- en IT-doelstellingen.

Doelstelling:

Er is een framework voor Information Risk Management opgesteld en afgestemd op de doelstellingen van de organisatie en het framework voor (enterprise) Risk Management.

Volwassenheidsniveaus:

1	(a) Informatierisico's zijn niet of worden ad hoc bepaald. (b) Er is geen risico framework voor Information Risk Management en geen Information Risk Management proces.
2	(a) Beleid voor Information Risk Management en een Information Risk Management proces zijn opgesteld; meestal op een hoog abstractieniveau en wordt alleen toegepast bij grote projecten of als reactie op problemen. (b) Er is een beknopt framework voor Information Risk Management en risicobereidheid is op een hoog niveau bepaald. Deze zijn in beperkte mate in lijn met de organisatiedoelstellingen en bedrijfsrisico's.
3	(a) Er is organisatiebreed beleid voor Information Risk Management dat is goedgekeurd door het senior management. (b) Het beleid en de procesbeschrijving geven aan hoe om te gaan met de essentiële elementen van Risk Management (risicobereidheid/-profiel, risico-eigenaarschap, risicoproces, risicobeoordeling, risicomitigatie en risicoacceptatie). (c) Het framework voor Information Risk Management is in lijn met het framework voor organisatiebreed Risk Management en omvat componenten als strategie, programma's, projecten en uitvoering. (d) Classificatie van informatierisico's gebeurt op basis van een set van algemeen geldende karakteristieken vanuit het framework voor organisatiebreed Risk Management en getroffen maatregelen voor informatierisico's zijn gestandaardiseerd en geprioriteerd, waarbij rekening gehouden wordt met kans, impact en restrisico's. (e) Training in het kader van dit framework is geïmplementeerd. (f*) Beschrijving methode voor: Data Protection Impact Assessment (DPIA).
4	Aanvullend: (a) Het framework voor Information Risk Management en hoe de daaraan verbonden processen in de praktijk functioneren worden periodiek geëvalueerd. (b) Periodiek wordt gerapporteerd over (het framework voor) Information Risk Management, waardoor het management risico's kan monitoren en op basis daarvan overwogen besluiten kan nemen over welke risico's ze accepteert.
5	Aanvullend: (a) Het framework voor Information Risk Management focust ook op efficiëntie-aspecten van primaire bedrijfsvoering. (b) Information Risk Management is volledig geïntegreerd in alle IT- en bedrijfsvoering, wordt volledig geaccepteerd en betrekt hierin personeel en leveranciers. (c) Het framework voor Information Risk Management en de daaraan verbonden processen worden voortdurend verbeterd.

Referenties:

Normenkader Informatie-beveiliging HO 2015 ***01 Beleid en Organisatie***	1.5 4.10 6.4 6.5 6.6
COBIT 4.1	PO8.3 AI2.5 AI2.7 AI2.8
COBIT 5	APO11.02 APO11.05 BAI03.02 BAI03.03 BAI03.05 BAI03.06 BAI03.09
ISO 27K 2013	8.1 A.6.1.5 A.14.2.1 A.14.2.2 A.14.2.5 A.14.2.6 A.14.2.7 A.14.2.8 A.14.2.9
DNB 2014/2017	10.5 16.1
BIO 2019	6.1.5 14.2.1 14.2.1.1 14.2.2 14.2.2.1 14.2.5 14.2.5.1 14.2.6 14.2.6.1 14.2.7 14.2.7.1 14.2.8 14.2.9 14.2.9.1 14.2.9.2
NIST Cybersecurity Framework	RS.AN-1 RS.AN-2

Risk Management

3.2 (RM.02) Risicobeoordeling

Risico:

Inherente en restrisico's worden niet (tijdig) geïdentificeerd en beoordeeld. Kans en impact zijn niet vastgesteld, waardoor actieplannen, beperkende maatregelen of risico-initiatieven niet worden ingevoerd.

Doelstelling:

Risicobeoordelingen worden uitgevoerd om actuele risicoprofielen met betrekking tot bedrijfsdoelstellingen te bepalen. De waarschijnlijkheid en impact van alle geïdentificeerde risico's worden regelmatig beoordeeld, met behulp van kwalitatieve en kwantitatieve methoden. De waarschijnlijkheid en impact van inherente en restrisico's worden bepaald per categorie, op portefeuillebasis.

Volwassenheidsniveaus:

1	(a) Risicoanalyses worden zelden gedaan en zijn afhankelijk van individuen. (b) Soms worden risicoanalyses uitgevoerd als onderdeel van een projectplan.
2	(a) Risicoanalyses worden uitgevoerd als onderdeel van het Risk Management proces, en risico's worden kwalitatief of kwantitatief geïdentificeerd. (b) De kans en/of impact wordt vooral bepaald op basis van algemene criteria, niet volledig in lijn met de bedrijfsdoelen. (c) Risicoanalyses worden (als onderdeel van een project) beknopt gedocumenteerd.
3	(a) Door duidelijke en passende instructies vinden risicoanalyses consistent en herhaaldelijk plaats, als onderdeel van het Risk Management proces en het framework voor Information Risk Management. (b) De risicoanalysemethodiek is in lijn met bedrijfsbehoeften en identificeert belangrijke bedrijfsrisico's (inclusief kroonjuwelen). (c) De geïdentificeerde informatierisico's worden kwalitatief en/of kwantitatief beoordeeld gebruikmakend van het Risk Management proces/framework of good practice bronnen. (d) Afwijkingen van de risicobereidheid of het risicoprofiel met betrekking tot risico beperkende maatregelen worden aan het (senior) management gerapporteerd.
4	Aanvullend: (a) De correlatie tussen de geïdentificeerde risico's wordt geanalyseerd en gedocumenteerd. Zo zouden de resultaten van de cybersecurity threat analysis opgenomen kunnen worden in de overall risk heat map. (b) De risicoanalysemethodiek wordt periodiek geëvalueerd.
5	Aanvullend: (a) De risicoanalysemethodiek wordt ondersteund door geautomatiseerde tools, workflow processing en geïntegreerde dashboards.

Referenties:

Normenkader Informatie-beveiliging HO 2015 ***01 Beleid en Organisatie***	1.4 1.7 1.8
COBIT 4.1	PO4.9
COBIT 5	APO01.06
ISO 27K 2013	A.6.1.1 A.8.1.2 A.8.2.1 A.8.2.2 A.8.2.3
DNB 2014/2017	6.1
BIO 2019	6.1.1 6.1.1.1 6.1.1.2 6.1.1.3 6.1.1.4 8.1.2 8.2.1 8.2.1.1 8.2.2 8.2.3
NIST Cybersecurity Framework	PR.DS-1 PR.DS-2 PR.DS-5 PR.IP-6

Risk Management

3.3 (RM.03) Plan voor behandeling en beperking van risico's (inclusief risicoacceptatie)

Risico:

Risicobeperkende maatregelen worden niet geïdentificeerd en geïmplementeerd. Vereiste acties worden niet gecommuniceerd en uitgevoerd, wat leidt tot mogelijke manifestatie van risico's. Hoge kosten/lage baten gerelateerd aan matige of lage risico's. Het niet prioriteren van risico's kan leiden tot hogere kosten, lagere uitkeringen of reputatieschade.

Doelstelling:

Beheersactiviteiten worden op alle niveaus geprioriteerd en gepland om de benodigde mitigerende maatregelen te implementeren, inclusief het bepalen van kosten en baten en de verantwoordelijkheid voor de uitvoering. Goedkeuring wordt verkregen voor aanbevolen acties en acceptatie van restrisico's en er wordt voor gezorgd dat uitgevoerde acties onder verantwoordelijkheid van betrokken proceseigenaar(s) vallen. De uitvoering van plannen wordt bewaakt en eventuele afwijkingen worden gerapporteerd aan het senior management.

Volwassenheidsniveaus:

1	(a) Er is geen plan voor het aanpakken of mitigeren van risico's. (b) Als een risico wordt geïdentificeerd, worden de risicobeperkende maatregelen op inconsistente manier toegepast. Dit is afhankelijk van individuele competenties.
2	(a) Plannen voor het aanpakken en mitigeren van risico's zijn gemaakt, maar niet formeel vastgelegd. (b) Risicobeperkende maatregelen zijn onvolledig en niet geformaliseerd/goedgekeurd, en eigenaarschap is slechts gedeeltelijk toegewezen aan risicomaatregelen of geaccepteerde risico's.
3	(a) Er is een proces geïmplementeerd om risico's formeel vast te leggen en op te nemen in een risico-actieplan. (b) Overgebleven risico's en maatregelen zijn geïdentificeerd, geanalyseerd en gedocumenteerd (in een risicoregister of -actieplan). (c) De geïdentificeerde maatregelen of acceptatie van restrisico's zijn gedocumenteerd, goedgekeurd door het (senior) management en toegewezen aan een (risico)eigenaar. (d) De voortgang van implementatie van risicobeperkende maatregelen en eventuele afwijkingen worden gemonitord. (e) Het risico-actieplan wordt onderhouden en aangepast indien nodig. Het senior management is eigenaar van het risico-actieplan.
4	Aanvullend: (a) Indien van toepassing wordt de prioritering van risicobeperkende maatregelen en argumenten voor risico-acceptatie heroverwogen. (b) Geïdentificeerde risicoreacties geven ook inzicht in de kosten en baten daarvan, inclusief bewaking van het budget. (c) De operationele effectiviteit van het Risk Management proces wordt regelmatig geëvalueerd.
5	Aanvullend: (a) Het documenteren, analyseren, bewaken en rapporteren van Risk Management data gebeurt (grotendeels) geautomatiseerd. (b) Strategieën voor het mitigeren van risico's worden voortdurend door het senior management geëvalueerd.

Referenties:

Normenkader Informatie-beveiliging HO 2015 ***01 Beleid en Organisatie***	1.7 5.1
COBIT 4.1	PO2.3
COBIT 5	APO03.02
ISO 27K 2013	8.2.1 8.3.1 9.1.1
DNB 2014/2017	2.2
BIO 2019	8.2.1 8.2.1.1 8.3.1 8.3.1.1 8.3.1.2 9.1.1 Supplement BIG 7.2.1.2
NIST Cybersecurity Framework	DE.AE-1

Personeelsbeheer

4.1 (HR.01) Werving

Risico:

Als het wervingsproces ontoereikend is, loopt de organisatie het risico dat werknemers onjuist gekwalificeerd of niet gescreend zijn.

Doelstelling:

Rekruteringsprocessen voor personeel worden onderhouden in overeenstemming met het algemene personeelsbeleid en de procedures van de organisatie (bijvoorbeeld werving, positieve werkomgeving, oriëntatie, enz.). Processen worden geïmplementeerd om ervoor te zorgen dat de organisatie beschikt over geschikt (IT-) personeel, met de vaardigheden die nodig zijn om de organisatiedoelen te bereiken. Screening maakt deel uit van het rekruteringsproces. De mate en frequentie waarmee deze screening wordt uitgevoerd, worden bepaald door hoe gevoelig en/of cruciaal de functie is en worden geïmplementeerd voor werknemers, aannemers en leveranciers.

Volwassenheidsniveaus:

1	(a) Activiteiten of maatregelen voor het werven van (IT) personeel zijn ad hoc geïmplementeerd en/of uitgevoerd.
2	(a) Wervingsprocessen voor (IT-)personeel zijn gedefinieerd en geïmplementeerd. (b) Er zijn processen geïmplementeerd om te garanderen dat het (IT) personeel van de organisatie goed is toegerust. (c) Af en toe wordt screening toegepast in het wervingsproces, maar dit is niet formeel vastgelegd.
3	(a) Wervingsprocessen voor (IT) personeel zijn vastgelegd en geïmplementeerd, conform het algemene personeelsbeleid en procedures (bijv. aanname, positieve werkomgeving, oriëntatie). (b) Er zijn processen geïmplementeerd om te garanderen dat het (IT) personeel goed is toegerust om bedrijfsdoelen te behalen. (c) Screening is onderdeel van het wervingsproces voor (IT) personeel. Hoe grondig en vaak deze screening wordt geëvalueerd is afhankelijk van de gevoeligheid/het belang van de functie. De screening vindt plaats voor personeel, aannemers en leveranciers. (d) De processen zijn goedgekeurd door het (senior) management.
4	Aanvullend: (a) De implementatie en effectiviteit van relevante wervingsprocedures en functieomschrijvingen worden periodiek geëvalueerd.
5	Aanvullend: (a) Op basis van de periodieke (zelf)evaluaties of risicoanalyses worden de implementatie en het ontwerp van de wervingsprocessen verbeterd. (b) Tekortkomingen in het wervingsproces worden gerapporteerd aan het (senior) management.

Referenties:

Normenkader Informatie-beveiliging HO 2015 ***02 Personeel, Studenten en Gasten***	1.5 6.9
COBIT 4.1	DS5.5
COBIT 5	APO01.04 DSS05.07 MEA03.02
ISO 27K 2013	A.6.1.5 A.18.2.2
DNB 2014/2017	1.1 3.2
BIO 2019	6.1.5 18.2.2 18.2.2.1
NIST Cybersecurity Framework	ID.BE-1 ID.GV-1 ID.GV-2 ID.GV-3

Personeelsbeheer

4.2 (HR.02) Certificering, training en scholing

Risico:

Gebrek aan professionele training van (IT-) personeel kan leiden tot een te kort aan competenties waardoor bijvoorbeeld onnodige overuren, onjuiste operationele procedures, inefficiënt projectmanagement, inbreuken op informatiebeveiliging, grote incidenten en bedrijfsonderbrekingen kunnen optreden.

Doelstelling:

Opleiding, training en/of ervaring worden regelmatig getoetst om te zien of het personeel over de benodigde competenties beschikt om taken naar behoren te vervullen. Basis (IT-)competenties zijn vastgesteld en, indien nodig, worden kwalificatie- en certificeringsprogramma's gebruikt om te controleren of ze worden bijgehouden.

Volwassenheidsniveaus:

1	(a) Training en educatie wordt ad hoc geïmplementeerd. (b) Er is geen certificering van personeel.
2	(a) Processen voor certificering, training en educatie worden geïmplementeerd. (b) Er zijn individuele persoonlijke ontwikkelplannen beschikbaar.
3	(a) Processen voor training en educatie zijn geïmplementeerd en worden uitgevoerd. (b) Er zijn individuele persoonlijke ontwikkelplannen beschikbaar. (c) Educatie, training en/of ervaring worden gebruikt om regelmatig te verifiëren of personeel over de benodigde vaardigheden beschikt. (d) De relevante processen zijn goedgekeurd door het (senior) management.
4	Aanvullend: (a) De benodigde core (IT-)vaardigheidseisen zijn gedefinieerd en waar gepast worden kwalificatie- en certificeringprogramma's gebruikt om te zorgen dat deze worden onderhouden. (b) Er is toezicht op de realisatie van persoonlijke ontwikkelplannen.
5	Aanvullend: (a) De implementatie van de processen voor certificering, training en educatie wordt jaarlijks geëvalueerd, waarbij educatie- en trainingsmaterialen worden gecheckt op relevantie, kwaliteit en effectiviteit.

Referenties:

Normenkader Informatie-beveiliging HO 2015 ***02 Personeel, Studenten en Gasten***	1.13 1.15 1.16 4.11 6.4 6.7
COBIT 4.1	DS1.3 DS1.5
COBIT 5	APO09.04 APO09.05
ISO 27K 2013	8.1 A.13.2.2 A.14.2.7 A.15.1.1 A.15.1.2 A.15.1.3 A.15.2.1 A.15.2.2
DNB 2014/2017	14.1
BIO 2019	13.2.2 14.2.7 14.2.7.1 15.1.1 15.1.1.1 15.1.1.2 15.1.1.3 15.1.2 15.1.2.1 15.1.2.2 15.1.2.3 15.1.2.4 15.1.2.5 15.1.2.6 15.1.3 15.1.3.1 15.2.1 15.2.1.1 15.2.2 Supplement BIG: 6.2.1.7
NIST Cybersecurity Framework	ID.SC-1 ID.SC-2 ID.SC-3 ID.SC-4 ID.SC-5

Personeelsbeheer

4.3 (HR.03) Afhankelijkheid van individuen

Risico:

Afhankelijkheid van sleutelfiguren brengt risico's met zich mee als deze personen vertrekken of langere tijd niet inzetbaar zijn, als een belangrijk ontwikkelteam de organisatie verlaat of als het niet mogelijk is om IT-personeel te werven.

Doelstelling:

Er is een opvolgingsplanning en back-upplan voor vitale medewerkers en afdelingen.

Volwassenheidsniveaus:

1	(a) Opvolgings- en back-upplannen zijn niet geïmplementeerd. (b) Single points of failure met betrekking tot het personeel zijn niet geïdentificeerd.
2	(a) Back-up en vervanging van belangrijke medewerkers/functies worden op afdelingsniveau geregeld.
3	(a) Opvolgingsplanning, job rotatie en back-up van het personeel zijn geïmplementeerd. (b) Er zijn trainingsprogramma's om het risico van een te grote afhankelijkheid van sleutelfiguren te verkleinen. (c) De meeste sleutelfuncties/posities zijn geïdentificeerd en formeel gedefinieerd door het (senior) management.
4	Aanvullend: (a) Alle belangrijke/kritieke personen en/of afdelingen zijn in de hele organisatie geïdentificeerd en/of worden periodiek geëvalueerd.
5	Aanvullend: (a) De effectiviteit van het proces voor de planning van opvolging en back-up van personeel wordt periodiek geëvalueerd. (b) De planning voor opvolging is in overeenstemming met de bedrijfs- en IT-strategie.

Referenties:

Normenkader Informatie-beveiliging HO 2015 ***02 Personeel, Studenten en Gasten***	NVT
COBIT 4.1	PO2.1
COBIT 5	APO03.01 APO03.02 APO03.04
ISO 27K 2013	A.14.2.5
DNB 2014/2017	2.1 3.1
BIO 2019	14.2.5 14.2.2.1
NIST Cybersecurity Framework	

Personeelsbeheer

4.4 (HR.04) Verandering of beëindiging van functie

Risico:

Gebruikerstoegang wordt niet tijdig uitgeschakeld nadat medewerkers het team hebben verlaten of om een andere reden geen toegang meer mogen hebben.
Door gebrekkige kennisoverdracht wordt de continuïteit van de functie bedreigd.

Doelstelling:

Wanneer er functiewijzigingen plaatsvinden, met name beëindiging van het dienstverband, wordt direct effectief actie ondernomen. Kennisoverdracht wordt geregeld, verantwoordelijkheden worden opnieuw toegewezen en toegangsrechten worden verwijderd, zodat risico's worden geminimaliseerd en de continuïteit van de functie wordt gewaarborgd.

Volwassenheidsniveaus:

1	(a) Wanneer er functiewijzigingen of ontslagen plaatsvinden worden er geen of ad-hoc-acties ondernomen.
2	(a) Toegangsrechten van werknemers worden gewijzigd, opnieuw toegewezen en/of verwijderd op basis van functiewijziging en/of ontslag, maar het tijdig intrekken van toegangsrechten is niet gewaarborgd.
3	(a) Goedgekeurde processen zijn geïmplementeerd om kennis over te dragen en toegangsrechten opnieuw toe te wijzen of in te trekken. (b) Kennisoverdracht is geregeld, verantwoordelijkheden zijn opnieuw toegewezen en toegangsrechten worden tijdig ingetrokken zodat risico's zijn geminimaliseerd en de continuïteit van de functie wordt gewaarborgd. (c) De stappen van functieoverdracht zijn vastgelegd.
4	Aanvullend: (a) Er worden ontslaggesprekken gevoerd en de juistheid en tijdigheid van veranderingen, opnieuw toewijzen of intrekken van toegangsrechten worden periodiek geëvalueerd.
5	Aanvullend: (a) De effectiviteit van de processen voor functiewijzigingen en/of ontslag wordt periodiek geëvalueerd en verbeterd.

Referenties:

Normenkader Informatie-beveiliging HO 2015 ***02 Personeel, Studenten en Gasten***	1.3 6.2 6.9 6.10
COBIT 4.1	ME4.7
COBIT 5	MEA02.05 MEA02.06 MEA02.07 MEA02.08
ISO 27K 2013	A.5.1.2 A.12.4.1 A.18.2.1 A.18.2.2 A.18.2.3
DNB 2014/2017	16.5
BIO 2019	5.1.2 5.1.2.1 12.4.1 12.4.1.1 12.4.1.2 12.4.1.3 12.4.1.4 12.4.1.5 18.2.1 18.2.1.1 18.2.1.2 18.2.2 18.2.2.1 18.2.3 18.2.3.1
NIST Cybersecurity Framework	DE.DP-2 DE.DP-3 DE.DP-4 DE.DP-5

Personeelsbeheer

4.5 (HR.05) Kennisdeling

Risico:

Het ontbreken van procedures en werkinstructies voor het mogelijk maken van kennisoverdracht leidt tot een ondoelmatig en inefficiënt gebruik van systemen voor het ondersteunen van bedrijfsprocessen. Het kan ook leiden tot ineffectieve en inefficiënte levering, onderhoud en ondersteuning van het systeem en de bijbehorende infrastructuur.

Doelstelling:

Overdracht van kennis en vaardigheden is geregeld, zodat eindgebruikers het systeem effectief en efficiënt kunnen gebruiken om bedrijfsprocessen te ondersteunen. Kennis en vaardigheden worden overgedragen zodat beheerders en technisch ondersteunend personeel het systeem en de bijbehorende infrastructuur op effectieve en efficiënte wijze kunnen leveren, ondersteunen en onderhouden.

Volwassenheidsniveaus:

1	(a) Overdracht van kennis is niet geïmplementeerd of wordt gedaan op ad-hoc basis.
2	(a) Er zijn informele, gedecentraliseerde processen voor kennisoverdracht geïmplementeerd. (b) Kennis en vaardigheden worden vaak overgedragen op individuele basis.
3	(a) Er zijn goedgekeurde processen op organisatieniveau geïmplementeerd om kennis over te dragen en gepaste documentatie-, training- en implementatiematerialen te onderhouden, zodat systemen op effectieve wijze business processen kunnen ondersteunen. Hier zijn zowel eindgebruikers als operationele en technische support bij betrokken.
4	Aanvullend: (a) Er wordt periodiek geëvalueerd of de ondersteunende documentatie toereikend is.
5	Aanvullend: (a) Kennis en vaardigheden worden overgedragen zodat eindgebruikers het systeem op efficiënte wijze kunnen gebruiken. (b) Kennis en vaardigheden worden overgedragen om operationele en technische supportpersoneel in staat te stellen om het systeem en haar infrastructuur efficiënt te kunnen leveren, ondersteunen en onderhouden.

Referenties:

Normenkader Informatie-beveiliging HO 2015 ***02 Personeel, Studenten en Gasten***	1.3 6.1
COBIT 4.1	DS5.4
COBIT 5	DSS05.04
ISO 27K 2013	A.5.1.2 A.9.2.5
DNB 2014/2017	17.2
BIO 2019	5.1.2 5.1.2.1 9.2.5 9.2.5.1 9.2.5.2 9.2.5.3
NIST Cybersecurity Framework	PR.AC-1 PR.AC-3

Personeelsbeheer

4.6 (HR.06) Veiligheidsbewustzijn

Risico:

Mensen die zich onvoldoende bewust zijn van informatiebeveiligingsrisico's begrijpen de mogelijke gevolgen van hun acties niet en kunnen die niet bij het uitvoeren van hun taken betrekken.

Doelstelling:

Er is een security-awareness programma om gebruikers bewust te maken van hun verantwoordelijkheid om de vertrouwelijkheid, beschikbaarheid en integriteit van informatie (middelen) te beschermen.

Volwassenheidsniveaus:

1	(a) Er zijn geen security-awareness activiteiten gedefinieerd of uitgevoerd.
2	(a) Security-awareness activiteiten worden uitgevoerd op afdelingsniveau.
3	(a) Er is een security-awareness programma opgenomen in het informatiebeveiligingsplan en wordt organisatiebreed uitgevoerd. (b) Het programma is in lijn met het (informatie)beveiligingsbeleid.
4	Aanvullend: (a) security-awareness activiteiten bevatten een verplicht e-learning programma dat succesvol moet worden volbracht, inclusief online examen. (b) Afronding van e-Learning modules door medewerkers wordt bewaakt en gerapporteerd aan het senior management.
5	Aanvullend: (a) De effecten van de security-awareness activiteiten worden gemonitord. (b) Correlatie van beveiligingsincidenten als gevolg van gebrek aan awareness leidt tot aanpassing van de beveiliging-awareness activiteiten.

Referenties:

Normenkader Informatie-beveiliging HO 2015 ***02 Personeel, Studenten en Gasten***	5.12 6.2 6.3
COBIT 4.1	DS5.5
COBIT 5	DSS05.04 DSS05.07
ISO 27K 2013	A.12.4.1 A.12.4.2 A.12.4.3
DNB 2014/2017	16.1
BIO 2019	12.4.1 12.4.1.1 12.4.1.2 12.4.1.3 12.4.1.4 12.4.1.5 12.4.2 12.4.2.1 12.4.2.2 12.4.2.3 12.4.2.4 12.4.3
NIST Cybersecurity Framework	PR.PT-1 DE.AE-2 DE.AE-3 DE.AE-4 DE.AE-5 DE.CM-1 DE.CM-2 DE.CM-3 DE.CM-7

Configuration Management

5.1 (CO.01) Identificatie en onderhoud van configuratie-items

Risico:

Verstoringen in de bedrijfsvoering als gevolg van ongeautoriseerde en ongedocumenteerde configuratiewijzigingen in de IT-omgeving, gebrek aan traceerbare bronnen tijdens de root-cause analyse, ondoelmatige afstemming op andere processen en het niet in staat zijn verantwoordelijke belanghebbenden te traceren.

Doelstelling:

Er zijn configuratieprocedures vastgesteld om het beheer en loggen van alle wijzigingen in de configuratiedatabase te ondersteunen. Deze procedures zijn in overeenstemming met (en een voorwaarde voor) procedures voor Change, Incident- en Problem Management.

Volwassenheidsniveaus:

1	(a) Er is geen configuratieprocedure. (b) Werkwijzen en procedures worden uitsluitend individueel toegepast en verschillen per platform.
2	(a) Er is een configuratieprocedure vastgesteld om configuratie-items te identificeren en te onderhouden, maar deze procedure is niet geformaliseerd. (b) De data-inhoud van geregistreerde items wordt niet gebruikt door gerelateerde processen zoals Change, Incident- en Problem Management,
3	(a) Er bestaan geformaliseerde configuratieprocedures en werkmethoden om alle configuratie-items en hun attributen te identificeren en te onderhouden. (b) De procedure is afgestemd met procedures voor Change, Incident- en Problem Management. (c) De procedure is gedocumenteerd, gestandaardiseerd en gecommuniceerd. (d) Er is beleid voor het labelen van fysieke bedrijfsmiddelen en nieuwe bedrijfsmiddelen worden geregistreerd in het inkoopproces. (e) Er zijn processen geïmplementeerd voor het beheer van aangeschafte, toegewezen, gearchiveerde en verlopen licenties, die ervoor zorgen dat aan de licentie voorwaarden/afspraken voldaan wordt.
4	Aanvullend: (a) Er is een proces voor het periodiek evalueren van relevante documentatie, tijdige uitvoering en integriteit van het configuratie database (inclusief licenties). (b) De implementatie en uitvoering van relevante procedures ten aanzien van Configuration Management worden periodiek geëvalueerd. (c) Er wordt regelmatig aan het management gerapporteerd, wat leidt tot verbeterplannen. (d) Procedures en standaarden zijn onderdeel van training.
5	Aanvullend: (a) Er wordt voortdurend geanalyseerd of er afwijkingen zijn en gevonden afwijkingen worden onderzocht. (b) Gebreken en trends worden gerapporteerd aan het management. (c) Gerelateerde processen zijn volledig geïntegreerd, en configuratiedata wordt geautomatiseerd gebruikt en actueel gehouden.

Referenties:

Normenkader Informatie-beveiliging HO 2015 ***04 Continuïteit***	2.6 4.8 4.9 4.12 5.12 6.2 6.3 6.5 6.10
COBIT 4.1	DS5.5
COBIT 5	DSS05.04 DSS05.07
ISO 27K 2013	A.12.4. A.12.4.2 A.12.4.3 A.12.7.1 A.12.6.1 A.12.6.2 A.14.2.8 A.16.1.3 A.16.1.4 A.18.2.1 A.18.2.3
DNB 2014/2017	16.1
BIO 2019	12.4.1 12.4.1.1 12.4.1.2 12.4.1.3 12.4.1.4 12.4.1.5 12.4.2 12.4.2.1 12.4.2.2 12.4.2.3 12.4.2.4 12.4.3 12.7.1 12.6.1 12.6.2 12.6.2.1 14.2.8 16.1.3 16.1.3.1 16.1.4 16.1.4.1 18.2.1 18.2.1.1 18.2.1.2 18.2.3 18.2.3.1
NIST Cybersecurity Framework	PR.PT-1 DE.AE-2 DE.AE-3 DE.AE-4 DE.AE-5 DE.CM-1 DE.CM-2 DE.CM-3 DE.CM-7

Configuration Management

5.2 (CO.02) Configuratiedatabase en baseline

Risico:

Zonder snelle detectie en correctie van onjuiste configuraties die de prestaties of integriteit negatief kunnen beïnvloeden, tasten de systeembetrouwbaarheid van de organisatie aan.

Doelstelling:

Een supporttool en een centrale opslag zijn ingericht voor alle relevante informatie over configuratie-items. Alle middelen en wijzigingen aan deze middelen worden gemonitord en vastgelegd. Na wijzigingen wordt voor ieder systeem en elke dienst als benchmark een baseline van configuratie-items geïmplementeerd.

Volwassenheidsniveaus:

1	(a) Basistaken op het gebied van Configuration Management, zoals het identificeren en bijhouden van een inventaris van configuratie-items, worden op ad-hoc basis uitgevoerd. (b) De documentatie van de configuratie is onvolledig en onbetrouwbaar.
2	(a) Configuration Management tools worden soms gebruikt, maar er is geen standaard. (b) Geïnstalleerde software, configuraties en documentatie worden geregistreerd, maar de gegevensinhoud van opgenomen items is beperkt.
3	(a) Alle middelen en wijzigingen in middelen worden gemonitord en vastgelegd in een centrale repository. (b) De relaties tussen configuratie-items worden geïdentificeerd en bijgehouden. (c) Een tool voor Configuration Management (of gelijksoortige tools) wordt (worden) geïmplementeerd voor alle platforms. (d) Er wordt enige automatisering ter ondersteuning gebruikt bij het volgen van wijzigingen in apparatuur en software. (e) Configuratie baselines voor componenten worden vastgesteld en gedocumenteerd als benchmark na wijzigingen. (f) Wijzigingen in de configuratiedatabase (CMDB) worden geregistreerd.
4	(a) Er worden geautomatiseerde tools voor het bijhouden van veranderingen in apparatuur en software gebruikt om de standaarden te handhaven en de stabiliteit te verbeteren. (b) Er zijn mechanismen om wijzigingen te toetsen aan wat is vastgelegd in de repository en aan de gedefinieerde baseline. (c) Periodiek worden fysieke controles uitgevoerd. (d) Wijzigingen die in de configuratiedatabase worden geregistreerd, worden periodiek geanalyseerd. (e) Er wordt periodiek aan het management gerapporteerd.
5	(a) Alle IT-middelen worden in een centrale Configuration Management database beheerd. Dit systeem bevat alle benodigde informatie over componenten en hun onderlinge relaties, alsmede informatie over reparatie, service, garantie, upgrades en technische assessments. (b) Processen en automatisering voor software en hardware Asset Management (inclusief licenties) zijn geïmplementeerd. (c) Het management ontvangt periodiek (geautomatiseerde) rapporten.

Referenties:

Normenkader Informatie-beveiliging HO 2015 ***06 Controle en Logging***	1.15 1.16 4.3 4.4 4.11 6.4 6.7
COBIT 4.1	DS1.5 DS1.6
COBIT 5	APO09.05 APO09.06
ISO 27K 2013	8.1 A.12.2.1 A.14.2.7 A.15.1.1 A.15.1.2 A.15.1.3 A.15.2.1 A.15.2.2
DNB 2014/2017	14.1
BIO 2019	12.2.1 12.2.1.1 12.2.1.2 12.2.1.3 12.2.1.4 12.2.1.5 14.2.7 14.2.7.1 15.1.1 15.1.1.1 15.1.1.2 15.1.1.3 15.1.2 15.1.2.1 15.1.2.2 15.1.2.3 15.1.2.4 15.1.2.5 15.1.2.6 15.1.3 15.1.3.1 15.2.1 15.2.1.1 15.2.2
NIST Cybersecurity Framework	ID.SC-1 ID.SC-2 ID.SC-3 ID.SC-4 ID.SC-5

Incident/Problem Management

6.1 (IM.01) Incident Management

Risico:

Incidenten zijn niet correct geclassificeerd en worden onjuist behandeld in het Incident Management proces, wat uiteindelijk leidt tot verminderde prestaties en kwaliteit van de informatievoorziening.

Doelstelling:

Een formeel Incident Management proces wordt gecommuniceerd en geïmplementeerd. Er zijn procedures ingesteld om ervoor te zorgen dat alle incidenten en storingen worden geregistreerd, geanalyseerd, gecategoriseerd en geprioriteerd naar impact. Alle incidenten worden bijgehouden en periodiek beoordeeld om ervoor te zorgen dat ze tijdig worden verholpen.

Volwassenheidsniveaus:

1	(a) Er is geen beleid voor Incident Management. (b) Er zijn geen rollen en verantwoordelijkheden vastgelegd. (c) Er zijn geen procedures om te garanderen dat alle incidenten en storingen worden gedocumenteerd en geanalyseerd. (d) Incidenten worden bijgehouden en geëvalueerd op individuele basis. (e) Reacties op informatiebeveiligingsincidenten zijn ad hoc.
2	(a) Er is een informeel Incident Management proces vastgesteld om kritische incidenten aan te pakken. (b) Rollen en verantwoordelijkheden zijn gedeeltelijk gedefinieerd. (c) De meeste incidenten worden gedocumenteerd en geanalyseerd, maar afwijkingen van de standaarden worden waarschijnlijk niet gedetecteerd. (d) Er zijn geen criteria bepaald voor het categoriseren en prioriteren van incidenten op basis van impact. (e) Incidenten worden ad hoc toegewezen. Er wordt handmatig en op individuele basis toezicht gehouden. (f) Er is geen formele training en communicatie over de standaardprocedures.
3	(a) Het beleid voor Incident Management is formeel gedocumenteerd en gecommuniceerd. (b) Rollen en verantwoordelijkheden van de organisatie en de leveranciers zijn duidelijk gedefinieerd. (c) Aspecten rondom juridisch en forensisch onderzoek zijn vastgesteld en toegewezen. (d) Het registreren, communiceren, toewijzen en analyseren van/over incidenten is formeel belegd in de organisatie. (e) Incidenten worden gecategoriseerd en geprioriteerd op basis van impact. (f) (Cyber)beveiligingsincidenten worden voorkomen of gedetecteerd en er is een proces om deze tijdig en effectief aan te pakken. (g) Informatie wordt op een proactieve en formele manier gedeeld door personeel. (h) Er wordt gemonitord of incidenten tijdig worden opgelost. (i) Er wordt beperkt gerapporteerd aan het management over incident- en oplossingsanalyses.
4	Aanvullend: (a) Incidenten worden proactief geanalyseerd om oorzaken te achterhalen. (b) Er is een functie (response team) geïmplementeerd om beveiligingscrises te herkennen en te managen. (c) Het Incident Management proces betrekt belangrijke functies binnen de organisatie en bij externe service providers. (d) Op het tijdig aanpakken van incidenten wordt streng toegezien. Onopgeloste incidenten (bekende foutmeldingen waar omheen gewerkt wordt) worden gedocumenteerd en gerapporteerd als input voor Problem Management. (e) De kwaliteit en operationele effectiviteit van het Incident Management proces worden periodiek geëvalueerd. (f*) Er is een overzicht van proces van intake tot afsluiting van een incident. (g*) Er is een procedurebeschrijving en mandatenregeling forensische deskundigen (CSIRT-team).
5	Aanvullend: (a) De registratie, rapportage en analyse van incidenten en oplossingen zijn volledig geautomatiseerd en geïntegreerd met Configuration- en Problem Management. (b) De meeste systemen zijn uitgerust met automatische detectie- en waarschuwingssystemen, die voortdurend gemonitord en beoordeeld worden. (c) Incident Management wordt voortdurend geanalyseerd voor verbetering.

Referenties:

Normenkader Informatie-beveiliging HO 2015 ***04 Continuïteit***	1.15 6.7 6.9
COBIT 4.1	ME2.6
COBIT 5	MEA02.01
ISO 27K 2013	8.1, A.15.1.2 A.15.2.1 A.18.2.2
DNB 2014/2017	16.3 16.4
BIO 2019	15.1.2 15.1.2.1 15.1.2.2 15.1.2.3 15.1.2.4 15.1.2.5 15.1.2.6 15.2.1 15.2.1.1 18.2.2 18.2.2.1
NIST Cybersecurity Framework	ID.SC-1 ID.SC-2 ID.SC-3 ID.SC-4 ID.SC-5 ID-GV.3 PR.AC-3 PR.MA-1 PR.MA-2 DE.CM-6 DE.DP-2 DE.DP-3 DE.DP-4 DE.DP-5

Incident/Problem Management

6.2 (IM.02) Incident escalatie

Risico:

Incidenten worden niet tijdig geïdentificeerd, opgelost, beoordeeld, geëscaleerd en geanalyseerd, wat uiteindelijk leidt tot verminderde prestaties en kwaliteit van de informatievoorziening.

Doelstelling:

Er worden procedures voor Incident Management (of voor de servicedesk) vastgesteld, zodat wanneer incidenten niet binnen de afgesproken termijn kunnen worden opgelost, serviceniveaus adequaat worden geëscaleerd en, indien nodig, wordt voorzien in een tijdelijke oplossing. Eigenaarschap van incidenten en levenscyclusmonitoring blijven de verantwoordelijkheid van de servicedesk voor gebruikersincidenten, ongeacht welke IT-groep aan de oplossing werkt.

Volwassenheidsniveaus:

1	(a) Er is geen beleid om incidenten die niet opgelost kunnen worden tijdig te laten escaleren. (b) Incidenten worden bijgehouden en geëvalueerd op individuele basis. (c) Reacties op verstoringen van informatiebeveiliging zijn onvoorspelbaar. (d) Er is niet vastgelegd wie verantwoordelijk is voor het oplossen van incidenten.
2	(a) Er is een informeel escalatieproces. (b) Incidenten die niet tijdig kunnen worden opgelost worden geëscaleerd. (c) Er zijn geen criteria bepaald voor het prioriteren van incidenten. (d) Er is geen gecentraliseerde kennisbank. (e) Response teams zijn ongetraind en afhankelijk van enkele belangrijke individuen.
3	(a) Het formeel vastgelegde beleid voor Incident Management bevat een escalatieprocedure. (b) Er zijn escalatiecriteria bepaald. (c) De escalatieprocedure is gebaseerd op serviceniveaus voor incidenten die niet meteen opgelost kunnen worden. (d) Categorisering en prioritering vindt plaats op basis van impactanalyse, de bepaalde criteria en serviceniveaus. (e) De response teams krijgen de benodigde training. (f) De verantwoordelijkheid voor het oplossen van een incident is toegewezen.
4	Aanvullend: (a) Advies is consistent en incidenten worden tijdig en volgens een gestructureerde escalatieprocedure opgelost. (b) Belangrijke incidenten worden aan het management gerapporteerd. (c) Escalatieprocedures zijn algemeen bekend, begrepen en toegepast. (d) Response teams krijgen regelmatig training. (e) Het escalatieproces wordt periodiek geëvalueerd.
5	Aanvullend: (a) Het escalatieproces wordt voortdurend geëvalueerd. (b) Het oplossen van incidenten wordt regelmatig geanalyseerd om het proces te verbeteren en tekortkomingen en trends worden aan het management gerapporteerd.

Referenties:

Normenkader Informatie-beveiliging HO 2015 ***04 Continuïteit***	NVT
COBIT 4.1	DS9.1
COBIT 5	BAI10.01 BAI10.02 BAI10.04 DSS02.01
ISO 27K 2013	A.8.1.1 A.8.1.2 A.8.1.3 A.12.6.1
DNB 2014/2017	13.2
BIO 2019	8.1.1 8.1.2 8.1.3 8.1.3.1 8.1.3.2 12.6.1 12.6.1.1
NIST Cybersecurity Framework	ID.AM-1 ID.AM-2 ID.AM-3 ID.AM-4 ID.AM-5

Incident/Problem Management

6.3 (IM.03) Incidentrespons op (cyber) beveiligingsincidenten

Risico:

Het ontbreken van een effectieve en tijdige reactie of follow-up van (cyber)beveiligingsincidenten leidt tot grote verstoringen van de infrastructuur, datalekken of informatiediefstal met financiële en/of imagoschade tot gevolg.

Doelstelling:

De organisatie beschikt over mogelijkheden voor incident response om (cyber-)beveiligingsincidenten snel te detecteren, te isoleren en de impact te beperken en om diensten op een betrouwbare manier te herstellen en weer in de lucht te brengen.

Volwassenheidsniveaus:

1	(a) Er zijn geen plannen/procedures om een gepaste afhandeling van (cyber) beveiligingsincidenten te garanderen. (b) Reacties op (cyber)beveiligingsincidenten vinden vaak op individuele basis plaats.
2	(a) Het management erkent de noodzaak om cyberincidenten af te handelen. (b) Er is een informele procedure voor het afhandelen van (cyber)beveiligingsincidenten. (c) De ontwikkeling van maatregelen voor preventie, aanpak, voorbereid zijn op en het herstellen na een (cyber)beveiligingsincident bevindt zich in een vroeg stadium.
3	(a) Naast de gebruikelijke Incident en Problem Management procedures zijn er ook plannen om preventie, risicobeperking, voorbereiding, tijdige reactie en herstel van (cyber)beveiligingsincidenten aan te pakken. (b) Er zijn rollen en verantwoordelijkheden vastgelegd en toegewezen. (c) De organisatie kan snel reageren op een verstoring, op gepaste schaal/escalatieniveau afhankelijk van mogelijke impact.
4	Aanvullend: (a) Plannen voor coördinatie van incident respons betrekken alle bedrijfsonderdelen, zoals beleid, juridische afdeling, communicatie, compliance en audit en bedrijfsvoering. (b) Er worden relevante relaties onderhouden met externe partijen als politie, CERT en gespecialiseerde bedrijven. (c) Alle (cyber)beveiligingsincidenten worden gemeld bij het management en relevante autoriteiten. (d) Responsplannen zijn gebaseerd op risicoanalyse van de gecompromiteerde data en/of kwetsbaarheidsanalyse. (e*) Aansluiting van incidentmanagement procedures met de procedures van de crisisbeheer organisatie. (f*) Inrichtingsdocumentatie waaruit blijkt dat tool(s) voor afhandeling van beveiligingsincidenten in gebruik zijn (IDS/IPS).
5	Aanvullend: (a) Risico- en trendanalyses worden ingezet om voortdurende verbeteringen in de preventie, aanpak, voorbereiding en herstel van (cyber)beveiligingsincidenten te bewerkstelligen. (b) Het oplossen van (cyber)beveiligingsincidenten wordt regelmatig geanalyseerd om het proces te verbeteren en tekortkomingen worden aan het management gerapporteerd.

Referenties:

Normenkader Informatie-beveiliging HO 2015 ***04 Continuïteit***	NVT
COBIT 4.1	DS13.1 DS13.2
COBIT 5	DSS01.01 DSS01.03
ISO 27K 2013	A.12.1.1
DNB 2014/2017	
BIO 2019	12.1.1
NIST Cybersecurity Framework	

Incident/Problem Management

6.4 (IM.04) Problem Management

Risico:

Incidenten worden niet correct geclassificeerd en verkeerd afgehandeld in het Incident Management proces, waardoor uiteindelijk de prestaties en kwaliteit van de informatievoorziening worden verminderd.

Doelstelling:

Een formeel Problem Management proces is gedefinieerd en geïmplementeerd. Er zijn procedures ingesteld om oorzaken van (potentiële) incidenten en problemen (proactief en reactief) te identificeren en bekende fouten te beheersen totdat ze zijn opgelost. Structurele fouten in IT-services worden geminimaliseerd, zodat aantal en impact van mogelijke problemen wordt verminderd.

Volwassenheidsniveaus:

1	(a) Er is geen beleid voor Problem Management. (b) Er zijn geen rollen en verantwoordelijkheden voor Problem Management vastgesteld. (c) Er zijn geen procedures om oorzaak en gevolg van incidenten te identificeren. (d) Problemen zullen waarschijnlijk niet gedetecteerd worden.
2	(a) Er is een informeel proces voor Problem Management. (b) Enkele belangrijke individuen kunnen helpen met problemen die hun expertise betreffen, maar de verantwoordelijkheid voor Problem Management is niet toegewezen. (c) De registratie en documentatie van problemen en de bijbehorende oplossingen zijn gebrekkig en inconsistent binnen de response teams.
3	(a) Er is formeel beleid voor Problem Management en deze is gecommuniceerd. (b) Er zijn procedures om de oorzaak van problemen te identificeren. (c) De rollen en verantwoordelijkheden van de organisatie en leveranciers zijn duidelijk vastgesteld. (d) Er is een formele plek in de organisatie waar problemen geregistreerd, gecommuniceerd, geanalyseerd en toegewezen worden aan verantwoordelijken. (e) Problemen worden geprioriteerd en toegewezen aan response teams conform het beleid. (f) Informatie wordt proactief en op formele wijze gedeeld binnen response teams. (g) Managementanalyse van probleemidentificatie en -oplossing is beperkt en informeel. (h) Bekende foutmeldingen worden geregistreerd en beheerst tot deze zijn opgelost.
4	Aanvullend: (a) Problemen worden proactief geanalyseerd om oorzaken op te sporen. (b) Externe bronnen (zoals leveranciers, gebruikersgroepen, conferenties) worden systematisch geraadpleegd om proactief problemen op te sporen. (c) Voortgang van probleemdiagnose en -oplossing wordt bewaakt en structurele fouten worden geminimaliseerd. (d) De meeste problemen worden geïdentificeerd, geregistreerd en gerapporteerd, en maatregelen worden genomen. (e) Problem Management wordt periodiek geëvalueerd.
5	Aanvullend: (a) Er worden tools gebruikt voor het documenteren, rapporteren en analyseren van problemen en oplossingen. (b) Problem Management processen zijn geïntegreerd met Configuration en Change Management. (c) De meeste systemen beschikken over automatische detectie- en waarschuwingssystemen, die voortdurend gemonitord en beoordeeld worden. (d) Problem Management wordt geanalyseerd met het oog op voortdurende verbetering.

Referenties:

Normenkader Informatie-beveiliging HO 2015 ***04 Continuïteit***	1.8 4.7
COBIT 4.1	DS9.2 DS9.3
COBIT 5	BAI10.03 BAI10.04 BAI10.05 DSS02.05
ISO 27K 2013	A.8.1.1 A.8.1.2 A.8.2.2 A.12.5.1 A.14.3.1
DNB 2014/2017	13.1
BIO 2019	8.1.1 8.1.2 8.2.2 12.5.1 14.3.1
NIST Cybersecurity Framework	ID.AM-1 ID.AM-2 ID.AM-3 ID.AM-4 ID.AM-5

Change Management

7.1 (CH.01) Normen en procedures voor aanpassingen

Risico:

Het ontbreken van een formeel IT Change Management proces, dat ervoor zorgt dat voorgestelde wijzigingen op gecontroleerde wijze worden beoordeeld, geautoriseerd, getest, geïmplementeerd, gedocumenteerd en vrijgegeven, kan leiden tot verstoringen in de bedrijfsvoering en/of verlies van (vertrouwelijke) gegevens.

Doelstelling:

Procedures voor formeel Change Management zijn opgezet om alle aanvragen (inclusief onderhoud en patches) voor wijzigingen in applicaties, procedures, processen, systeem- en serviceparameters en de onderliggende platforms op een gestandaardiseerde manier te behandelen.

Volwassenheidsniveaus:

1	(a) Er is geen beleid of procedure voor Change Management. (b) (Verzoeken voor) wijzigingen worden niet op een gestandaardiseerde of consistente manier behandeld. (c) Er zijn geen rollen en verantwoordelijkheden vastgesteld. (d) Wijzigen worden niet formeel goedgekeurd. (e) Wijzigingen worden niet of gebrekkig gedocumenteerd.
2	(a) Er is beleid voor Change Management om kritische wijzigingen aan te pakken. (b) Er is een Change Management procedure die meestal wordt uitgevoerd bij een wijziging. (c) Rollen en verantwoordelijkheden zijn gedeeltelijk vastgesteld. (d) Het proces is informeel en er kunnen ongeautoriseerde wijzigingen doorgevoerd worden. (e) Er is versiebeheer geïmplementeerd voor essentiële systeemparameters.
3	(a) Het beleid voor Change Management en de werkwijzen zijn gedocumenteerd, gestandaardiseerd en gecommuniceerd. (b) Er is een formeel Change Management proces voor het wijzigen van applicaties, procedures, processen, systemen en diensten, en de onderliggende platformen en infrastructuren. (c) Het proces omvat alle componenten van overzetten naar productie, inclusief autorisatie, impactanalyse, Release Management, bijhouden van wijzigingen en roll back-procedures. (d) Rollen en verantwoordelijkheden zijn vastgesteld en toegewezen. (Verzoeken voor) wijzigingen worden op een gestandaardiseerde manier behandeld. (e) Wijzigingen worden gedocumenteerd. Documentatie is correct en actueel. (f) Er is/wordt een systeem voor versiebeheer geïmplementeerd. (g*) Er is documentatie waaruit blijkt dat de organisatie wijzigingen conform de procedure heeft uitgevoerd, bijv.: • kopie gehanteerde RFC formulier (lijncontrole); • kopie impactanalyse van de wijziging (lijncontrole); • kopie acceptatieformulier, inclusief testuitkomsten (lijncontrole); • schermprint van de change die van ontwikkelomgeving naar productie omgeving wordt geïmplementeerd (lijncontrole).
4	Aanvullend: (a) Het beleid voor Change Management is volledig opgenomen in de organisatie en wordt consequent toegepast voor alle wijzigingen. (b) De kwaliteit en effectiviteit van het Change Management proces wordt periodiek geëvalueerd. (c) Er wordt aan het senior management gerapporteerd. (d) Er worden tools ingezet om ongeautoriseerde wijzigingen te detecteren. (e*) Er is een overzicht van recente wijzigingen (wijzigingskalender - jaar/kwartaal).
5	Aanvullend: (a) Het beleid voor Change Management wordt regelmatig geëvalueerd en herzien. (b) Rollen en verantwoordelijkheden worden voortdurend geëvalueerd. (c) Uitzonderingen worden geanalyseerd en onderzocht. (d) Tekortkomingen en trends worden regelmatig aan het management gerapporteerd, wat leidt tot verbeterplannen. (e) De eisen aan rapportage worden regelmatig geëvalueerd en herzien.

Referenties:

Normenkader Informatie-beveiliging HO 2015 ***04 Continuïteit***	1.17 1.18 2.6 4.12 4.13 6.8
COBIT 4.1	DS5.6 DS8.1 DS8.2 DS8.4 DS8.5
COBIT 5	DSS02.01 DSS02.02 DSS02.03 DSS02.05 DSS02.06 DSS02.07
ISO 27K 2013	A.7.2.3 A.12.6.1, A.16.1.1 A.16.1.2 A.16.1.3 A.16.1.4 A.16.1.5 A.16.1.6 A.16.1.7
DNB 2014/2017	15.1 15.2
BIO 2019	7.2.3 12.6.1 12.6.1.1 16.1.1 16.1.2 16.1.2.1 16.1.2.2 16.1.2.3 16.1.2.4 16.1.2.5 16.1.2.6 16.1.2.7 16.1.3 16.1.3.1 16.1.4 16.1.4.1 16.1.5 16.1.6 16.1.6.1 16.1.6.2 16.1.7 16.1.7.1 Supplement BIG: 13.1.1.5 13.1.1.6 [A]
NIST Cybersecurity Framework	RS.RP-1 PR.IP-9 PR.IP-10 RS.CO-1 RS.CO-2 RS.CO-3 RS.CO-4 RS.AN-3 RS.AN-4 RS.MI-1 RS.MI-2

Change Management

7.2 (CH.02) Impact assessment, prioriteren en autoriseren

Risico:

Een verkeerde impact assessment, prioritering of autorisatie kan tot verstoring, verminking of verlies van (vertrouwelijke) data leiden.

Doelstelling:

Alle wijzigingsverzoeken worden op een gestructureerde manier beoordeeld om de impact te bepalen voor operationele systemen en functionaliteit. Alle wijzigingen zijn gecategoriseerd, geprioriteerd en geautoriseerd.

Volwassenheidsniveaus:

1	(a) Er is geen procedure voor assessment, prioritering en autorisatie van wijzigingen. (b) Rollen en verantwoordelijkheden zijn niet vastgesteld. (c) Impact assessments voor wijzigingsverzoeken worden op ad-hoc-basis uitgevoerd en er kunnen ongeautoriseerde wijzigingen plaatsvinden. (d) Het proces voor categoriseren en prioriteren van wijzigingen is niet gestandaardiseerd.
2	(a) Er wordt een analyse gedaan van de business impact van IT-wijzigingen. (b) Criteria voor de analyse zijn in ontwikkeling. (c) Er is een informeel proces voor categoriseren, prioriteren en autoriseren van wijzigingen. (d) Rollen en verantwoordelijkheden zijn gedeeltelijk vastgesteld. (e) Bij het goedkeuringsproces worden vooral de business proceseigenaren betrokken.
3	(a) Er is een formele procedure voor categoriseren, prioriteren en autoriseren van wijzigingen en deze is gecommuniceerd. (b) Voorafgaand aan de wijziging wordt een impact assessment uitgevoerd. Implicaties op het gebied van (cyber)veiligheid, juridische zaken, contracten en wet- en regelgeving worden in dit proces meegenomen. (c) Er is een formele procedure voor het autoriseren van wijzigingen. (Change Advisory Board) (d) Elk wijzigingsverzoek wordt formeel (via de Change Advisory Board) goedgekeurd door de business proceseigenaar en de stakeholders. (e) Prioritering en categorisering is gebaseerd vooraf vastgestelde criteria. (f*) Verslagen van resultaten van wijzigingen (wel/niet succesvol, reden van succes/falen, vervolgactie, aard van de impact).
4	(a) De procedure voor assessment, categorisering, prioritering en autorisatie van wijzigingen wordt consistent uitgevoerd. (b) Alle wijzigingen worden gedegen gepland en beoordeeld op impact om de kans op post- productie problemen te minimaliseren. (c) Het aantal verstoringen en data fouten ten gevolge van verkeerde specificaties en/of incomplete impact assessment is beperkt tot een minimum. (d) De operationele effectiviteit van de procedures wordt periodiek geëvalueerd.
5	(a) De assessment procedure wordt regelmatig geëvalueerd en geactualiseerd. (b) De prestatie indicatoren worden regelmatig geëvalueerd. (c) Het management ontvangt regelmatig rapportages die leiden tot verbeterplannen. (d) Rapportage-eisen worden regelmatig geëvalueerd en geactualiseerd.

Referenties:

Normenkader Informatie-beveiliging HO 2015 ***04 Continuïteit***	1.17 1.18 4.8 4.12 4.13 4.14 6.8
COBIT 4.1	DS8.3
COBIT 5	DSS02.04
ISO 27K 2013	A.16.1.1 A.16.1.2 A.16.1.4 A.16.1.5 A.16.1.7 A.17.1.1 A.17.1.2
DNB 2014/2017	15.2
BIO 2019	16.1.1 16.1.2 16.1.2.1 16.1.2.2 16.1.2.3 16.1.2.4 16.1.2.5 16.1.2.6 16.1.2.7 16.1.4 16.1.4.1 16.1.5 16.1.7 16.1.7.1 17.1.1 17.1.2
NIST Cybersecurity Framework	RS.RP-1 PR.IP-9 PR.IP-10 RS.CO-1 RS.CO-3 RS.CO-4 RS.AN-3 RS.AN-4 RS.MI-1 RS.MI-2

Change Management

7.3 (CH.03) Noodaanpassingen

Risico:

Kritieke verstoring van bedrijfsprocessen kan niet tijdig worden opgelost, omdat er extra doorlooptijd nodig is bij de standaardprocedure voor Change Management.
Ongeautoriseerde wijzigingen die zijn aangebracht tijdens een noodsituatie, worden niet geregistreerd waardoor ze onopgemerkt blijven en later tot verstoringen of securityproblemen leiden.

Doelstelling:

Wijzigingen tijdens een noodsituatie die onmiddellijke implementatie vereisen, worden op de juiste manier afgehandeld om minimale impact op systemen en IT-toepassingen te garanderen. De noodsituatiewijziging wordt na implementatie geregistreerd, geëvalueerd, getest en goedgekeurd door het senior management.

Volwassenheidsniveaus:

1	(a) Er is geen procedure voor Change Management voor noodwijzigingen. (b) (Verzoeken voor) noodwijzigingen worden niet op een gestructureerde manier afgehandeld. (c) Er is geen of gebrekkige documentatie van noodwijzigingen. (d) Rollen en verantwoordelijkheden zijn niet gedefinieerd. (e) Er vindt geen formele goedkeuring van noodwijzigingen plaats.
2	(a) Er is een (informeel) Change Management proces voor noodwijzigingen, die de meest kritieke aspecten van het proces omvat. (b) Rollen en verantwoordelijkheden zijn gedeeltelijk gedefinieerd. (c) Na de noodwijziging wordt het beheer niet altijd volledig afgemaakt.
3	(a) De Change Management procedure voor noodwijzigingen is formeel vastgelegd, gedocumenteerd en gecommuniceerd. (b) (Verzoeken tot) noodwijzigingen worden op een gestandaardiseerde manier uitgevoerd. (c) Rollen en verantwoordelijkheden zijn helder gedefinieerd en toegewezen. (d) Noodwijzigingen zijn geautoriseerd en gedocumenteerd. (e) Controlestappen, inclusief goedkeuring, worden conform procedure uitgevoerd na de noodwijziging. (f) Kritieke afwijkingen van het proces worden geëvalueerd.
4	Aanvullend: (a) De Change Management procedure voor noodwijzigingen, inclusief de evaluatie na de implementatie, wordt consequent gevolgd voor alle noodwijzigingen. (b) De documentatie is correct en actueel. (c) Er is een proces voor de bewaking van de kwaliteit en de performance van het Change Management proces voor noodwijzigingen. (d) De kwaliteit en effectiviteit van het proces worden periodiek geëvalueerd
5	Aanvullend: (a) Het Change Management proces voor noodwijzigingen wordt regelmatig geëvalueerd en geactualiseerd. (b) Uitzonderingen worden geanalyseerd en onderzocht. (c) Er wordt regelmatig aan het management gerapporteerd, wat leidt tot verbeterplannen. (d) Rapportage-eisen worden regelmatig geëvalueerd en geactualiseerd. (e) Rollen en verantwoordelijkheden worden regelmatig geëvalueerd.

Referenties:

Normenkader Informatie-beveiliging HO 2015 ***04 Continuïteit***	4.13
COBIT 4.1	
COBIT 5	APO12.06 DSS04.03 DSS05.07
ISO 27K 2013	A.16.1.5
DNB 2014/2017	15.1 15.2
BIO 2019	16.1.5
NIST Cybersecurity Framework	RS.RP-1 PR.IP-9 PR.IP-10 RS.CO-1 RS.CO-2 RS.CO-3 RS.CO-4 RS.AN-3 RS.AN-4 RS.MI-1 RS.MI-2

Change Management

7.4 (CH.04) Testomgeving

Risico:

Het ontbreken van een veilige, gecontroleerde en representatieve testomgeving kan leiden tot onvoldoende/onbetrouwbare tests voordat wijzigingen worden aangebracht in de productieomgeving van een kritieke applicatie, wat een negatief effect zou kunnen hebben op de functionaliteit, prestaties en beveiliging van de toepassing.

Doelstelling:

Er is een beveiligde testomgeving gedefinieerd en ingericht, die representatief is voor de geplande productieomgeving met betrekking tot beveiliging, interne controles, operationele procedures, gegevenskwaliteit, privacy vereisten en systeembelasting.

Volwassenheidsniveaus:

1	(a) Er is geen beveiligde testomgeving gedefinieerd en ingericht voor het ontwikkelen en testen van wijzigingen. (b) Er is geen beleid voor het gebruik van een testomgeving. (c) Het is waarschijnlijk dat er door gebrekkig Change Management fouten ontstaan die leiden tot verstoringen in de productieomgeving.
2	(a) Er is een informeel beleid voor het gebruik van een testomgeving voor het ontwikkelen en testen van wijzigingen. (b) Wijzigingen worden buiten de productieomgeving ontwikkeld en getest. (c) De testomgeving is voor de kritieke aspecten representatief voor de productieomgeving.
3	(a) Formeel beleid is vastgesteld en geïmplementeerd voor de testomgeving. (b) Er is een veilige testomgeving gedefinieerd en ingericht. (c) De testomgeving representeert de productieomgeving en komt overeen in aspecten zoals workload/stress, besturingssystemen, applicatiesoftware, databasemanagement, netwerken en infrastructuur. (d) De testomgeving staat volledig los van de productieomgeving. (e) De testomgeving is beschermd tegen ongeautoriseerde toegang en gebruik. (f) Het eigenaarschap van de test- en productieomgeving is duidelijk toegewezen. (g) Er zijn richtlijnen voor het gebruik van data in de testomgeving, zodat aan privacywetten wordt voldaan.
4	Aanvullend: (a) Er is een proces voor de bewaking van het gebruik van de testomgeving, en incidenten worden beoordeeld en opgelost. (b) De test- en productieomgevingen worden periodiek geëvalueerd om te garanderen dat de testomgeving nog voldoende representatief is voor de productieomgeving. (c) De beveiliging van de testomgeving en het test-datamanagement wordt periodiek geëvalueerd. (d*) Omgevingen zijn herkenbaar gescheiden, zoals door afwijkende gebruikers-ID's en/of ander schermopbouw/-kleuren. (e*) Ontwikkeltools zijn niet op productie-omgeving aanwezig. (f*) Er zijn beheer- en change logs inclusief zichtbare monitoring en evaluatie daarop.
5	Aanvullend: (a) Beleid wordt voortdurend geëvalueerd en verbeterd. (b) Rollen en verantwoordelijkheden worden voortdurend geëvalueerd. (c) Er wordt regelmatig aan het management gerapporteerd, wat leidt tot verbeterplannen. (d) De eisen voor rapportage worden regelmatig geëvalueerd en geactualiseerd. (f) Er zijn tools geïmplementeerd voor het creëren van subsets en het anonimiseren van data.

Referenties:

Normenkader Informatie-beveiliging HO 2015 ***04 Continuïteit***	1.17 1.18 2.6 4.8
COBIT 4.1	DS10.1 DS10.2 DS10.3 DS10.4
COBIT 5	DS03.01 DS03.02 DS03.03 DS03.04 DS03.05
ISO 27K 2013	A.7.2.3 A.12.6.1 A.16.1.1 A.16.1.2 A.16.1.3
DNB 2014/2017	15.1 15.2
BIO 2019	7.2.3 12.6.1 16.1.1 16.1.2 16.1.2.1 16.1.2.2 16.1.2.3 16.1.2.4 16.1.2.5 16.1.2.6 16.1.2.7 16.1.3 16.1.3.1 Supplement BIG: 13.1.1.5 13.1.1.6
NIST Cybersecurity Framework	RS.RP-1 PR.IP-9 PR.IP-10 RS.CO-1 RS.CO-2 RS.CO-3 RS.CO-4 RS.AN-3 RS.AN-4 RS.MI-1 RS.MI-2

Change Management

7.5 (CH.05) Testen van aanpassingen

Risico:

Ontoereikend of onvolledig testen kan leiden tot verstoring van de bedrijfsvoering of tot onbetrouwbare gegevensverwerking.

Doelstelling:

Voorafgaand aan migratie naar de operationele omgeving worden wijzigingen op onafhankelijke wijze getest in overeenstemming met het gedefinieerde testplan. Er wordt voor gezorgd dat het plan rekening houdt met beveiliging en prestaties.

Volwassenheidsniveaus:

1	(a) Er is geen beleid voor het testen van wijzigingen. (b) Rollen en verantwoordelijkheden voor het testen van wijzigingen zijn niet vastgelegd. (c) Testen wordt individueel/ad hoc gedaan. (d) Er worden geen testplannen gemaakt voor het testen plaatsvindt.
2	(a) Er is een informele procedure voor het testen van wijzigingen geïmplementeerd. (b) Rollen en verantwoordelijkheden zijn gedeeltelijk vastgesteld. (c) Er zijn testplannen gemaakt, maar er zijn geen formele criteria voor de inhoud van testplannen. (d) Er zijn gedeeltelijk maatregelen geïmplementeerd om er voor te zorgen dat wijzigingen volgens het testplan getest worden. (e) Testresultaten worden gedeeltelijk gedocumenteerd. (f) Er zijn geen criteria voor het bewaren of verwijderen van testresultaten.
3	(a) Formeel beleid voor het testen van wijzigingen is gedocumenteerd en gecommuniceerd. (b) Rollen en verantwoordelijkheden zijn vastgesteld en toegewezen. (c) Er worden testplannen gemaakt voordat de tests worden uitgevoerd. (d) Er zijn criteria vastgesteld om te zorgen dat belangrijke elementen, zoals beveiliging en prestatie, opgenomen zijn in het testplan. (e) Wijzigingen worden onafhankelijk volgens de testplannen getest. (f) Er is een beheerprocedure geïmplementeerd voor het bewaren en verwijderen van testresultaten. (g) Fallback of back-out plannen worden voorbereid en getest voordat wijzigingen in productie worden genomen.
4	Aanvullend: (a) Alle wijzigingen van essentiële applicaties worden geëvalueerd en getest zodat er geen negatieve gevolgen zijn voor de bedrijfsvoering of de beveiliging. (b) Wijzigingen worden alleen getest in de testomgeving. (c) Prestatie- en beveiligingseisen zijn gevalideerd. (d) De testprocedures, testplannen en uitvoering van testprocedures worden periodiek geëvalueerd.
5	Aanvullend: (a) Beleid wordt voortdurend geëvalueerd en verbeterd. (b) Rollen en verantwoordelijkheden worden voortdurend geëvalueerd. (c) Alle incidenten met Change Management/testprocessen worden geëvalueerd en opgelost. (d) Er wordt regelmatig aan het management gerapporteerd, wat leidt tot verbeterplannen. (e) De eisen aan de rapportages worden regelmatig geëvalueerd en geactualiseerd.

Referenties:

Normenkader Informatie-beveiliging HO 2015 ***04 Continuïteit***	4.1
COBIT 4.1	AI6.1 AI6.4 AI6.5
COBIT 5	BAI06.01 BAI06.02 BAI06.03 BAI06.04
ISO 27K 2013	8.1 A.12.1.2 A.14.2.2 A.14.2.4
DNB 2014/2017	10.1
BIO 2019	12.1.2 12.1.2.1 14.2.2 14.2.2.1
NIST Cybersecurity Framework	

Change Management

7.6 (CH.06) Promotie naar productie

Risico:

Als gevolg van onveilige overdracht van wijzigingen naar de productieomgeving treedt verstoring van de bedrijfsvoering op of vinden ongeautoriseerde wijzigingen plaats.

Doelstelling:

Na testen wordt het gewijzigde systeem op gecontroleerde wijze en volgens het implementatieplan overgezet naar productie. Goedkeuring wordt verkregen van belangrijke stakeholders, zoals gebruikers, systeemeigenaar en operationeel management. Waar nodig wordt het gewijzigde systeem enige tijd naast het oude systeem gebruikt en worden gedrag en resultaten vergeleken.

Volwassenheidsniveaus:

1	(a) Er is geen beleid voor de overdracht van gewijzigde systemen naar productie. (b) De implementatieplannen worden ad hoc ontworpen. (c) Er zijn geen rollen of verantwoordelijkheden gedefinieerd.
2	(a) Er is een informeel beleid voor de overdracht van gewijzigde systemen dat essentiële aspecten, zoals goedkeuring van het proces, bevat. (b) Rollen en verantwoordelijkheden zijn gedeeltelijk gedefinieerd. (c) Er worden implementatieplannen gemaakt, maar er zijn geen formele criteria voor de inhoud. (d) Om overdracht volgens het gedefinieerde implementatieplan te laten verlopen zijn er gedeeltelijk beheersmaatregelen geïmplementeerd. (e) Doorgaans worden acceptatietests uitgevoerd.
3	(a) Formeel beleid voor de overdracht van gewijzigde systemen is gedocumenteerd en gecommuniceerd. (b) Er zijn procedures voor het gebruik van OTAP omgevingen. Er zijn ook goedkeuringsprocessen. (c) Het goedkeuringsproces bevat een formeel vastgelegde sign-off door belangrijke stakeholders. (d) Rollen en verantwoordelijkheden zijn gedefinieerd en toegewezen. (e) Toegangsregels voor de verschillende (OTAP) omgevingen zijn gedefinieerd om functiescheiding te bewerkstellen. (f) Voor overdracht worden implementatieplannen gemaakt, en overdracht vindt plaats volgens deze plannen. (g) Waar nodig (op basis van impactanalyse) wordt het veranderde systeem een tijdje parallel aan het oude systeem gedraaid, waarbij gedrag en resultaat wordt vergeleken. (h) Acceptatiecriteria worden bepaald en acceptatietests worden uitgevoerd en gelogd. (i) Er zijn beheersmaatregelen om te garanderen dat geaccepteerde wijzigingen daadwerkelijk onderdeel zijn van de overdracht naar productie (volledig).
4	Aanvullend: (a) Er is een procedure voor het updaten van systeemdocumentatie, relevante calamiteitenplannen, etc. (b) Het overdrachtsbeleid wordt consequent geïmplementeerd. (c) Een wijziging wordt pas afgesloten als alle activiteiten en registraties zijn geïmplementeerd en geëvalueerd. (d) De overdracht van in productie te nemen systemen wordt regelmatig gevealuleerd
5	Aanvullend: (a) Beleid, rollen en verantwoordelijkheden worden voortdurend geëvalueerd en verbeterd. (b) Alle incidenten tijdens testen en implementatie worden geëvalueerd en opgelost. (c) Er wordt regelmatig aan het management gerapporteerd, wat leidt tot verbeteringsplannen. (d) Rapportage-eisen worden regelmatig geëvalueerd en geactualiseerd.

Referenties:

Normenkader Informatie-beveiliging HO 2015 ***04 Continuïteit***	4.1 4.8
COBIT 4.1	AI6.2
COBIT 5	BAI06.01
ISO 27K 2013	8.1 A.12.1.2 A.12.6.1 A.14.2.2 A.14.2.4
DNB 2014/2017	overnemen
BIO 2019	12.1.2 12.1.2.1 12.6.1 14.2.2 14.2.2.1
NIST Cybersecurity Framework	

Systeemontwikkeling

8.1 (SD.01) Methodiek voor veilige softwareontwikkeling en -implementatie

Risico:

Software- en/of systeemontwikkeling zijn niet ontworpen en geïmplementeerd volgens overeengekomen functionele, technische en beveiligingseisen, goedkeuringsnormen en de informatiearchitectuur, waardoor niet aan de business requirements wordt voldaan.

Doelstelling:

Er is een gestructureerde aanpak (levenscyclus voor veilige softwareontwikkeling) voor interne ontwikkeling (en aanschaf) van software geïmplementeerd, die ervoor zorgt dat potentiële risico's voor bedrijfsvoering adequaat worden beoordeeld en beperkt, en dat de aspecten vertrouwelijkheid, integriteit en beschikbaarheid worden meegenomen. Voor elke nieuwe ontwikkeling (of acquisitie) is goedkeuring vereist door het juiste niveau van het bedrijfs- en IT-management.

Volwassenheidsniveaus:

1	(a) Er is geen gestructureerde aanpak. (b) Systeem- en softwareontwikkeling gebeuren ad hoc.
2	(a) Er zijn richtlijnen voor veilig coderen die niet altijd worden toegepast. (b) Evaluatie van beveiligingseisen en broncodes vinden plaats op individueel initiatief. (c) Er zijn geen formele beveiligingsmijlpalen geïmplementeerd in projectmanagementmethodiek en beveiligingstesten.
3	(a) De organisatie heeft een gestructureerde aanpak voor interne ontwikkeling en aanschaf van software geïmplementeerd. (b) Er zijn verplichte standaarden voor veilig coderen bepaald. Security-by-Design, Privacy-by-Design en Privacy-by-Default worden door richtlijnen en standaarden afgedwongen. (c) Voor elke nieuwe ontwikkeling of aanschaf is goedkeuring nodig van het juiste niveau van het business- of IT-management. (d) De methodiek voor assurance van softwarekwaliteit bevat verplichte "mijlpalen voor informatiebeveiliging" (met inbegrip van risicobeoordeling, broncodebeoordeling en tests) die niet kunnen worden omzeild en deze worden gedocumenteerd. (e) Awareness training voor beveiliging wordt op vrijwillige basis gevolgd. (f*) Privacy by design is uitgangspunt en een impact assessment informatiebeveiliging is standaard onderdeel van het projectplan. (g*) Er is een (architectuur)model(len) systeem omgeving. (h*) Er is inrichtingsdocumentatie (good practices inrichtingen). (i*) Er is een procedurebeschrijving voor uitbestede ontwikkeling van programmatuur; (j*) Er is/zijn (een) overeenkomst(en) waaruit afgesproken beveiligingstestactiviteiten blijken.
4	Aanvullend: (a) De effectiviteit van een formele en gestructureerde aanpak wordt periodiek geëvalueerd en herzien indien nodig. (b) Er is een verplicht beveiligings- en risicotrainingsprogramma voor ontwikkelaars. (c*) In projectevaluaties is aandacht voor informatiebeveiliging zichtbaar. (d*) Kopieën opleidingscertificaten betrokken ontwikkelaars, testers en beheerders.
5	Aanvullend: (a) Op basis van ontwikkelingen in dreigingen worden periodiek risicoanalyses uitgevoerd. De scope van deze analyses omvat de geïmplementeerde softwareproducten en de ontwikkelingsmethodiek zelf. (b) Restrisico's worden gerapporteerd aan het verantwoordelijke (senior) IT-management.

Referenties:

Normenkader Informatie-beveiliging HO 2015 ***01 Beleid en Organisatie***	4.1
COBIT 4.1	AI6.3
COBIT 5	BAI06.02
ISO 27K 2013	8.1, A.12.1.2
DNB 2014/2017	10.1
BIO 2019	12.1.2 12.1.2.1
NIST Cybersecurity Framework	

Systeemontwikkeling

8.2 (SD.02) Toegang tot de productieomgeving door ontwikkelaars

Risico:

Ontwikkelaars met toegang tot de productieomgeving brengen de scheiding van taken in gevaar, wat uiteindelijk zou kunnen leiden tot ongeoorloofde toegang tot of wijzigingen in programma's en gegevens.

Doelstelling:

Medewerkers (ontwikkelaars) die betrokken zijn bij de ontwikkeling en implementatie van wijzigingen in in-scope-applicaties en ondersteunende besturingssystemen en databases, hebben geen schrijftoegang tot de productieomgeving. Medewerkers (ontwikkelaars) die verantwoordelijk zijn voor het vrijgeven van de broncode voor productie hebben geen schrijftoegang tot de test- of ontwikkelomgeving.

Volwassenheidsniveaus:

1	(a) Er is geen beleid voor toegangsrestricties tot de productieomgeving voor ontwikkelaars.
2	(a) Er is een beperkt beleid bepaald voor toegang tot productie voor ontwikkelaars. (b) Ontwikkelaars hebben geen schrijftoegang tot de productieomgeving. (c) Bij kritieke incidenten wordt aan ontwikkelaars schrijftoegang tot productie verleend.
3	(a) Een samenhangend beleid is bepaald, geïmplementeerd en goedgekeurd door het (senior) management. (b) Ontwikkelaars hebben geen schrijftoegang tot productie, en systeembeheerders die software overzetten naar productie hebben geen schrijftoegang tot de ontwikkel-, test- en acceptatieomgeving. (c) Uitzonderingen op het beleid worden vooraf goedgekeurd door de systeem-/proceseigenaar en tijdens de tijdelijke schrijftoegang wordt gebruik gemaakt van logging en/of het 4-ogen principe. (d*) Er is beleid of procesbeschrijving voor het beheer van speciale bevoegdheden. (e*) Er zijn functie- of rolbeschrijvingen van de beheerders van speciale bevoegdheden. (f*) Er is informatie uit systemen waaruit blijkt dat de technische of functioneel beheerders die speciale bevoegdheden hebben, ook een gewone gebruikers-ID hebben voor hun reguliere werkzaamheden.
4	Aanvullend: (a) De effectiviteit van de implementatie en de uitvoering van het beleid worden periodiek geëvalueerd en gedocumenteerd. (b) Verbeteringen worden bepaald op basis van de evaluatie. (c) De logs van bij uitzondering toegestane toegang worden periodiek beoordeeld.
5	Aanvullend: (a) Voor de schrijftoegang tot productie wordt gebruik gemaakt van real-time monitoring en detectie. Dit is geïmplementeerd door middel van geautomatiseerde detectietechnologie, bijv. SIEM. (b) Uitzonderingen worden maandelijks aan het (senior) management gerapporteerd.

Referenties:

Normenkader Informatie-beveiliging HO 2015 ***05 Vertrouwelijkheid en Integriteit***	4.2 4.10
COBIT 4.1	AI7.4
COBIT 5	BAI07.04
ISO 27K 2013	8.1 A.9.4.5 A.12.1.4 A.14.2.6 A.14.3.1
DNB 2014/2017	10.3
BIO 2019	9.4.5 12.1.4 12.1.4.1 12.1.4.2 14.2.6 14.2.6.1 14.3.1 Supplement BIG: 12.4.3.2
NIST Cybersecurity Framework	

Systeemontwikkeling

8.3 (SD.03) Data conversie en/of migratie

Risico:

Afwijkingen tijdens dataconversie/-migratie worden niet (tijdig) gedetecteerd, wat leidt tot verminderde integriteit (bijvoorbeeld nauwkeurigheid en volledigheid van gegevens of systemen.

Doelstelling:

Het management beschikt over beheersmaatregelen om te zorgen dat de dataconversie accuraat en volledig is. Deze dataconversie-controles zijn opgesteld om de data-integriteit gedurende het conversieproces te behouden.

Volwassenheidsniveaus:

1	(a) Er zijn geen beheersmaatregelen gedefinieerd met betrekking tot dataconversie en/of -migratie
2	(a) Er zijn beperkte beheersmaatregelen geïmplementeerd om de juistheid en volledigheid van dataconversie/-migratie te valideren. (b) De gedefinieerde beheersmaatregelen zijn niet volledig gedocumenteerd.
3	(a) Er wordt een risico- en bedrijfsimpactanalyse uitgevoerd ter rechtvaardiging van de gedefinieerde beheersmaatregelen. (b) Het ontwerp van de beheersmaatregelen is gedocumenteerd en formeel aanvaard door de eigenaar van het systeem of het proces. (c) De beheersmaatregelen waarborgen de juistheid en volledigheid van de data conversie/migratie en bewaken ook de integriteit van de data. (d) De resultaten van de (handmatige en/of geautomatiseerde) uitgevoerde integriteitscontroles worden gedocumenteerd en beoordeeld door de eigenaar van het systeem of het proces om de dataconversie formeel te accepteren.
4	Aanvullend: (a) Een evaluatie van het dataconversie-/migratieproces wordt uitgevoerd door het projectteam. (b) Leer- en verbeterpunten worden geïdentificeerd en gedocumenteerd voor toekomstig gebruik.
5	Aanvullend: (a) De aanpak van conversie/migratie is ingebed in de projectmanagementmethodiek. (b) Controles (op juistheid, volledigheid en integriteit) zijn volledig geautomatiseerd. Handmatige interventies zijn uitzonderlijk.

Referenties:

Normenkader Informatie-beveiliging HO 2015 ***05 Vertrouwelijkheid en Integriteit***	4.1 6.5
COBIT 4.1	AI7.6
COBIT 5	BAI07.05 BAI03.08
ISO 27K 2013	8.1 A.9.4.5 A.12.1.2 A.14.2.3 A.14.2.8 A.14.3.1
DNB 2014/2017	10.4
BIO 2019	9.4.5 12.1.2 12.1.2.1 14.2.3 14.2.8 14.3.1
NIST Cybersecurity Framework	

Datamanagement

9.1 (DM.01) Data (en systeem) eigenaarschap

Risico:

Onduidelijk of dubbelzinnig eigenaarschap kan de effectieve besluitvorming, bescherming van gegevens en informatiesystemen, en de controle over het datamanagement in gevaar brengen.

Doelstelling:

Het bedrijf beschikt over procedures en hulpmiddelen, waarmee het de verantwoordelijkheid voor het eigenaarschap van informatie en informatiesystemen kan adresseren. Eigenaren nemen beslissingen over het classificeren van informatie en (informatie)systemen en beschermen ze in overeenstemming met deze classificatie.

Volwassenheidsniveaus:

1	(a) Er is geen formeel beleid voor data-eigenaarschap. (b) (Informatie)systeemeigenaarschap wordt niet of informeel aangepakt. (c) Er zijn geen rollen en verantwoordelijkheden voor data-eigenaarschap toegewezen.
2	(a) Er is beleid voor (informatie)systeem- en data-eigenaarschap. (b) Het beleid geeft een duidelijke omschrijving van rollen, verantwoordelijkheden en eigenaarschap. (c) Niet voor alle data en (informatie)systemen zijn verantwoordelijkheden toegewezen.
3	(a) Het goedgekeurde beleid geeft een duidelijke omschrijving van rollen, verantwoordelijkheden en eigenaarschap. (b) Beleid en procedures ondersteunen de bescherming van informatiemiddelen, maken efficiënte levering en gebruik van businessapplicaties mogelijk en zorgen voor effectieve besluitvorming over (informatie)beveiliging. (c) Beleid en procedures worden naar de hele organisatie gecommuniceerd en toegepast op bedrijfskritische data en informatiesystemen.
4	Aanvullend: (a) Beleid en procedures zijn geïmplementeerd in de organisatie en worden toegepast op alle applicatiesystemen, enterprise architectuur, interne en externe datacommunicatie. (b) Eigenaarschap van belangrijke data (en systemen) wordt periodiek geëvalueerd.
5	Aanvullend: (a) Het voldoen aan het datamanagementbeleid wordt periodiek aan het senior management gerapporteerd. (b) Het beleid wordt jaarlijks geëvalueerd, geactualiseerd en goedgekeurd door het senior management.

Referenties:

Normenkader Informatie-beveiliging HO 2015 ***01 Beleid en Organisatie***	6.6
COBIT 4.1	AI7.8
COBIT 5	BAI07.06
ISO 27K 2013	A.14.2.9 A.14.2.3
DNB 2014/2017	10.5
BIO 2019	14.2.9 14.2.9.1 14.2.9.2 14.2.3
NIST Cybersecurity Framework	

Datamanagement

9.2 (DM.02) Classificatie

Risico:

Beslissingen over het classificeren van informatie en (informatie)systemen, evenals het gerelateerde beschermingsniveau, zijn niet in lijn met de business requirements. Gegevens kunnen op diverse manieren worden gecompromitteerd als gevoelige gegevens niet op het juiste niveau worden geclassificeerd.

Doelstelling:

Stel een classificatieschema op dat in de hele organisatie van toepassing is, op basis van de kriticiteit en gevoeligheid (bijvoorbeeld openbaar, vertrouwelijk, topgeheim) van organisatiegegevens. Dit schema bevat details over het eigenaarschap van gegevens; gedefinieerde passende (informatie)beveiligingsniveaus en beschermingsmaatregelen; en een korte beschrijving van eisen voor het bewaren en vernietigen van gegevens, en gevoeligheid. Het wordt gebruikt als basis voor het toepassen van maatregelen zoals toegangscontrole, archivering en versleuteling.

Volwassenheidsniveaus:

1	(a) Er is geen classificatieschema. (b) De organisatie maakt geen verschil tussen de niveaus van gevoeligheid van data.
2	(a) De classificatie van data is informeel en ad hoc. (b) Individuele interpretaties van dataclassificatieschema's worden toegepast. (c) Data-eigenaars (indien toegewezen) bepalen zelf de gevoeligheid van de data en eventuele behoefte aan extra (cyber)maatregelen.
3	(a) Er is een dataclassificatieschema en richtlijnen voor het gebruik daarvan geïmplementeerd en toegepast binnen de hele organisatie. (b) Eigendom van data, definities en eisen voor verschillende niveaus van dataclassificatie worden allemaal nadrukkelijk beschreven in de richtlijnen. (c) De richtlijnen worden gebruikt als een basis voor het toepassen van de benodigde (cyber)beheersmaatregelen voor kritische businessprocessen en/of applicaties. (d) Het classificatieschema is goedgekeurd door het senior management.
4	Aanvullend: (a) De richtlijnen worden gebruikt als basis voor het toepassen van de benodigde (cyber)beheersmaatregelen voor alle businessprocessen en applicaties binnen de gehele organisatie. (b) De implementatie en uitvoering van relevante procedures en de juistheid en volledigheid van de classificatieschema's worden periodiek geëvalueerd.
5	Aanvullend: (a) (Wijzigingen in) dataclassificatie wordt volledig ondersteund door geautomatiseerde tools, workflow processing en geïntegreerde dashboards. (b) Dataclassificatie is onderdeel van informatie/data lifecycle management. (c*) Er is documentatie van informatie waaruit blijkt dat classificaties periodiek wordt gereviewed.

Referenties:

Normenkader Informatie-beveiliging HO 2015 ***01 Beleid en Organisatie***	1.19 4.5 4.6
COBIT 4.1	DS11.2
COBIT 5	DSS04.08 DSS06.04
ISO 27K 2013	A.8.3.1 A.12.3.1 A.18.1.3
DNB 2014/2017	12.1
BIO 2019	8.3.1 12.3.1 12.3.1.1 12.3.1.2 12.3.1.3 12.3.1.4 12.3.1.5 18.1.3 18.1.3.1
NIST Cybersecurity Framework	PR.DS-1 PR.DS-2 PR.DS-5 PR.IP-6

Datamanagement

9.3 (DM.03) Beveiligingseisen voor datamanagement

Risico:

Ontoereikende (informatie)beveiligingseisen voor datamanagement kunnen leiden tot het niet behalen van bedrijfsdoelstellingen en niet-naleving van het (informatie)beveiligingsbeleid van de organisatie en van wet- en regelgeving (boetes).

Doelstelling:

Beleid en procedures zijn vastgesteld en geïmplementeerd om (informatie)beveiligingseisen te identificeren en toe te passen op de ontvangst, verwerking, opslag en doorgifte van relevante gegevens in lijn met bedrijfsdoelstellingen, het (informatie)beveiligingsbeleid van de organisatie en wettelijke vereisten (bijvoorbeeld privacy van bepaalde gegevens).

Volwassenheidsniveaus:

1	(a) Er is geen beleid voor veilig datamanagement vastgelegd.
2	(a) Beperkte en informele (informatie)veiligheidswensen voor datamanagement zijn bepaald. (b) Er is geen organisatiebreed beleid om (informatie)veiligheidswensen voor datamanagement te bepalen of toe te passen.
3	(a) Er is een beleid bepaald, geïmplementeerd en gecommuniceerd om gevoelige data te beschermen tegen ongeautoriseerde toegang en incorrecte uitwisseling. (b) Het beleid is goedgekeurd door het (senior) management. (c) Er is een formeel proces dat gevoelige data identificeert en uitspraken doet over vertrouwelijkheid en het voldoen aan relevante wet- en regelgeving (bv. data privacy). (d) Er is overeenstemming met proceseigenaren over dataclassificatie. (e) De eisen voor essentiële (informatie)systemen zijn in overeenstemming met organisatiedoelen. De eisen zijn opgesteld voor fysieke en logische toegang tot data output, waarvan de vertrouwelijkheid duidelijk gedefinieerd en afgewogen is.
4	Aanvullend: (a) De implementatie en uitvoering van procedures omtrent (informatie)veiligheidseisen voor datamanagement worden periodiek geëvalueerd. (b) De eisen voor alle informatiesystemen ten aanzien van o.a. fysieke beveiliging, back-up van gevoelige data en opslag in de cloud zijn vastgesteld. (c) Er zijn awareness programma's ontwikkeld om werknemers bewust te maken van het veilig omgaan met en verwerken van gevoelige data.
5	Aanvullend: (a) De definitie en toepassing van (informatie)veiligheidseisen zijn opgenomen in informatie/data lifecycle management. (b) Bij het opstellen van (informatie)veiligheidseisen voor datamanagement wordt rekening gehouden met efficiëntie en kosten. (c*) Rapportage vanuit controlemechanismen. (d*) Audit rapportages

Referenties:

Normenkader Informatie-beveiliging HO 2015 ***05 Vertrouwelijkheid en Integriteit***	4.8 4.9
COBIT 4.1	AI3.3 AI6.1 DS5.9
COBIT 5	BAI03.10 DSS05.01
ISO 27K 2013	A.12.6.1 A.12.6.2
DNB 2014/2017	18.2
BIO 2019	12.6.1 12.6.1.1 12.6.2 12.6.2.1 Supplement BIG: 12.6.1.5
NIST Cybersecurity Framework	PR.MA-1 PR.MA-2 PR.IP-12 DE.CM-6 DE.CM-8 RS.MI-3

Datamanagement

9.4 (DM.04) Inrichting van opslag en retentie

Risico:

Het ontbreken van procedures betreffende gegevensopslag, bewaartermijnen en archivering leidt tot het niet behalen van bedrijfsdoelstellingen en het niet naleven van het (informatie)beveiligingsbeleid van de organisatie en van wet- en regelgeving.

Doelstelling:

Er zijn procedures gedefinieerd en geïmplementeerd voor het effectief en efficiënt opslaan, bewaren en archiveren van gegevens, zodat wordt voldaan aan organisatiedoelstellingen, het (informatie)beveiligingsbeleid van de organisatie en wettelijke vereisten.

Volwassenheidsniveaus:

1	(a) Er zijn geen procedures voor dataopslag, -bewaring en archivering. (b) Dataopslag is ongestructureerd.
2	(a) Er zijn beperkte eisen gedefinieerd voor dataopslagtechnieken. (b) Er zijn enkele informele richtlijnen voor bewaring en archivering.
3	(a) Er zijn formele procedures en richtlijnen voor het opslaan, bewaren en archiveren van data. (b) In lijn met bedrijfsvoering zijn er eisen gesteld aan het opslaan, bewaren en archiveren van data (technieken) en deze zijn geïmplementeerd. (c) Er is voor gezorgd dat deze eisen in overeenstemming zijn met (informatie)beveiligingsbeleid, contractuele afspraken en wet- en regelgeving.
4	Aanvullend: (a) Afspraken en maatregelen over het opslaan en bewaren worden periodiek geëvalueerd om te bewerkstelligen dat deze nog steeds in overeenstemming zijn met de organisatiedoelen. (b) De implementatie en uitvoering van relevante procedures voor het opslaan, bewaren en archiveren van data worden periodiek geëvalueerd. (c) Datamanagementtechnieken zoals Command Query Responsibility Segregation (CQRS, leesacties zijn gescheiden van schrijfacties) worden bewaakt of geïmplementeerd.
5	Aanvullend: (a) Data- en bewaarmaatregelen zijn onderdeel van informatie/data lifecycle management. (b) Implementatie, uitvoering en kosten van de data lifecycle managementprocedures worden regelmatig geëvalueerd en gerapporteerd aan het senior management. (c) Datamanagementtechnieken zoals Event Sourcing (ES) worden gevolgd of geïmplementeerd.

Referenties:

Normenkader Informatie-beveiliging HO 2015 ***04 Continuïteit***	4.3 4.4 4.8
COBIT 4.1	
COBIT 5	DSS05.01 DSS05.02 DSS05.07
ISO 27K 2013	A.12.2.1 A.12.6.1
DNB 2014/2017	18.2 20.1
BIO 2019	12.2.1 12.2.1.1 12.2.1.2 12.2.1.3 12.2.1.4 12.2.1.5 12.6.1 12.6.1.1
NIST Cybersecurity Framework	PR.DS-4 PR.DS-6 PR.DS-8 PR.IP-1 PR.IP-12 PR.PT-2, PR.PT-4 DE.CM-6 DE.CM-8

Datamanagement

9.5 (DM.05) Uitwisseling van (gevoelige) gegevens

Risico:

Ongeautoriseerde toegang tot bronnen (gegevens) verbonden met een netwerk of openbaarmaking van gevoelige informatie die over het netwerk wordt verzonden. Dit kan uiteindelijk leiden tot diefstal, corruptie, ongepast of ongeautoriseerd gebruik van informatiemiddelen.

Doelstelling:

(Cyber)beleid en procedures zijn vastgesteld en geïmplementeerd zodat aan bedrijfseisen voor de bescherming van gegevens en software wordt voldaan wanneer gegevens en software worden uitgewisseld binnen de organisatie of met een externe partij. Gevoelige transactiegegevens worden alleen uitgewisseld via een vertrouwd pad of medium waarbij (cyber)maatregelen zijn genomen om de authenticiteit van de inhoud, bewijs van versturen, bewijs van ontvangst en onweerlegbaarheid van de oorsprong aan te tonen.

Volwassenheidsniveaus:

1	(a) Er is geen beleid of richtlijn voor de uitwisseling van (gevoelige) data binnen de organisatie of met externe partijen. (b) De organisatie biedt de mogelijkheid om veilig bestanden en documenten uit te wisselen, maar deze mogelijkheden worden niet (consequent) gebruikt.
2	(a) Er is een informeel beleid voor data-uitwisseling. (b) De technieken voor veilige data-uitwisseling die de organisatie biedt worden door organisatiebreed gebruikt.
3	(a) Het (cyber)beleid en de procedures zijn gedefinieerd en geïmplementeerd om data en software te beschermen en uitwisseling mogelijk te maken. (b) Het (cyber)beleid is goedgekeurd door het senior management en wordt algemeen toegepast. (c) Bedrijfsdata wordt geclassificeerd naar de mate van vertrouwelijkheid. (d) Data die uitgewisseld wordt buiten de organisatie moet voor versturen versleuteld worden. (e) Logs van essentiële applicaties worden geëvalueerd en incorrecte of incomplete data-uitwisselingen worden tegengehouden. (f*) Kopie van gegevensuitwisselingsovereenkomst. (g*) Kopie van een verwerkersovereenkomst. (h*) Kopie van beleid en procedurebeschrijving voor scheiding van netwerken/ kopie netwerk architectuur (i*) Registratie van uitgegeven certificaten en/of tokens.
4	Aanvullend: (a) Voordat gevoelige data wordt verstuurd, wordt de verwerking ervan d.m.v. application controls gevalideerd. (b) De relevante applicaties die betrokken zijn bij het loggen en stoppen van incorrecte of incomplete data-uitwisselingen worden periodiek geëvalueerd. (c) Het data-uitwisselingsbeleid en diens effectiviteit worden periodiek geëvalueerd.
5	Aanvullend: (a) De data-uitwisselingsmethodiek wordt ondersteund door geautomatiseerde (real-time) tooling, workflow processing en geïntegreerde dashboards. (b) Er wordt periodiek gerapporteerd over data-uitwisseling.

Referenties:

Normenkader Informatie-beveiliging HO 2015 ***05 Vertrouwelijkheid en Integriteit***	1.14 4.15
COBIT 4.1	AI3.2 DS5.7
COBIT 5	BAI03.03 DSS02.03 DSS05.05
ISO 27K 2013	A.14.1.1 A.17.2.1
DNB 2014/2017	18.1
BIO 2019	14.1.1 14.1.1.1 17.2.1 Supplement BIG: 12.1.1.6
NIST Cybersecurity Framework	PR.DS-4 PR.IP-1 PR.IP-2 PR.IP-7 PR.IP-8 PR.PT-3 PR.PT-5 RS.CO-5 RS.AN-5

Datamanagement

9.6 (DM.06) Verwijdering van data

Risico:

Het niet-grondig verwijderen van informatie kan leiden tot niet-naleving van wet- en regelgeving of ongeoorloofde toegang tot (vertrouwelijke) informatie.

Doelstelling:

Er zijn (cyber)procedures vastgesteld en geïmplementeerd om ervoor te zorgen dat aan business requirements voor het beschermen van (gevoelige) gegevens en software wordt voldaan bij het verwijderen of overdragen van gegevens of hardware.

Volwassenheidsniveaus:

1	(a) Data wordt ad hoc verwijderd. (b) Er zijn geen formeel vastgelegde procedures voor opschoning en verwijdering van data.
2	(a) Er zijn informele procedures geïmplementeerd zodat apparatuur en media die gevoelige data bevatten worden verwijderd via een centraal punt in de organisatie. (b) De verantwoordelijkheden voor dataverwijdering zijn gedeeltelijk gedefinieerd.
3	(a) Er zijn (cyber)procedures formeel vastgelegd en geïmplementeerd om er op toe te zien dat er aan business requirements en wet- en regelgeving voor het beschermen van (gevoelige) data en software wordt voldaan wanneer data en hardware wordt verwijderd of overgedragen. (b) Apparatuur en media met gevoelige informatie worden zoveel mogelijk opgeschoond voor gebruik of verwijdering. (c) De verantwoordelijkheden voor verwijderingsprocedures zijn duidelijk gedefinieerd.
4	Aanvullend: (a) Niet-opgeschoonde apparatuur en media worden gedurende het verwijderingsproces op een beveiligde manier getransporteerd. (b) Verwijderde apparatuur en media met gevoelige informatie zijn gedocumenteerd zodat ze te traceren zijn. (c) De implementatie en uitvoering van relevante procedures voor dataverwijdering worden periodiek geëvalueerd. (d*) Vernietiging door leveranciers wordt gecontroleerd en er wordt verslag van gedaan.
5	Aanvullend: (a) Er is een procedure voor de verwijdering van actieve media van de media-inventaris bij verwijdering van het medium. (b) Er is een procedure voor het onderhoud van de inventaris zodat recente verwijderingen meegenomen worden in het logbestand. (c) Dataverwijdering is een integraal onderdeel van de informatie/data lifecycle management.

Referenties:

Normenkader Informatie-beveiliging HO 2015 ***03 Ruimtes en Apparatuur***	4.3 4.4 5.2 5.13 5.14 5.15
COBIT 4.1	DS5.9
COBIT 5	DSS05.01
ISO 27K 2013	A.9.1.2, A.12.2.1 A.13.1.1 A.13.1.2 A.13.1.3
DNB 2014/2017	19.1
BIO 2019	9.1.2 9.1.2.1 9.1.2.2 12.2.1 12.2.1.1 12.2.1.2 12.2.1.3 12.2.1.4 12.2.1.5 13.1.1 13.1.2 13.1.2.1 12.1.2.2 13.1.2.3 13.1.3 13.1.3.1
NIST Cybersecurity Framework	PR.DS-6 PR.DS-8 PR.IP-1 PR.IP-2 PR.IP-7 PR.IP-8 PR.IP-12 RS.CO-5 RS.AN-5 DE.CM-4 DE.CM-5

Identity & Access Management

10.1 (ID.01) Toegangsrechten

Risico:

Onjuiste toegangsregels en/of toegangsgroepen kunnen ervoor zorgen dat conflicten m.b.t. functiescheiding een negatief effect hebben op het bedrijfsproces en het functioneren van de toepassing.

Doelstelling:

De organisatie heeft toegangsgroepen (of rollen) gedefinieerd op basis van vastgestelde bedrijfsregels, waaronder functiescheiding, in een SOLL-autorisatiematrix. Er zijn procedures die tijdige initiatie en update in de SOLL-autorisatiematrices voor alle toepassingen regelen. Het management keurt wijzigingen in vastgestelde rechten voor toegangsgroepen (of rollen) goed. Alle gebruikers activiteiten zijn traceerbaar tot op het individu (bijv. gebaseerd op een combinatie van gebruikersnaam en wachtwoord of token of biometrische informatie).

Volwassenheidsniveaus:

1	(a) Er is geen beleid voor informatietoegang. (b) Afwezigheid van SOLL-autorisatie matrix. (c) Niet alle activiteiten kunnen getraceerd worden naar uniek identificeerbare gebruikers.
2	(a) Er is informeel beleid voor informatietoegang geïmplementeerd. (b) Een SOLL-autorisatie matrix is gedefinieerd maar niet formeel vastgesteld. (c) Activiteiten van gebruikers met veel rechten kunnen getraceerd worden naar uniek identificeerbare gebruikers. (d) De gedefinieerde rollen en toegangsrechten van gebruikers zijn conform organisatiebehoeften. (e) Functie-eisen zijn verbonden aan gebruikers-ID's.
3	(a) Het beleid en de SOLL-matrix voor toegangsrechten van gebruikers en rollen zijn gedefinieerd, formeel vastgesteld en gecommuniceerd en worden nauwgezet onderhouden. (b) De identificatie, authenticatie en autorisatie van gebruikers zijn geïmplementeerd en worden afgedwongen. (c) Toegangsrechten toegekend op basis van de SOLL matrix worden regelmatig vergeleken met de IST situatie. (d) Activiteiten van gebruikers kunnen worden getraceerd naar uniek identificeerbare gebruikers. (e) Gebruikers ID's en toegangsrechten worden bijgehouden in een centrale opslag.
4	Aanvullend: (a) (Kosten effectieve) technische en beleidsmatige maatregelen voor gebruikersidentificatie, gebruikersauthenticatie en het afdwingen van gebruikersrechten worden up-to-date gehouden en periodiek geëvalueerd en gedocumenteerd. (b) Op basis van de evaluaties worden verbeteringen bepaald.
5	Aanvullend: (a) De performance en verbeteringen van de toegangsregelsprocedure en toepassingen worden voortdurend gevolgd.

Referenties:

Normenkader Informatie-beveiliging HO 2015 ***05 Vertrouwelijkheid en Integriteit***	4.5 4.6
COBIT 4.1	DS11.5
COBIT 5	DSS04.08
ISO 27K 2013	A.12.3.1
DNB 2014/2017	11.4
BIO 2019	12.3.1 12.3.1.1 12.3.1.2 12.3.1.3 12.3.1.4 12.3.1.5
NIST Cybersecurity Framework	RC.RP-1 RC.IM-1 RC.IM-2

Identity & Access Management

10.2 (ID.02) Administratie van toegangsrechten

Risico:

Ongeautoriseerde toegang tot gegevens, applicaties, besturingssystemen en gerelateerde bronnen (bijvoorbeeld databasetabellen, wachtwoordtabellen, geheugen), veroorzaakt door een ontoereikend proces voor het toewijzen, bewaken, beoordelen en beëindigen van gebruikersrechten. Onjuiste toewijzing van gebruikerstoegangsrechten kan leiden tot conflicten m.b.t. functiescheiding met een negatief effect op bedrijfsprocessen en applicatieprestaties.

Doelstelling:

Toegangsrechten voor werknemers worden toegewezen in overeenstemming met toegewezen taakverantwoordelijkheden (bijvoorbeeld via op rollen gebaseerde toegang). Beheerprocedures zijn beschikbaar om activiteiten vast te stellen voor het aanvragen, uitgeven of sluiten van een account en de bijbehorende toegangsrechten voor gebruikers. De procedure omvat tevens de methode die door het senior management wordt gebruikt om deze activiteiten op de juiste wijze te autoriseren. Toegang wordt verschaft op basis van het need-to-know/need-to-have principe.

Volwassenheidsniveaus:

1	(a) Er is geen beleid voor gebruikersaccounts en en bijbehorende rechten. (b) Er is geen administratieve procedure voor het vastleggen van gebruikers en rollen. (c) Toegangsrechten worden op ad-hoc-wijze toegekend afhankelijk van individuen. (d) Gebruikers zouden meer rechten kunnen hebben dan volgens het 'need-to-know/have' principe nodig is.
2	(a) Er is informeel beleid voor alle gebruikersaccounts en toegangsrechten (intern, extern, administrator) en omstandigheden (normaal, noodgeval). (b) Er is een administratieve procedure voor het vastleggen van accounts en rechten, maar deze is niet formeel vastgesteld. (c) Toegang tot informatie is bepaald op basis van Risk Management en komt overeen met beleids- en beveiligingseisen. (d) Accounts en diens toegangsrechten worden geblokkeerd/ingetrokken als een gebruiker ontslag neemt of ontslagen wordt.
3	(a) Het beleid voor alle accounts en toegangsrechten is gedefinieerd, gedocumenteerd, formeel vastgesteld en gecommuniceerd. (b) Hieronder valt ook de toestemmingsprocedure voor de data-/of systeemeigenaar die toegangsrechten toekent. (c) Er is een geschikte functiescheiding voor het aanvragen, toekennen, implementeren en intrekken van toegangsrechten van gebruikers. (d) De toegangsrechten van werknemers zijn geïmplementeerd op basis van hun rollen. (e*) Kopie van een integriteitscode die bestemd is voor technische en functioneel beheerders (indien opgenomen in functieomschrijving of contract, kopie functieomschrijving of contract). (f*) Authenticatiecodes worden geautomatiseerd gegenereerd en beveiligd (via separaat kanaal) gecommuniceerd.
4	Aanvullend: (a) De toegangsrechten van werknemers worden periodiek vergeleken met hun verantwoordelijkheden. (b) Op basis van deze vergelijkingen worden verbeteringen voorgesteld.
5	Aanvullend: (a) De performance en verbetering van accountbeheer en gerelateerde toegangsrechten worden voortdurend gemonitord. (b) Tools (bijv. provisioning) voor Identity & Access Management zijn succesvol geïmplementeerd.

Referenties:

Normenkader Informatie-beveiliging HO 2015 ***05 Vertrouwelijkheid en Integriteit***	4.15
COBIT 4.1	DS3.1 DS3.2 DS3.3 DS3.4 DS3.5
COBIT 5	BAI04.01 BAI04.02 BAI04.03 BAI04.04 BAI04.05
ISO 27K 2013	A.12.1.3 A.17.2.1
DNB 2014/2017	
BIO 2019	12.1.3 12.1.3.1 17.2.1
NIST Cybersecurity Framework	

Identity & Access Management

10.3 (ID.03) Super Users

Risico:

Onvoldoende beheer van super-users kan leiden tot ongeoorloofde toegang tot programma's en gegevens of tot verstoring van IT-services.

Doelstelling:

Het management heeft maatregelen ingevoerd die ervoor zorgen dat super-user toegang beperkt is tot de juiste (beperkte) groep individuen en dat activiteiten die worden uitgevoerd met super-user accounts worden gemonitord. Super-user accounts moeten worden goedgekeurd door verantwoordelijk management.

Volwassenheidsniveaus:

1	(a) Er is geen beleid voor invulling en gebruik van super-user rechten. (b) Er is geen procedure voor het toekennen van super-user rechten. (c) Er is geen gedefinieerde groep individuen aan wie super-user rechten toegekend mogen worden.
2	(a) Er is een informeel beleid voor het gebruik en een informele procedure voor de toekenning van super-user rechten. (b) De individuen die geautoriseerd zijn om super-user rechten toe te kennen zijn goedgekeurd door het management. (c) Gebruik van de super-user rechten wordt vastgelegd en in geval van een incident geanalyseerd.
3	(a) Er is een formele procedure voor super-user rechten gedefinieerd, gedocumenteerd en gecommuniceerd. (b) Individuen met super-user rechten zijn vastgelegd en toekenning is goedgekeurd door het verantwoordelijke management. (c) Gebruik van de super-user rechten wordt gelogd en geëvalueerd.
4	Aanvullend: (a) Gebruik van de super-user rechten wordt voortdurend gemonitord. (b) De super-user procedure en de super-user toegang wordt periodiek geëvalueerd.
5	Aanvullend: (a) Op basis van de periodieke evaluaties wordt de super-user procedure verbeterd (als onderdeel van IAM). (b) Tekortkomingen en trends worden gerapporteerd aan het senior management.

Referenties:

Normenkader Informatie-beveiliging HO 2015 ***05 Vertrouwelijkheid en Integriteit***	4.14
COBIT 4.1	DS4.1 DS4.2
COBIT 5	DSS04.01 DSS04.02 DSS04.03
ISO 27K 2013	A.6.1.3 A.6.1.4 A.17.1.1 A.17.1.2
DNB 2014/2017	11.1
BIO 2019	6.1.3 6.1.3.1 6.1.3.2 17.1.1 17.1.2
NIST Cybersecurity Framework	RC.RP-1 RC.IM-1 RC.IM-2

Identity & Access Management

10.4 (ID.04) Noodtoegang (envelopprocedure/breek-het-glasprocedure)

Risico:

Het ontbreken van een adequate procedure voor noodtoegang kan leiden tot ongeoorloofde toegang tot programma's en gegevens of tot verstoring van IT-services.

Doelstelling:

Er is een noodprocedure vastgesteld om in geval van nood toegang tot accounts met super-user rechten te beheren, die door de organisatie wordt gevolgd.

Volwassenheidsniveaus:

1	(a) Er is geen noodprocedure. (b) Het gebruik van noodtoegang met super-user rechten wordt niet of ad hoc gemonitord.
2	(a) Er is een noodprocedure maar deze is niet formeel vastgesteld. (b) Er is bepaald welke individuen geautoriseerd zijn om tijdelijke super-user rechten toe te kennen. (c) Noodingrepen worden vastgelegd. (d) Na elke noodtoegang worden wachtwoorden gewijzigd.
3	(a) De formele noodprocedure is gedefinieerd, gedocumenteerd en gecommuniceerd. (b) Het gebruik van de noodprocedure wordt bijgehouden. (c) Het gebruik van de noodprocedure wordt geëvalueerd, samen met de uitgevoerde ingrepen met super-user rechten en wijzigingen van de noodwachtwoorden.
4	Aanvullend: (a) De implementatie en de uitvoering van de noodprocedure worden periodiek geëvalueerd.
5	Aanvullend: (a) Geautomatiseerde Privileged Access Management (PAM) tools zijn geïmplementeerd. (b) Op basis van de periodieke evaluaties worden de noodprocedure en diens implementatie verbeterd. (c) Tekortkomingen en trends worden aan het senior management gerapporteerd.

Referenties:

Normenkader Informatie-beveiliging HO 2015 ***05 Vertrouwelijkheid en Integriteit***	4.5 4.6
COBIT 4.1	DS4.9
COBIT 5	DSS04.07
ISO 27K 2013	A.12.3.1
DNB 2014/2017	11.3
BIO 2019	12.3.1 12.3.1.1 12.3.1.2 12.3.1.3 12.3.1.4 12.3.1.5
NIST Cybersecurity Framework	

Identity & Access Management

10.5 (ID.05) Periodieke beoordeling van toegangsrechten

Risico:

Ongeautoriseerde toegang tot het besturingssysteem, gegevens en applicaties (inclusief programma's, tabellen en gerelateerde bronnen) veroorzaakt door onjuiste toegangsrechten en onvoldoende bewaking van schending daarvan. Onjuiste toekenning van toegangsrechten aan gebruikers en niet tijdig intrekken van toegangsrechten kan leiden tot problemen op het gebied van scheiding van taken of ongeoorloofde toegang tot informatie waardoor bedrijfsprocessen en applicatieprestaties negatief beïnvloed worden.

Doelstelling:

Het management beoordeelt periodiek de gebruikerstoegang die geïmplementeerd is voor de relevante applicaties (IST-situatie) om de juistheid van geïmplementeerde accounts en rollen (de toegangsrechten) te bevestigen, en valideert dat toegangsrechten passend zijn voor toegewezen taken, zoals bepaald door de toegangsregels (SOLL-situatie). Elke onjuiste toegang die tijdens het beoordelingsproces wordt opgemerkt, wordt direct ingetrokken. Deze controle houdt in dat SOLL- en IST-matrices worden vergeleken door het verantwoordelijke management.

Volwassenheidsniveaus:

1	(a) Er is geen formeel vastgelegde procedure voor Identity & Access Management voor besturingssystemen en -applicaties. (b) Er is geen SOLL-situatie gedefinieerd. (c) Evaluatie wordt ad hoc door individuen gedaan.
2	(a) Er is een procedure voor Identity & Access Management voor besturingssystemen en -applicaties, maar deze is niet formeel vastgelegd. (b) Er worden ad hoc SOLL-IST-evaluaties uitgevoerd voor gebruikers met veel privileges (verkopers, leveranciers, zakenpartners).
3	(a) De procedures voor Identity & Access Management en SOLL-IST evaluaties zijn gedefinieerd, gedocumenteerd en formeel vastgelegd. (b) De SOLL en IST matrices worden voor alle gebruikers periodiek vergeleken, geëvalueerd en goedgekeurd door het management. (c) Ongepaste toegangsrechten worden ingetrokken. (d) De procedures voor Identity & Access Management en de SOLL-IST evaluaties worden periodiek geëvalueerd en zijn effectief.
4	Aanvullend: (a) Op basis van periodieke evaluaties worden de procedures voor het beheer van toegangsrechten en SOLL-IST evaluaties gereviewd en verbeterd (als onderdeel van IAM).
5	Aanvullend: (a) Tekortkomingen en trends worden automatisch gerapporteerd aan het senior management (en indien van toepassing worden toegangsrechten automatisch ingetrokken conform gerapporteerde uitzonderingen). (b) Periodiek worden er database checks uitgevoerd om de huidige processen te toetsen in relatie tot de functiescheidingsmatrix, waarbij er gekeken wordt naar ongebruikelijk transacties/ gebieden voor verbetering (bijv. d.m.v. procesmining technieken).

Referenties:

Normenkader Informatie-beveiliging HO 2015 ***06 Controle en Logging***	4.15
COBIT 4.1	DS11.1
COBIT 5	DSS01.01, DSS04.07
ISO 27K 2013	A.17.2.1
DNB 2014/2017	11.4
BIO 2019	17.2.1
NIST Cybersecurity Framework	RC.RP-1 RC.IM-1 RC.IM-2

Security Management

11.1 (SM.01) Security baselines

Risico:

Afwezige of onjuiste beveiligings-baselines kunnen leiden tot een afwijkende of inconsistente implementatie van beveiligingsparameters, wat uiteindelijk leidt tot ongeautoriseerde toegang of verstoring van IT-services.

Doelstelling:

Beveiligingsbaselines en richtlijnen voor IT-infrastructuur zijn vastgesteld om het risico van ongeoorloofde toegang tot IT-middelen te beperken. Beveiligingsbaselines worden formeel vastgelegd, periodiek geactualiseerd en goedgekeurd door het senior management. Verantwoordelijk IT-personeel wordt hiervan op de hoogte gesteld. Geïmplementeerde beveiligingsinstellingen voor IT-middelen worden periodiek beoordeeld op naleving van beveiligingsbaselines. Afwijkingen van de baselines zijn gedocumenteerd en goedgekeurd.

Volwassenheidsniveaus:

1	(a) Er zijn geen beveiligingsbaselines.
2	(a) Er zijn beveiligingsbaselines gedefinieerd voor belangrijkste IT-infrastructuurcomponenten. (b) Beveiligingsbaselines worden ad-hoc geïmplementeerd en afwijkingen van de baselines worden niet gedocumenteerd.
3	(a) Beveiligingsbaselines zijn gedefinieerd, goedgekeurd door het senior management en gecommuniceerd naar verantwoordelijk IT-personeel. (b) De geïmplementeerde beveiligingsinstellingen voor IT-middelen worden periodiek gecontroleerd op overeenstemming met de beveiligingsbaselines. (c) Resultaten worden gedocumenteerd, afwijkingen worden gedocumenteerd en goedgekeurd (of gecorrigeerd). (d) Voor nieuwe IT infrastructuur componenten en projectmanagement processen wordt implementatie van beveiligingsbaselines afgedwongen. (e) In hoeverre aan de baseline wordt voldaan wordt periodiek gerapporteerd aan het senior management.
4	Aanvullend: (a) Beveiligingsbaselines worden periodiek geëvalueerd en geactualiseerd (indien nodig).
5	Aanvullend: (a) Het bewaken van de mate waarin aan de beveiligingsbaselines wordt voldaan, wordt gedaan door middel van continuous monitoring/audittools. (b) Afwijkingen van de baselines worden real-time gerapporteerd en indien nodig gecorrigeerd.

Referenties:

Normenkader Informatie-beveiliging HO 2015 ***01 Beleid en Organisatie***	4.14
COBIT 4.1	
COBIT 5	DSS04.03 DSS04.04 DSS04.06
ISO 27K 2013	A.17.1.1 A.17.1.2
DNB 2014/2017	11.1
BIO 2019	17.1.1 17.1.2
NIST Cybersecurity Framework	RC.RP-1 RC.IM-1 RC.IM-2

Security Management

11.2 (SM.02) Authenticatiemechanismes

Risico:

Onjuiste authenticatie kan leiden tot ongeoorloofde toegang tot programma's/gegevens doordat misbruik wordt gemaakt van identiteiten van geautoriseerde gebruikers en/of niet alle activiteiten van gebruikers zijn herleidbaar tot unieke identificeerbare gebruikers.

Doelstelling:

Alle gebruikers (intern, extern en tijdelijk) en hun activiteiten op IT-systemen moeten uniek identificeerbaar zijn. Het management is verantwoordelijk voor de periodieke controle van de lijst met actieve ID's in relevante applicaties om te bepalen of unieke user-IDs zijn geïmplementeerd om traceerbaarheid te garanderen en ervoor te zorgen dat algemene en systeemaccounts geblokkeerd of op andere wijze beschermd zijn. Alle onjuiste of inactieve user-IDs die tijdens het controleproces worden opgemerkt, worden tijdig gedeactiveerd.

Volwassenheidsniveaus:

1	(a) Geen beleid voor beheer van gebruikersauthenticatie. (b) Geen procedure voor Identity & Access Management. (c) Authenticatie niet afgedwongen voor het verlenen van toegang. (d) Niet alle systeemprocessen en activiteiten van gebruikers kunnen getraceerd worden naar een uniek identificeerbare gebruiker. (e) Ad-hoc-maatregelen zijn afhankelijk van individuen.
2	(a) Er is een informeel beleid voor gebruikersauthenticatie. (b) Er zijn administratieve procedures voor identificatie, authenticatie en autorisatie van gebruikers maar deze zijn niet formeel. (c) Voor het verlenen van toegang wordt authenticatie afgedwongen. (d) Alle activiteiten van gebruikers kunnen getraceerd worden naar uniek identificeerbare gebruikers. (e) De rollen die zijn vastgelegd voor het verlenen van toegang zijn in lijn met de organisatiebehoeften, gebaseerd op need-to-know en goedgekeurd door de proceseigenaar. (f) Functie-eisen zijn gekoppeld aan user-IDs. (g) Systeem- of generieke user-IDs zijn beschermd.
3	(a) Formeel beleid en procedures voor gebruikersauthenticatie en Identity & Access Management zijn gedefinieerd, gedocumenteerd, geformaliseerd en gecommuniceerd. Hieronder valt ook de toestemmingsprocedure voor de data- of systeemeigenaar die toegangsrechten toekent. (b) Voor logische toegang tot alle systemen en bronnen wordt gebruik gemaakt van toegangsbepaling en authenticatiebeheer voor alle gebruikers. (c) Er is een strikte functiescheiding voor het aanvragen, toekennen, implementeren en intrekken van toegangsrechten van gebruikers. (d) User-IDs en toegangsrechten worden bijgehouden in een centrale opslag. (e) Ongepaste of inactieve gebruikersrechten worden tijdig uitgeschakeld. (f) Het gebruik van tweefactorauthenticatie wordt afgedwongen voor niet vertrouwde omgevingen en kritieke systemen.
4	Aanvullend: (a) De implementatie en uitvoering van relevante procedures worden periodiek geëvalueerd en vastgelegd. Op basis van deze evaluaties worden verbeteringen doorgevoerd.
5	Aanvullend: (a) De performance en verbetering van Identity & Access Management, authenticatietechnieken en -controls worden voortdurend gemonitord.

Referenties:

Normenkader Informatie-beveiliging HO 2015 ***05 Vertrouwelijkheid en Integriteit***	2.3
COBIT 4.1	PO7.8
COBIT 5	APO07.01
ISO 27K 2013	A.7.2.3 A.7.3.1 A.8.1.4 A.9.2.6
DNB 2014/2017	8.5
BIO 2019	7.2.3 7.3.1 8.1.4 9.2.6
NIST Cybersecurity Framework	

Security Management

11.3 (SM.03) Mobiele apparaten en telewerken

Risico:

Verloren of gestolen mobiele apparaten, het afluisteren of onderscheppen van draadloze communicatie, onbeveiligde persoonlijke (mobiele) systemen en het verspreiden van malware kunnen bedrijfsgegevens in gevaar brengen.

Doelstelling:

Het borgen van informatiebeveiliging bij het gebruik van mobiele apparaten en telewerkfaciliteiten. Mobile device management, versleuteling en bescherming tegen malware zijn aanwezig om de risico's te beperken.

Volwassenheidsniveaus:

1	(a) Beleid voor het gebruik en beveiliging van mobiele apparaten en/of telewerkfaciliteiten ontbreekt. (b) Procedures voor het aanvragen, goedkeuren, verstrekken en accepteren van mobiele apparaten en/of telewerkfaciliteiten ontbreken. (c) Bedrijfsgegevens worden mogelijk onversleuteld opgeslagen op mobiele apparaten.
2	(a) Er is informeel beleid voor het beveiligen van mobiele apparaten en/of telewerkfaciliteiten. (b) Er is een informele procedure voor het aanvragen, goedkeuren, verstrekken en accepteren van mobiele apparaten en/of telewerkfaciliteiten (c) Toegang tot een mobiel apparaat wordt alleen verleend na gebruik van een (sterk) wachtwoord. (d) Er worden geen bedrijfsgegevens opgeslagen op mobiele apparaten (zero footprint), of anders worden alleen versleutelde gegevens opgeslagen op een mobiel apparaat.
3	(a) Formeel beleid en procedures voor het beveiligen van mobiele apparaten en/of telewerkfaciliteiten worden gedocumenteerd en gecommuniceerd (mobile device management). (b) Anti-malware software op mobiele apparaten wordt up-to-date gehouden. (c) In geval van verlies of diefstal wordt de communicatie met gecentraliseerde applicaties afgesloten. (d) Er worden geen bedrijfsgegevens opgeslagen op telewerkfaciliteiten thuis of elders (zero footprint). (e) De vertrouwde (logische) werkplek is beschermd tegen malware. (f) Bedrijfsgegevens in niet vertrouwde omgevingen worden alleen afgedrukt na een risicobeoordeling.
4	Aanvullend: (a) De implementatie en uitvoering van mobile device management wordt periodiek geëvalueerd en gedocumenteerd. Op basis van evaluaties worden verbeteringen vastgesteld.
5	Aanvullend: (a) Prestaties en verbeteringen van beveiligde mobiele apparaten en/of telewerkfaciliteiten worden continu gemonitord.

Referenties:

Normenkader Informatie-beveiliging HO 2015 ***05 Vertrouwelijkheid en Integriteit***	2.2 6.6
COBIT 4.1	PO7.5 AI4.3 AI4.4
COBIT 5	APO07.02 BAI08.01 BAI08.02 BAI08.03 BAI08.04
ISO 27K 2013	A.6.1.4 A.7.2.2 A.12.1.1 A.14.2.9 A16.1.6
DNB 2014/2017	8.3 9.1 9.2
BIO 2019	6.1.4? 7.2.2 7.2.2.1 7.2.2.2 7.2.2.3 12.1.1 14.2.9 14.2.9.1 14.2.9.2 16.1.6 16.1.6.1 16.1.6.2 Supplement BIG: 6.1.7.2
NIST Cybersecurity Framework	PR.AT-1 PR.AT-2 PR.AT-3 PR.AT-4 PR.AT-5

Security Management

11.4 (SM.04) Logging

Risico:

Niet registreren en/of het ontbreken van periodieke beoordeling van logbestanden kan ertoe leiden dat ongepaste of ongebruikelijke activiteiten niet op tijd worden opgemerkt of dat er onvoldoende vervolgacties worden uitgevoerd.
Bewaartermijnen van logbestanden en toegangsrechten tot logbestanden zijn niet in overeenstemming met bedrijfseisen of wet- en regelgeving.

Doelstelling:

Eisen voor logging zijn gedefinieerd op basis van monitoring- en rapportagebehoeften en geïmplementeerd in systemen, databases en netwerkcomponenten.
Logs worden periodiek beoordeeld op indicaties van ongepaste of ongebruikelijke activiteiten en er worden adequate follow-up acties gedefinieerd.
Bewaartermijnen van logs en toegangsrechten zijn in lijn met de business requirements.

Volwassenheidsniveaus:

1	(a) Eisen voor logging zijn gedeeltelijk gedefinieerd en gedocumenteerd. (b) Logging wordt niet structureel en slechts ad hoc geëvalueerd en is afhankelijk van individuen.
2	(a) Eisen zijn gedocumenteerd maar niet formeel vastgelegd. (b) Er is een procedure voor de evaluatie van logging gedefinieerd maar niet formeel vastgelegd. (c) Logging is geïmplementeerd voor relevante IT-componenten en wordt periodiek geëvalueerd. (d) Activiteiten van administrators en operators worden ook gelogd en periodiek geëvalueerd. (e) Interne systeemklokken worden gesynchroniseerd. (f) Er zijn bewaartermijnen voor logs en toegangsrechten.
3	(a) Eisen voor logging zijn formeel vastgelegd; de procedures en toegepaste technieken voor het onderhouden, opslaan en evalueren van logging zijn gedocumenteerd, formeel vastgelegd, en gebaseerd op risico-analyse. (b) De procedure is conform business requirements. (c) Het loggen van ongebruikelijke activiteiten en incorrecte of gebrekkige logging wordt gedocumenteerd, geanalyseerd en opgevolgd met gepaste maatregelen.
4	Aanvullend: (a) De implementatie en uitvoering van relevante procedures en werkwijzes worden periodiek geëvalueerd en gedocumenteerd. Verbeteringen worden bepaald op basis van deze evaluaties.
5	Aanvullend: (a) Geautomatiseerde detectie en response technologie, zoals SIEM, is volledig geïmplementeerd. (b) De performance en verbeteringen van de logging procedures worden voortdurend bewaakt.

Referenties:

Normenkader Informatie-beveiliging HO 2015 ***06 Controle en Logging***	2.2 2.4 2.5 5.7
COBIT 4.1	PO7.4 DS7.1 DS7.2
COBIT 5	APO01.04 APO07.03 APO13.02
ISO 27K 2013	A.7.2.1 A.7.2.2 A.7.2.3 A.8.1.3 A.8.2.3 A.9.3.1 A.11.2.8 A.11.2.9 A.13.2.4
DNB 2014/2017	9.1 9.2
BIO 2019	7.2.1 7.2.1.1 7.2.2 7.2.2.1 7.2.2.2 7.2.2.3 7.2.3 8.1.3 8.1.3.1 8.1.3.2 8.2.3 9.3.1 9.3.1.1 11.2.8 11.2.9 11.2.9.1 11.2.9.2 11.2.9.3 11.2.9.4 13.2.4
NIST Cybersecurity Framework	PR.AT-1 PR.AT-2 PR.AT-3 PR.AT-4 PR.AT-5

Security Management

11.5 (SM.05) Testen van, inspectie van en toezicht op beveiliging

Risico:

Wanneer beveiligingsmaatregelen niet worden getest en inspectie en monitoring ontbreken, kan dit ertoe leiden dat ongebruikelijke en/of abnormale activiteiten niet tijdig worden gedetecteerd en/of aangepakt. Het niet onderhouden van de baseline voor informatiebeveiliging kan leiden tot onveilige implementatie van IT-componenten.

Doelstelling:

Implementatie van IT-beveiliging wordt proactief getest en bewaakt. IT-beveiliging moet regelmatig worden getoetst om ervoor te zorgen dat de door de organisatie goedgekeurde baseline voor informatiebeveiliging wordt gehandhaafd. Een log- en bewakingsfunctie maakt vroegtijdige preventie en/of detectie en daaropvolgende tijdige rapportage van ongebruikelijke en/of abnormale activiteiten die moeten worden aangepakt, mogelijk.

Volwassenheidsniveaus:

1	(a) De implementatie van IT-beveiliging wordt ad hoc getest. (b) Er zijn geen procedures of beleid.
2	(a) Er is een procedure met richtlijnen voor het testen van beveiligingsmaatregelen, maar deze focust vooral op het testen van units of componenten. (b) Penetratietesten of social engineering-oefeningen worden op ad-hoc-basis uitgevoerd. (c) Toezicht op ongebruikelijke of abnormale activiteiten vindt plaats door de logs achteraf te checken.
3	(a) Er zijn procedures en beleid voor het scannen, testen en beheren van IT beveiliging gedefinieerd en geïmplementeerd. Deze zijn goedgekeurd door het senior management. (b) Er is een beveiligingsbaseline geïmplementeerd voor alle IT componenten die essentieel zijn voor bedrijfsvoering. (c) Penetratietesten en social engineering testen worden gepland en periodiek uitgevoerd. (d) Er is een log- en controlefunctie ingericht voor vroegtijdige preventie en/of detectie en vervolgens tijdige melding van ongewone en/of abnormale activiteiten. Er wordt extra aandacht besteed aan cyber security dreigingen.
4	Aanvullend: (a) Alle IT componenten, netwerkapparatuur, diensten en applicaties zijn geïnventariseerd en elk component heeft een beveiligingsrisico-rating gekregen en wordt conform die rating gescand of getest. (b) Alle IT componenten die essentieel zijn voor bedrijfsvoering worden (automatisch) opgenomen in de CMDB en real-time gecontroleerd op beveiligingsincidenten, conform bedrijfsbehoeften. (c) Red teaming oefeningen worden gepland en periodiek uitgevoerd. (d) Het proces van security testen, surveillance en monitoring wordt periodiek geëvalueerd.
5	Aanvullend: (a) Het testen van IT beveiliging is opgenomen in de projectmanagement- en software-ontwikkelingsmethodieken, zodat beveiliging gegarandeerd meegenomen wordt in ontwerp-, ontwikkelings- en testeisen. Zo wordt het risico dat nieuwe of veranderende systemen kwetsbaarheden introduceren zoveel mogelijk beperkt. (b) Dreigingen op het gebied van cyber security worden voortdurend in de gaten gehouden door geautomatiseerde detectie en response technologie (bijv. SIEM).

Referenties:

Normenkader Informatie-beveiliging HO 2015 ***06 Controle en Logging***	NVT
COBIT 4.1	PO7.5
COBIT 5	APO07.02
ISO 27K 2013	
DNB 2014/2017	8.3
BIO 2019	
NIST Cybersecurity Framework	

Security Management

11.6 (SM.06) Patchmanagement

Risico:

Afwezigheid van patches of beveiligingsoplossingen kan ertoe leiden dat bekende kwetsbaarheden worden misbruikt om ongeautoriseerde toegang tot de IT-infrastructuur te verkrijgen.

Doelstelling:

Beschikbare patches en/of beveiligingsfixes worden geïnstalleerd in overeenstemming met vooraf vastgesteld en goedgekeurd beleid (inclusief dat voor besturingssystemen, databases en geïnstalleerde applicaties) en aanbevelingen van CSIRT en/of leveranciers.

Volwassenheidsniveaus:

1	(a) Er is geen beleid voor patchmanagement. (b) Individuele risicoanalyse voor kwetsbaarheden en patches. (c) Ad-hoc-installatie van patches en/of beveiligingsfixes.
2	(a) Er is een informeel beleid voor patchmanagement. (b) Risico's op kwetsbaarheden en installatie van patches/fixes worden gemanaged maar niet gedocumenteerd. (c) Patches worden vaak geïmplementeerd met onvoldoende oog voor informatiebeveiliging.
3	(a) Er is een formeel vastgelegd beleid voor patchmanagement. (b) Patchmanagement is op organisatieniveau geïmplementeerd en gedocumenteerd, in lijn met Change Management. (c) Patches worden in de basis overgenomen in samenwerking met CSIRT. (d) IT-personeel check handmatig de patchlevels van besturingssystemen, databases en applicaties.
4	Aanvullend: (a) De effectiviteit van patchmanagement wordt regelmatig geëvalueerd. Deze evaluaties worden gedocumenteerd en verbeteringen worden bepaald. (b) Patchmanagement wordt meer benaderd op basis van risico's (dan vanuit compliance).
5	Aanvullend: (a) Er zijn automatische controles op patchlevels en alerts voor IT-personeel (maar geen automatische installatie van patches). (b) Rapportages worden automatisch gegenereerd voor het senior management.

Referenties:

Normenkader Informatie-beveiliging HO 2015 ***04 Continuïteit***	3.2 3.14
COBIT 4.1	DS11.4
COBIT 5	DSS05.08
ISO 27K 2013	A.8.3.1 A.8.3.2 A.11.2.7
DNB 2014/2017	12.2
BIO 2019	8.3.1 8.3.1.1 8.3.1.2 8.3.2 8.3.2.1 8.3.2.2 11.2.7
NIST Cybersecurity Framework	PR.DS-1 PR.DS-2 PR.DS-5 PR.IP-6

Security Management

11.7 (SM.07) Threat en Vulnerability Management

Risico:

Gebrek aan inzicht in wie de organisatie zal aanvallen, hoe de organisatie zal worden aangevallen en welke kwetsbaarheden en aanvalspaden kunnen worden misbruikt om kritieke bedrijfsmiddelen te bereiken, verhoogt het risico dat een schadelijke inbreuk plaatsvindt.

Doelstelling:

Er is een proces voor Threat en Vulnerability Management geïmplementeerd om bedreigingen te identificeren en kwetsbaarheden, die kunnen leiden tot een verslechtering van de prestaties van of een aanval op bedrijfsmiddelen, tijdig te detecteren en te verhelpen. Het aantal aanvalsvectoren wordt ook beschouwd, waardoor de algehele blootstelling wordt verminderd.

Volwassenheidsniveaus:

1	(a) Er is geen proces voor Threat en Vulnerability Management. (b) Er wordt niet geautomatiseerd op kwetsbaarheden gescand. (c) Vrijwel alles wordt handmatig, systeem voor systeem, gedaan.
2	(a) Er is een eenvoudig en informeel Threat en Vulnerability Management proces geïmplementeerd. (b) Er is een vulnerability scanner, idealiter voor zowel web- als netwerkvectoren, die tevens scant op incorrecte configuratie van apparatuur. (c) Scanning gebeurt ad hoc.
3	(a) Er is een formeel vastgelegd proces voor Threat en Vulnerability Management (inclusief samenwerking met CSIRT) geïmplementeerd, gedreven vanuit compliance en bekende risico's. (b) Er is een tool voor het beoordelen van kwetsbaardheden die waarschijnlijk met scans vanuit verschillende bronnen gevoed wordt. (c*) Er is een overzicht van detectiemaatregelen, die worden ingezet (virusscanners, IDS, IPS); (d*) Gebruik, incidenten en follow-up van ingezette detectiemaatregelen worden gemonitord.
4	(a) Threat en Vulnerability Management (en patching) is geïmplementeerd als onderdeel van een ecosysteem in plaats van als losse entiteit. (b) Er is een geavanceerd en grondig proces geïmplementeerd voor kwetsbaarheid voor het valideren van kwetsbaarheden dat gebruik maakt van penetratietesten. (c) Het red team concept is geïmplementeerd voor formele penetratietesten. (d) Er wordt periodiek gerapporteerd over Threat en Vulnerability Management. (e) Het Threat en Vulnerability Management proces wordt periodiek geëvalueerd.
5	(a) De afdelingen IT-beveiliging en IT-operations implementeren processen om gezamenlijk de lifecycle van kwetsbaarheden te managen. (b) Het geïmplementeerde proces is cruciaal voor closed-loop Threat en Vulnerability Management, van bedreigingsidentificatie tot herstel en validatie. (c) Data voor Threat en Vulnerability Management is geïntegreerd met alle andere aspecten van IT-beveiliging en operations, om 'near real-time' aanpassingen in Security Management en netwerk- en datacentermanagement mogelijk te maken. (d) Metrics richten zich op het verbeteren van beveiliging, in plaats van enkel het rapporteren van kwetsbaarheden.

Referenties:

Normenkader Informatie-beveiliging HO 2015 ***04 Continuïteit***	3.7 4.8 4.15
COBIT 4.1	AI3.3
COBIT 5	BAI03.10
ISO 27K 2013	8.1, A.11.1.5 A.11.2.4 A.12.6.1 A.14.2.3 A.14.3.1 A.17.2.1
DNB 2014/2017	18.2
BIO 2019	11.1.5 11.2.4 12.6.1 12.6.1.1 14.2.3 14.3.1 17.2.1
NIST Cybersecurity Framework	PR.MA-1 PR.MA-2 PR.IP-12 DE.CM-6 DE.CM-8 RS.MI-3

Security Management

11.8 (SM.08) Beschikbaarheid en bescherming van infrastructuur

Risico:

Verstoring van de bedrijfsvoering door onveilige overdracht van wijzigingen naar de productie-infrastructuur, door systeemonderhoud of routinematig onderhoud.
Blootstelling van (gevoelige) IT-infrastructuur aan verminderde integriteit en beschikbaarheid door gebrek aan interne beheersing, beveiligingsmaatregelen en maatregelen ten behoeve van traceerbaarheid.

Doelstelling:

Interne beheers-, beveiligings- en auditmaatregelen worden geïmplementeerd tijdens configuratie, integratie en onderhoud van hardware en infrastructuursoftware om middelen te beschermen en beschikbaarheid en integriteit te waarborgen.
Verantwoordelijkheden voor het gebruik van gevoelige infrastructuurcomponenten zijn duidelijk gedefinieerd en bekend bij degenen die infrastructuurcomponenten ontwikkelen en integreren. Het gebruik ervan wordt gecontroleerd en geëvalueerd.

Volwassenheidsniveaus:

1	(a) Er is geen proces gedefinieerd voor de bescherming en beschikbaarheid van infrastructuurcomponenten. (b) Het belang van IT-infrastructuur wordt onderkend, maar er mist een consistente totaalaanpak. (c) Er is geen aparte testomgeving voor IT-infrastructuur.
2	(a) Infrastructuurbescherming en -beschikbaarheid wordt ondersteund door enkele (formele) procedures en het belang van IT-infrastructuur is duidelijk. (b) Voor enkele omgevingen is een aparte testomgeving voor IT-infrastructuur.
3	(a) Er is een helder gedefinieerd en door iedereen begrepen proces voor de bescherming en beschikbaarheid van de IT-infrastructuur. (b) De procesbeschrijving is in lijn met de business requirements en goedgekeurd door het senior management. (c) De verantwoordelijkheden voor het gebruik van gevoelige componenten van de infrastructuur zijn gedefinieerd en begrepen door de ontwikkelaars van infrastructuurcomponenten en degenen die ze implementeren. (d) Het testen betreft o.a. de functionaliteit, beveiliging, beschikbaarheid en integriteit, en evt. andere aanbevelingen van de leverancier. (e) Test- en productieomgevingen van de IT-infrastructuur zijn van elkaar gescheiden. (f) Alle applicatiesoftware wordt voor installatie getest in een gescheiden maar vergelijkbare omgeving van productie. De installatie van gelicenseerde software is conform richtlijnen van de leverancier.
4	Aanvullend: (a) Onderhoud van gevoelige IT-infrastructuurcomponenten wordt gelogd en regelmatig geëvalueerd door verantwoordelijk management. (b) Van alle infrastructuurdata en -software wordt een back-up gemaakt voor het uitvoeren van installatie- of onderhoudstaken. (c) De implementatie en uitvoering van relevante procedures worden periodiek geëvalueerd en gedocumenteerd.
5	Aanvullend: (a) De bescherming en beschikbaarheid van de infrastructuur is proactief afgeleid van de eisen binnen de organisatie ten aanzien van beveiliging en beschikbaarheid. (b) De infrastructuurcomponenten worden voortdurend bewaakt door geautomatiseerde detectie en responsetechnologie, bijv. SIEM, als integraal onderdeel van de infrastructuur.

Referenties:

Normenkader Informatie-beveiliging HO 2015 ***04 Continuïteit***	1.11 3.3 3.4 3.5 3.6 3.9 3.10 3.11 3.13
COBIT 4.1	DS12.2
COBIT 5	DSS01.04 DSS01.05 DSS05.05 DSS06.06
ISO 27K 2013	A.11.1.1 A.11.1.2 A.11.1.3 A.11.1.4 A.11.2.1 A.11.2.2 A.11.2.3 A.11.2.6 A.11.2.5
DNB 2014/2017	21.1
BIO 2019	11.1.1 11.1.1.1 11.1.2 11.1.2.1 11.1.3 11.1.3.1 11.1.4 11.1.4.1 11.1.4.2 11.2.1 11.2.2 11.2.3 11.2.6 11.2.5
NIST Cybersecurity Framework	

Security Management

11.9 (SM.09) Onderhoud van de infrastructuur

Risico:

Verstoringen in de bedrijfsvoering als gevolg van onveilige overdracht van wijzigingen in de productie-infrastructuur, systeem en routine-onderhoud.

Doelstelling:

Een strategie/plan voor het onderhoud van de infrastructuur is ontwikkeld en borgt dat wijzigingen worden beheerd in overeenstemming met de Change Management procedure van de organisatie, inclusief periodieke beoordelingen van organisatiebehoeften, patchmanagement, upgradestrategieën, risico's, beoordeling van kwetsbaarheden en beveiligingseisen.

Volwassenheidsniveaus:

1	(a) Er is geen proces gedefinieerd voor het onderhoud van de infrastructuur. (b) Wijzigingen aan de infrastructuur voor nieuwe applicaties worden gedaan zonder formele strategie of totaalplan. (c) Onderhoud wordt uitgevoerd op basis van incidenten/korte termijnplanning.
2	(a) Er is een informeel proces voor onderhoud van infrastructuur geïmplementeerd. (b) Onderhoud van IT-infrastructuur is niet gebaseerd op een gedefinieerde strategie en neemt organisatiebehoeften niet in overweging. (c) Enkele onderhoudsactiviteiten worden gepland en/of gecoördineerd. (d) Documentatie voor essentiële systeemsoftware wordt onderhouden.
3	(a) Er is een duidelijk, gedefinieerd en begrepen proces voor de onderhoud van IT infrastructuur. (b) De procesomschrijving is in lijn met changemanagement en goedgekeurd door het (senior) management. (c) Het proces ondersteunt de behoeften van essentiële business applicaties, is in lijn met IT en business strategieën en wordt consequent toegepast. (d) Onderhoud wordt gepland, ingeroosterd en gecoördineerd. (e) De documentatie voor systeemsoftware wordt onderhouden en periodiek geactualiseerd met leveranciersdocumentatie voor alle systemen.
4	Aanvullend: (a) Het onderhoudsproces van technische infrastructuur wordt consequent toegepast op alle IT componenten en focust zich op hergebruik. (b) Het proces is goed georganiseerd en proactief. (c) De IT infrastructuur ondersteunt de business applicaties adequaat. (d) De effectiviteit van de infrastructurele onderhoudsprocedures wordt periodiek geëvalueerd.
5	Aanvullend: (a) Het onderhoudsproces voor technische infrastructuur is proactief en in lijn met essentiële business applicaties en technische architectuur. (b) Er wordt regelmatig onderzoek gedaan naar de relevante organisatiebehoeften, patchmanagement, upgrade strategieën, risico's, beoordeling van kwetsbaarheden en beveiligingseisen. (c) Er worden "good practices" gebruikt voor technische oplossingen, en de organisatie is op de hoogte van de nieuwste platformontwikkelingen en managementtools. (d) Kosten worden bespaard door infrastructuurcomponenten te standaardiseren en automatisering toe te passen.

Referenties:

Normenkader Informatie-beveiliging HO 2015 ***03 Ruimtes en Apparatuur***	3.4 3.7 3.8 3.9 3.13
COBIT 4.1	DS12.3
COBIT 5	DSS05.05 DSS06.06
ISO 27K 2013	A.11.1.2 A.11.1.5 A.11.1.6 A.11.2.1 A.11.2.6
DNB 2014/2017	21.2
BIO 2019	11.1.2 11.1.2.1 11.1.5 11.1.6 11.2.1 11.2.6
NIST Cybersecurity Framework	PR.AC-2

Security Management

11.10 (SM.10) Cryptographic Key Management

Risico:

Bescherming betreffende de vertrouwelijkheid, authenticiteit of integriteit van informatie mislukt als gevolg van ontoereikende cryptografische technieken. Dit kan uiteindelijk leiden tot diefstal, corruptie, onjuist of ongeautoriseerd gebruik van informatiemiddelen.

Doelstelling:

Er zijn beleid en procedures voor het genereren, veranderen, intrekken, vernietigen, verspreiden, certificeren, opslag, invoer, gebruik en archivering van cryptografische sleutels om sleutels te beschermen tegen aanpassing en ongeautoriseerde toegang.

Volwassenheidsniveaus:

1	(a) Geen beleid of procedure voor Key Lifecycle Management.
2	(a) Er zijn informeel beleid en procedures voor Key Lifecycle Management.
3	(a) Er zijn formeel vastgelegd beleid en procedures voor Key Lifecycle Management. (b) Beschermende maatregelen zijn geïmplementeerd om informatie veilig met elkaar te kunnen delen (bv door toepassing van encryptie). (c) De vertrouwelijkheid en integriteit van private keys wordt afgedwongen. (d*) Er is een overzicht gehanteerde tools.
4	Aanvullend: (a) De effectiviteit van de procedures voor Cryptographic Key Management wordt periodiek geëvalueerd.
5	Aanvullend: (a) Op basis van de periodieke assessments worden de procedures voor het beheer van cryptografische sleutels geëvalueerd en verbeterd. Tekortkomingen worden gerapporteerd aan het senior management.

Referenties:

Normenkader Informatie-beveiliging HO 2015 ***05 Vertrouwelijkheid en Integriteit***	1.13 1.15 1.16 2.7 4.3 4.4 4.11 4.14
COBIT 4.1	DS2.3
COBIT 5	APO10.04
ISO 27K 2013	8.1 A.7.1.1 A.7.1.2 A.12.2.1 A.13.2.2 A.15.1.1 A.15.1.2 A.15.1.3 A.15.2.2
DNB 2014/2017	14.2
BIO 2019	7.1.1 7.1.1.1 7.1.2 7.1.2.1 12.2.1 12.2.1.1 12.2.1.2 12.2.1.3 12.2.1.4 12.2.1.5 13.2.2 15.1.1 15.1.1.1 15.1.1.2 15.1.1.3 15.1.2 15.1.2.1 15.1.2.2 15.1.2.3 15.1.2.4 15.1.2.5 15.1.2.6 15.1.3 15.1.3.1 15.2.2
NIST Cybersecurity Framework	ID.SC-1 ID.SC-2 ID.SC-3 ID.SC-4 ID.SC-5

Security Management

11.11 (SM.11) Network security

Risico:

Ongeautoriseerde toegang tot systemen verbonden met een netwerk of openbaarmaking van gevoelige informatie die over het netwerk wordt verzonden. Dit kan uiteindelijk leiden tot diefstal, corruptie, onjuist of ongeautoriseerd gebruik van informatiemiddelen.

Doelstelling:

Beveiligingstechnieken en bijbehorende beheerprocedures (bijv. firewalls, beveiligingsapparatuur, netwerksegmentatie en inbraakdetectie) worden gebruikt voor het autoriseren van toegangs- en besturingsinformatiestromen van en naar netwerken. Er wordt gebruik gemaakt van "best practices" op dit gebied (bijv. GovCert, ISO/IEC, ITSec).

Volwassenheidsniveaus:

1	(a) Er is geen netwerkbeveiligingsbeleid. (b) Er zijn geen procedures of richtlijnen. (c) Ad-hoc-risicoanalyse en het gebruik van maatregelen door individuen.
2	(a) Er is een informeel netwerkbeveiligingsbeleid. (b) Er worden procedures voor implementatie van netwerkbeveiliging gevolgd maar deze zijn niet formeel vastgesteld. (c) Best practices worden gebruikt maar niet op een gestructureerde manier.
3	(a) Er is een netwerkbeveiligingsbeleid vastgesteld en geïmplementeerd: procedures, richtlijnen en documentatie voor het beheer van essentiële netwerkcomponenten zijn ingericht en worden onderhouden. (b) Beveiligingstechnieken worden gebruikt voor toegangsautorisatie, beheer van informatiestromen en verschillende beveiligingszones. (c) Er wordt gebruik gemaakt van geschikte encryptie bij het transport van gevoelige data over niet vertrouwde netwerken.
4	Aanvullend: (a) De relevante procedures worden periodiek geëvalueerd op actualiteit en uitvoering. De uitkomsten hiervan worden gedocumenteerd. (b) Op basis van deze evaluaties worden verbeteringen doorgevoerd.
5	Aanvullend: (a) Op basis van de periodieke assessment worden de procedures geëvalueerd en verbeterd. Tekortkomingen worden gerapporteerd aan het senior management.

Referenties:

Normenkader Informatie-beveiliging HO 2015 ***05 Vertrouwelijkheid en Integriteit***	NVT
COBIT 4.1	DS4.4 DS4.5
COBIT 5	DSS04.02 DSS04.04 DSS04.05 DSS04.06
ISO 27K 2013	17.1.3
DNB 2014/2017	11.2
BIO 2019	17.1.3 17.1.3.1 17.1.3.2 17.1.3.3
NIST Cybersecurity Framework	

Security Management

11.12 (SM.12) Beheersing van malware-aanvallen

Risico:

Als er onvoldoende maatregelen zijn getroffen tegen kwaadaardige software en voor het installeren van actuele beveiligingspatches kan ten gevolge van ongeautoriseerde wijzigingen door niet-geautoriseerde gebruikers afbreuk worden gedaan en schade worden toegebracht aan de integriteit van informatiesystemen (en gegevens).
Dit kan uiteindelijk leiden tot diefstal, verminking en ongepast of ongeautoriseerd gebruik van informatie.

Doelstelling:

Preventie, detectie en correctiemaatregelen zijn aanwezig (met name actuele beveiligingspatches en virusscanning) in de hele organisatie om informatiesystemen en technologie te beschermen tegen malware (bijv. virussen, wormen, spyware, spam).

Volwassenheidsniveaus:

1	(a) Er is geen beleid voor het voorkomen van malware. (b) Er is geen (volledig) geautomatiseerde anti-malware software. (c) Er zijn geen (volledig) up-to-date virusdefinities.
2	(a) Er is anti-malwarebeleid, maar dit is niet formeel vastgelegd. (b) Er is antivirussoftware in gebruik. (c) De virusdefinities zijn up-to-date. (d) De meeste inkomende e-mails worden gefilterd op malware.
3	(a) Er is anti-malwarebeleid gedefinieerd, gedocumenteerd en gecommuniceerd. (b) Medewerkers zijn zich bewust van hun verantwoordelijkheid om zich aan het beleid te houden. (c) Geautomatiseerde antivirussoftware is in gebruik en formeel vastgelegd. (d) Beveiligingssoftware (versies en patches) wordt centraal gedistribueerd en bevat up-to-date virusdefinities. (e) Alle (inkomende en uitgaande) e-mail wordt gefilterd op spam en malware. (f) Er zijn maatregelen genomen om het verspreiden van malware te beperken.
4	Aanvullend: (a) De effectiviteit van het distributieproces, de gebruikelijke evaluatie van nieuwe bedreigingen en het filteren van de e-mails wordt periodiek geëvalueerd.
5	Aanvullend: (a) De periodieke assessments worden gebruikt om het beheersen van malware aanvallen te evalueren en te verbeteren. (b) Tekortkomingen worden aan het senior management gerapporteerd.

Referenties:

Normenkader Informatie-beveiliging HO 2015 ***04 Continuïteit***	1.4 2.1 2.5 2.7
COBIT 4.1	PO7.1 PO7.6
COBIT 5	APO07.01 APO07.05 APO07.06
ISO 27K 2013	A.6.1.1 A.7.1.1 A.7.1.2 A.13.2.4
DNB 2014/2017	8.1 8.4
BIO 2019	6.1.1 6.1.1.1 6.1.1.2 6.1.1.3 6.1.1.4 7.1.1 7.1.1.1 7.1.2 7.1.2.1 13.2.4 Supplement BIG: 8.1.2.3
NIST Cybersecurity Framework	

Security Management

11.13 (SM.13) Bescherming van beveiligingstechnologie

Risico:

Vertrouwelijkheid van beveiligingsdocumentatie komt in gevaar wanneer informatie en informatiesystemen beschikbaar zijn voor onbevoegde gebruikers en voor niet-geautoriseerde doeleinden kunnen worden gebruikt. De integriteit van informatiesystemen kan worden aangetast en beschadigd door ongeoorloofde wijzigingen door niet-geautoriseerde gebruikers als er onvoldoende maatregelen zijn getroffen. Dit kan uiteindelijk leiden tot diefstal, corruptie, onjuist of ongeautoriseerd gebruik van informatiemiddelen.

Volwassenheidsniveaus:

1	(a) Er zijn geen specifieke maatregelen getroffen om aan beveiliging gerelateerde technologie te beschermen. (b) Reguliere documentatie en beveiligingsdocumentatie worden op dezelfde manier opgeslagen.
2	(a) Er zijn beleid en procedures opgesteld om de gevolgen van een inbreuk in de beveiliging te beperken (deze bevatten specifiek beheersmaatregelen voor Configuration Management, applicatietoegang, databeveiliging en fysieke beveiligingseisen).
3	Aanvullend: (a) Beveiligingsfuncties zijn ontworpen om wachtwoordregels (bijv. minimum lengte, soort karakters, geldigheidsduur en voorkomen van hergebruik) te ondersteunen. (a) Toegang is geautoriseerd en op juiste wijze goedgekeurd.
4	Aanvullend: (a) Het toekennen en goedkeuren van toegang, mislukte toegangspogingen, geblokkeerde toegang en geautoriseerde toegang tot gevoelige bestanden of data worden geregistreerd.
5	Aanvullend: (a) Veiligheidsrapportage wordt door het systeem gegenereerd en gebruikt om (kwaadaardig) binnendringen via kwetsbaarheden van het netwerk te voorkomen. (b) De maatregelen zijn onderdeel van een jaarlijkse managementreview van veiligheidsvoorzieningen voor fysieke en logische toegang tot bestanden en data.

Doelstelling:

Technologie gerelateerd aan beveiliging is bestand gemaakt tegen manipulatie en beveiligingsdocumentatie wordt niet onnodig openbaar gemaakt.

Referenties:

Normenkader Informatie-beveiliging HO 2015 ***05 Vertrouwelijkheid en Integriteit***	
COBIT 4.1	PO7.2 DS7.1 DS7.2
COBIT 5	APO07.03
ISO 27K 2013	7.2 A.7.2.2
DNB 2014/2017	8.2
BIO 2019	7.2.2 7.2.2.1 7.2.2.2 7.2.2.3 Supplement BIG: 8.2.2.2
NIST Cybersecurity Framework	

Fysieke beveiliging

12.1 (PH.01) Fysieke beveiligingsmaatregelen

Risico:

Beveiligingsmaatregelen op fysieke locaties (voor IT-apparatuur) zijn niet in lijn met bedrijfseisen. Ongeautoriseerde fysieke toegang kan de integriteit en beschikbaarheid van IT-componenten in gevaar brengen.

Doelstelling:

Voor (kantoor)ruimtes heeft de organisatie fysieke beveiligingsmaatregelen vastgesteld en geïmplementeerd in overeenstemming met de bedrijfseisen, zodat de toegang tot informatiesystemen op passende wijze wordt beperkt en die er tevens voor zorgen dat risico's met betrekking tot diefstal, temperatuur, brand, rook, water, trillingen, terreur, vandalisme, stroomuitval, chemicaliën of explosieven effectief worden voorkomen, gedetecteerd en beperkt.
Toegang tot locaties, gebouwen en gebieden wordt gemotiveerd, geautoriseerd, geregistreerd en gemonitord. Dit geldt voor alle personen die het terrein betreden, inclusief personeel, tijdelijk personeel, klanten, leveranciers, bezoekers of welke andere derde partij dan ook.

Volwassenheidsniveaus:

1	(a) Er wordt geen fysiek beveiligingsbeleid gehanteerd. (b) De organisatie kan niet snel diefstal of aanvallen op gebouwen en apparatuur detecteren. (c) Het beheer van faciliteiten en apparatuur is afhankelijk van de bekwaamheid van enkele individuen.
2	a) Er zijn beleidskaders voor fysieke beveiliging, maar deze zijn niet volledig en worden niet consequent gehanteerd. Overtreding van regels wordt niet opgemerkt. (b) Fysieke beveiliging is een informeel proces en standaarden worden niet consequent toegepast binnen de organisatie.
3	(a) Er is een alomvattend, op risico's gebaseerd beleid inzake fysieke beveiliging, dat is gedocumenteerd, gecommuniceerd en wordt ondersteund door (toegangs)systemen ten behoeve van de bescherming en ondersteuning van medewerkers (tijdelijke werknemers, klanten, leveranciers, bezoekers, etc.) en voor incidentrespons en -rapportage. (b) Het beleid is goedgekeurd door het senior management. (c) Er zijn effectieve maatregelen genomen om bedreigingen en ongeautoriseerde toegang tot terrein en gebouwen of het meenemen van apparatuur te voorkomen, te detecteren en tegen te houden. (d) Fysieke beveiligingsmaatregelen zijn passend voor de organisatie en worden actief meegewogen vanaf de eerste fase van een eventuele verhuizing of verbouwing; er wordt rekening gehouden met ontwerp- en certificeringseisen voor zonering en controle. (e) Verantwoordelijkheden en eigenaarschap zijn duidelijk vastgesteld. (f*) Er is documentatie (gedocumenteerd beleid en procedurebeschrijvingen), waarin beheersmaatregelen voor de fysieke bescherming tegen schade door brand, stroomuitval, overstroming, aardschokken, explosies, oproer en andere vorm van natuurlijke of menselijke calamiteiten zijn beschreven. (g*) Beheersmaatregelen voor het beveiligen van de stroomvoorziening en beheersmaatregelen tegen interceptie of beschadiging van telecommunicatiekabels die voor dataverkeer of ondersteunende informatiediensten worden gebruikt tegen interceptie of beschadiging zijn beschreven en geïmplementeerd.
4	Aanvullend: (a) Het fysieke beveiligingsbeleid behandelt ook de veiligheid en bescherming van personeel en apparatuur wanneer deze niet op locatie zijn. Het beleid schrijft ook voor dat het management toezicht houdt op de effectiviteit van de beheersmaatregelen en het voldoen aan standaarden, en dat er in het risicomanagementproces rekening gehouden wordt met de mogelijkheid tot herstel van faciliteiten en apparatuur. (b) Voor alle faciliteiten is bepaald welke standaarden van toepassing zijn. Dit betreft o.a. terreinkeuze, bouw, bewaking, veiligheid van personeel, mechanica, elektronica en bescherming tegen omgevingsfactoren (bijv. brand, blikseminslag, overstroming) (c) Het voldoen aan het beleid wordt op ad-hoc basis geëvalueerd (door de 2nd line of defense).
5	Aanvullend: (a) Er is een goedgekeurde, lange termijnplanning voor de faciliteiten die essentieel zijn voor de ondersteuning van het terrein en de IT omgeving, gebaseerd op het beleid. (b) Alle faciliteiten zijn geïnventariseerd en geclassificeerd volgens het Risk Management proces. (c) Het al dan niet voldoen aan het beveiligingsbeleid wordt periodiek gerapporteerd aan het senior management. (d) Het beleid wordt jaarlijks geëvalueerd, geactualiseerd en opnieuw goedgekeurd door het senior management.

Referenties:

Normenkader Informatie-beveiliging HO 2015 ***03 Ruimtes en Apparatuur***	1.21 4.2
COBIT 4.1	PO4.11
COBIT 5	APO01.02
ISO 27K 2013	A.6.1.2 A.7.2.1 A.12.1.4
DNB 2014/2017	7.1
BIO 2019	6.1.2 6.1.2.1 7.2.1 7.2.1.1 12.1.4 12.1.4.1 12.1.4.2
NIST Cybersecurity Framework	

Fysieke beveiliging

12.2 (PH.02) Beheer van fysieke toegangsrechten

Risico:

Er zijn geen procedures gedefinieerd en geïmplementeerd om de toegang tot locaties, gebouwen en gebieden te verlenen, te beperken en in te trekken op basis van organisatiebehoeften, inclusief in noodsituaties. Toegang tot locaties, gebouwen en gebieden kan niet worden gerechtvaardigd, geautoriseerd, gelogd of gemonitord.
Hierdoor kunnen onbevoegden of kwaadwillenden zich ongecontroleerd/ongehinderd toegang tot de gebouwen, apparatuur of personeel verschaffen en de essentiële processen verstoren.

Doelstelling:

Procedures worden vastgesteld en gevolgd om toegang tot IT-kritieke ruimtes of datacenters (bijv. locaties, gebouwen en ruimten) toe te staan, te beperken en in te trekken, afhankelijk van organisatiebehoeften, inclusief noodtoegang. Adequate beveiligingsmaatregelen (zoals slot op deur, toegangssysteem met kaartsleutel, cijferslot, etc.) worden gebruikt om fysieke toegang tot computerfaciliteiten waarin zich belangrijke applicaties bevinden te beperken.

Volwassenheidsniveaus:

1	(a) Er zijn geen procedures vastgelegd voor de administratie van fysieke toegang. (b) Personeel heeft onbeperkt fysieke toegang tot het terrein, de gebouwen en de ruimtes van de organisatie. (c) Andere procedures voor beheer en bescherming van fysieke IT-eigendommen zijn niet of nauwelijks vastgelegd.
2	(a) Er zijn informele procedures om toegang tot specifieke ruimtes te beperken. (b) Fysieke beveiligingsdoelen zijn niet gebaseerd op formele standaarden of organisatiedoelen. (c) Onderhoudsprocedures voor de faciliteiten worden niet (goed) vastgelegd en hangen vooral af van de "good practices" van enkele individuen.
3	(a) Er worden formeel vastgelegde procedures voor de administratie van fysieke toegang toegepast. (b) Er worden beveiligingsmaatregelen en toegangsbeperkingen toegepast zodat alleen geautoriseerd personeel fysieke toegang heeft tot gebouwen, IT-kritieke omgevingen of data centers. (c) Toegang tot fysieke IT omgevingen (serverruimtes) wordt verleend op basis van functie en verantwoordelijkheden. (d) Werknemers moeten een zichtbare identificatie dragen en bezoekers worden geregistreerd en begeleid. (e) Er zijn procedures om de toegangsprofielen up-to-date te houden. (f) Er is een proces geïmplementeerd om alle toegangen tot fysieke IT omgevingen te controleren en te bewaken, waarbij alle bezoekers, inclusief leveranciers en onderhoudspersoneel, worden geregistreerd. (g) Verantwoordelijkheden en eigenaarschap zijn duidelijk toegewezen en gecommuniceerd. .
4	Aanvullend: (a) Daadwerkelijke toegang (en overtredingen van het toegangsbeleid) wordt streng gecontroleerd en periodiek bekeken. (b) Gestandaardiseerde technieken worden toegepast om omgevings- en veiligheidsfactoren voor fysieke beveiliging aan te pakken. (c) De doeltreffendheid van de autorisaties en het gebruik van de toe te passen standaarden worden door het management periodiek onderzocht. (d) Het management heeft doelen en metrics vastgesteld voor het beheer van fysieke IT omgevingen. (e) De operationele effectiviteit van de fysieke beveiligingsprocedures wordt periodiek geëvalueerd.
5	Aanvullend: (a) Toegangsbeheer wordt voortdurend gecontroleerd. (b) De omgeving wordt beheerd en bewaakt door gespecialiseerde apparatuur en hardware ruimtes worden niet meer "bemand". (c) Preventief onderhoudsprogramma's handhaven strikte tijdschema's, en gevoelige apparatuur wordt regelmatig getest en gecontroleerd. (d) Strategieën en standaarden voor faciliteiten zijn conform IT beschikbaarheidsdoelen en geïntegreerd in business continuity planning en crisismanagement. (e) De fysieke beveiligingsfaciliteiten worden door het management geëvalueerd en geoptimaliseerd op basis van de vastgestelde doelen en metrics.

Referenties:

Normenkader Informatie-beveiliging HO 2015 ***03 Ruimtes en Apparatuur***	5.1 5.5
COBIT 4.1	DS5.3 DS5.4
COBIT 5	DSS05.04
ISO 27K 2013	A.9.1.1 A.9.2.3 A.9.4.5 A.14.2.1
DNB 2014/2017	17.1
BIO 2019	9.1.1 9.2.3 9.2.3.1 9.4.5 14.2.1 14.2.1.1 Supplement BIG: 12.4.3.2
NIST Cybersecurity Framework	

IT operatie

13.1 (OP.01) Job processing

Risico:

Geautomatiseerde IT-taken, zowel eenmalig ingeplande als periodieke opdrachten ('batch processing') worden niet volgens plan uitgevoerd en afwijkingen van de planning worden niet geïdentificeerd en tijdig opgelost.

Doelstelling:

De organisatie heeft procedures voor geautomatiseerde job scheduling. Taakactiviteiten worden gecontroleerd en omvatten:

- het gebruik van interfaces tussen relevante systemen om te bevestigen dat de datatransmissies volledig, nauwkeurig en geldig zijn.
- de resultaten van de back-ups om de succesvolle uitvoering te bevestigen.

Storingen worden geregistreerd en opgelost via de procedure voor Incident Management.
De mogelijkheid om taakschema's, batchtaken en geautomatiseerde interfaces te wijzigen is beperkt tot geautoriseerde personen.

Volwassenheidsniveaus:

1	(a) Er zijn geen procedures vastgesteld voor job processing.
2	(a) Er zijn verschillende runbooks voor productietaken beschikbaar en deze beschrijven in het algemeen taken en interfaces voor de meest relevante systemen. (b) Job processing wordt lokaal (per afdeling) geïmplementeerd en er is geen correlatie tussen verschillende systemen. (c) Afwijkingen in (back-up) job scheduling worden niet centraal geregistreerd (via Incident Management).
3	(a) Een runbook voor job scheduling is beschikbaar en is afgestemd op de bedrijfsdoelstellingen (overeengekomen door systeem- of proceseigenaar). (b) Het runbook bevat gedetailleerde informatie en instructies. (c) Job processing en interfacebewaking worden centraal geïmplementeerd en worden centraal beheerd, inclusief de correlatie tussen verschillende systemen. (d) Uitzonderingen of afwijkingen in de job processing worden geregistreerd via het Incident Management proces.
4	Aanvullend: (a) Rapportage over job processing maakt deel uit van de rapportage over het service level. (b) De operationele effectiviteit van het job processing proces wordt periodiek geëvalueerd.
5	Aanvullend: (a) Speciale tooling wordt gebruikt om de job processing en de opvolging van daaraan gerelateerde afwijkingen te automatiseren (bijv. automatische herstart), afhankelijk van hoe belangrijk de taken zijn.

Referenties:

Normenkader Informatie-beveiliging HO 2015 ***06 Controle en Logging***	1.19 1.20 2.4 4.5 4.6 5.16 5.17
COBIT 4.1	DS11.6
COBIT 5	DSS01.01 DSS05.08 DSS06.05
ISO 27K 2013	A.8.2.3 A.8.3.1 A.8.3.3 A.11.2.9 A.12.3.1 A.13.2.3 A.14.1.2 A.14.1.3 A.14.3.1 A.18.1.3 A.18.1.4
DNB 2014/2017	12.3
BIO 2019	8.2.3 8.3.1 8.3.1.1 8.3.1.2 8.3.3 8.3.3.1 8.3.3.2 11.2.9 11.2.9.1 11.2.9.2 11.2.9.3 11.2.9.4 12.3.1 12.3.1.1 12.3.1.2 12.3.1.3 12.3.1.4 12.3.1.5 13.2.3 13.2.3.1 13.2.3.2 13.2.3.3 13.2.3.4 14.1.2 14.1.3 14.3.1 18.1.3 18.1.3.1 18.1.4 18.1.4.1 18.1.4.2
NIST Cybersecurity Framework	PR.DS-1 PR.DS-2 PR.DS-5 PR.IP-6 PR.PT-3 PR.PT-5

IT operatie

13.2 (OP.02) Procedures voor back-up en herstel

Risico:

Verlies van gegevens in geval van een systeemstoring of integriteitskwestie als gevolg van onnauwkeurige, onvolledige, niet tijdige back-up van kritieke gegevens en monitoring daarvan.

Doelstelling:

De organisatie heeft een strategie geïmplementeerd voor het maken van back-ups van relevante data en programma's. Back-up en herstelprocedures zijn formeel gedefinieerd en geïmplementeerd voor alle daarvoor aangewezen systemen. Het back-upschema en de retentieperiode zijn in lijn met de door de organisatie geaccepteerde risico's voor dataverlies gebaseerd op de gevoeligheid van het systeem en de kosten voor handmatig herstel. Herstelprocedures worden periodiek getest en gedocumenteerd.

Volwassenheidsniveaus:

1	(a) Er zijn geen procedures voor back-up en herstel.
2	(a) Er zijn procedures voor back-up en herstel van systemen, applicaties, data en documentatie. (b) Het back-upschema en de retentie-eisen zijn niet (volledig) in lijn met de eisen van de organisatie.
3	(a) Er zijn passende procedures en beleid voor de back-up van systemen, applicaties, data en documentatie, en deze nemen zowel organisatie- als beveiligingseisen in overweging. (b) Beleid en procedures zijn in lijn met organisatiebehoeften en goedgekeurd door het (senior) management. (c) De verantwoordelijkheden voor het maken, herstellen en bewaken van back-ups zijn duidelijk toegewezen. (d) Prioriteit voor dataherstel is gebaseerd op eisen die de organisatie heeft bepaald en procedures in het kader van de continuïteit van IT-diensten.
4	Aanvullend: (a) Door middel van het Risk Management model en IT-service continuïteitsplan wordt periodiek bepaald welke data essentieel is voor de organisatie. (b) Er worden periodiek voldoende hersteltesten uitgevoerd om te garanderen dat alle componenten van back-ups effectief en correct hersteld kunnen worden. (c) De operationele effectiviteit van back-up- en herstelprocedures worden periodiek geëvalueerd.
5	Aanvullend: (a) De performance van het back-up- en herstelproces wordt periodiek aan het (senior) management gerapporteerd en indien nodig worden verbeteringen voorgesteld. (b) De procedures zijn een belangrijk onderdeel van de disaster recovery planning van de organisatie. (c) Systemen, applicaties, gegevens en documentatie die door derden worden onderhouden of verwerkt, worden adequaat geback-upt of anderszins beveiligd. (d) Teruggave van back-ups door derden is verplicht en escrow- of deponeringsregelingen worden overwogen.

Referenties:

Normenkader Informatie-beveiliging HO 2015 *04 Continuïteit*	1.12 5.2 5.13 5.14 5.15 5.16
COBIT 4.1	DS5.11
COBIT 5	DSS05.02
ISO 27K 2013	A.9.1.2 A.13.1.1 A.13.1.2 A.13.1.3 A.13.2.1 A.13.2.3 A.14.1.2
DNB 2014/2017	18.5
BIO 2019	9.1.2 9.1.2.1 9.1.2.2 13.1.1 13.1.2 13.1.2.1 13.1.2.2 13.1.2.3 13.1.3 13.1.3.1 13.2.1 13.2.3 13.2.3.1 13.2.3.2 13.2.3.3 13.2.3.4 14.1.2
NIST Cybersecurity Framework	PR.DS-1 PR.DS-2 PR.DS-5 PR.IP-6

IT operatie

13.3 (OP.03) Capacity and Performance Management

Risico:

Prestaties en capaciteit worden niet goed en tijdig gemanaged, waardoor verstoringen van de bedrijfsvoering optreden wanneer de maximale capaciteit is bereikt of het prestatieniveau tot een minimum is gedaald.

Doelstelling:

De organisatie heeft procedures geïmplementeerd om ervoor te zorgen dat de prestaties en capaciteit van IT-services en de IT-infrastructuur de overeengekomen servicedoelstellingen op een kosteneffectieve en tijdige manier kunnen realiseren. Capacity and Performance Management houdt rekening met alle middelen die nodig zijn om de IT-service te leveren en met plannen voor korte-, middellange- en lange termijn business requirements, inclusief het voorspellen van toekomstige behoeften op basis van eisen voor werkbelasting, opslag en onvoorziene gebeurtenissen.

Volwassenheidsniveaus:

1	(a) Er is geen Capacity and Performance Management geïmplementeerd.
2	(a) Er is een proces (en technologie) geïmplementeerd om relatief eenvoudige tracking en handmatige rapportage van "raw performance metrics" op serverniveau te bewerkstelligen. (b) Rapportage is handmatig en ad hoc (vooral op basis van incidenten).
3	(a) Er is een proces (en technologie) gedefinieerd en geïmplementeerd om samenhangende tracking en geautomatiseerde rapportage van "raw performance metrics" op server- of partition niveau te bewerkstelligen. (b) De geautomatiseerde periodieke rapportage op basis van metrics wordt voor het grootste deel van de infrastructuur gedaan. Deze rapportages maken het signaleren van trends en problemen mogelijk en geven beperkt inzicht in toekomstige behoeften.
4	(a) Er is een proces (en technologie) voor volledig geautomatiseerde tracking, analyse en rapportage van metrics sterk gerelateerd aan business services. (b) Naast gegevens over de werkbelasting van systemen en applicaties wordt ook rekening gehouden met prestatie- en capaciteitsmetrics die sterk samenhangen met business of service metrics (bijv. configuratie, kosten, responstijden, etc.). (c) Er vindt periodiek geautomatiseerde, op uitzondering-georiënteerde analyse en rapportage plaats. (d) Het voorspellen van toekomstige behoeften wordt gedaan op basis van periodieke rapportage. (e) Operationele effectiviteit van de Capacity and Performance Management processen wordt periodiek geëvalueerd.
5	Aanvullend: (a) Belangrijke onderdelen van de infrastructuur en het applicatielandschap worden geanalyseerd om toekomstige behoeften te voorspellen. Dit wordt gestructureerd uitgevoerd om prestatie- en continuïteitsplanning te ondersteunen.

Referenties:

Normenkader Informatie-beveiliging HO 2015 ***04 Continuïteit***	1.1 1.2 1.6 1.21 3.1 5.1 5.3 5.6
COBIT 4.1	DS5.3
COBIT 5	DSS05.04 DSS06.03
ISO 27K 2013	A.5.1.1 A.6.1.2 A.6.2.1 A.6.2.2 A.9.1.1 A.9.2.1 A.9.2.4
DNB 2014/2017	17.1
BIO 2019	5.1.1 5.1.1.1 6.1.2 6.1.2.1 6.2.1 6.2.1.1 6.2.1.2 6.2.2 9.1.1 9.2.1 9.2.1.1 9.2.1.2 9.2.4
NIST Cybersecurity Framework	

Bedrijfscontinuïteitsmanagement

14.1 (BC.01) Bedrijfscontinuïteitsplanning

Risico:

Het ontbreken van aan risico gerelateerd inzicht in potentiële impact op de bedrijfsvoering en in de eisen betreffende herstelvermogen, alternatieve verwerking en herstel van alle kritieke IT-services.
Dit zou uiteindelijk kunnen leiden tot een grote verstoring van de belangrijkste bedrijfsfuncties.

Doelstelling:

Business- en IT-continuïteitsplannen worden ontwikkeld op basis van het framework en zijn ontworpen om de impact van een grote verstoring op de belangrijkste bedrijfsfuncties en bedrijfsprocessen te verminderen. De plannen zijn gebaseerd op risicogericht inzicht in potentiële bedrijfsimpact en houden rekening met vereisten betreffende veerkracht, alternatieve verwerkings- en herstelmogelijkheden in alle kritieke IT-services. De plannen omvatten ook gebruiksrichtlijnen, rollen en verantwoordelijkheden, procedures, communicatieprocessen en de testmethode.

Volwassenheidsniveaus:

1	(a) Er is geen bedrijfsgericht IT-continuïteitsplan. (b) De IT-organisatie heeft een beperkt en algemeen herstelplan voor het netwerk en de systemen.
2	(a) IT- (en uiteindelijk business-)continuïteitsplannen worden ontwikkeld op basis van een informeel (en beknopt) framework. Deze plannen zijn niet compleet en gebaseerd op een risico-gerelateerd begrip van potentiële bedrijfseffecten. (b) In het geval van een grote onderbreking kunnen betrokken belangrijke processen en systemen wellicht worden hersteld, maar herstelactiviteiten zullen waarschijnlijk ontoereikend zijn. (c) Als kritieke programma's/data verloren gaat en/of belangrijk personeel vertrekt, kunnen belangrijke businessprocessen gedurende een langere periode niet uitgevoerd worden.
3	(a) Business- en IT- continuïteitsplannen zijn gedefinieerd, geïntegreerd en goedgekeurd door het senior management. (b) De organisatie heeft een bedrijfsimpactanalyse uitgevoerd, op basis waarvan recovery-time doelen zijn bepaald en volledig gedocumenteerde IT-herstelplannen en business continuïteitsplannen zijn opgesteld om deze doelen te bereiken. (c) De plannen betreffen gebruikershandleidingen, rollen, verantwoordelijkheden, crisismanagement, communicatieprocessen en de testmethode. (d) Dankzij deze plannen kan de organisatie waarschijnlijk belangrijke operationele processen voortzetten in het geval van een grote onderbreking.
4	Aanvullend: (a) De continuïteitsplannen bevatten een roulerend schema van tabletop en live simulatietesten van de continuïteits- en crisismanagementplannen, waarin verbeteringen zijn doorgevoerd op basis van de resultaten van eerdere tests. (b) Tekortkomingen bij de uitvoering van continuïtiteitsplannen worden gerapporteerd.
5	Aanvullend: (a) Business continuïteitsplannen en gerelateerde processen worden periodiek geëvalueerd. (b) Zowel tekortkomingen in (de effectiviteit of efficiëntie van) de continuïteitsplannen als verbeteringen worden gerapporteerd aan het senior management.

Referenties:

Normenkader Informatie-beveiliging HO 2015 ***04 Continuïteit***	1.4 1.21 2.3 5.1 5.3 5.4 5.6 5.7 5.8 5.9 6.1
COBIT 4.1	DS5.4
COBIT 5	DSS05.04 DSS06.03
ISO 27K 2013	A.6.1.1 A.6.1.2 A.7.3.1 A.9.1.1 A.9.2.1 A.9.2.2 A.9.2.3 A.9.2.4 A.9.2.5 A.9.2.6 A.9.3.1 A.9.4.2 A.9.4.3 A.9.4.1
DNB 2014/2017	17.2
BIO 2019	6.1.1 6.1.1.1 6.1.1.2 6.1.1.3 6.1.1.4 6.1.2 6.1.2.1 7.3.1 9.1.1 9.2.1 9.2.1.1 9.2.1.2 9.2.2 9.2.2.1 9.2.2.2 9.2.2.3 9.2.3 9.2.3.1 9.2.4 9.2.5 9.2.5.1 9.2.5.2 9.2.5.3 9.2.6 9.3.1 9.3.1.1 9.4.2 9.4.2.1 9.4.2.2 9.4.3 9.4.3.1 9.4.3.2 9.4.3.3 9.4.3.4 9.4.3.5 9.4.1 9.4.1.1 9.4.1.2
NIST Cybersecurity Framework	PR.AC-1 PR.AC-3

Bedrijfscontinuïteitsmanagement

14.2 (BC.02) Testen van Disaster recovery

Risico:

Verstoringen van het bedrijfsproces door het inadequaat plannen en testen van IT-continuïteit (inclusief crisismanagement, rollen en verantwoordelijkheden, procedures, communicatieprocessen).

Doelstelling:

Bedrijfs- en IT-continuïteitsplannen worden regelmatig getest om ervoor te zorgen dat essentiële systemen en diensten effectief kunnen worden hersteld, dat tekortkomingen worden aangepakt en dat het plan relevant blijft. Dit vereist een zorgvuldige voorbereiding, documentatie, rapportage van de testresultaten en, afhankelijk van de resultaten, de implementatie van een actieplan. De mate van testherstel in afzonderlijke applicaties varieert van geïntegreerde testscenario's tot end-to-end-tests en geïntegreerde leverancierstests.

Volwassenheidsniveaus:

1	(a) Het testen van IT-continuïteitsplannen wordt niet of ad hoc uitgevoerd. (b) Er is een geïsoleerde testbenadering voor sommige kritieke applicaties en enkele eenvoudige hersteltests voor infrastructuurcomponenten.
2	(a) Het IT-continuïteitsplan wordt regelmatig getest (eenmaal per jaar). (b) Beperkte consolidatie van individuele hersteltestmethoden voor kritieke toepassingen. Het testen gebeurt meestal via geïsoleerde testen op individuele applicaties en onderliggende infrastructuur.
3	(a) Bedrijfs- en IT-continuïteitsplannen worden getest via goedgekeurde, geïntegreerde test-/herstelscenario's. (b) Bedrijfs- en IT-continuïteitsplannen worden op regelmatige basis getest (ten minste eenmaal per jaar) om ervoor te zorgen dat essentiële systemen effectief kunnen worden hersteld, dat tekortkomingen worden aangepakt en dat het plan up-to-date blijft. (c) Er is voorzien in een gedegen voorbereiding, documentatie, rapportage van de testresultaten en, afhankelijk van de resultaten, uitvoering van een actieplan.
4	Aanvullend: (a) Geïntegreerde bedrijfscontinuïteitstests worden uitgevoerd voor het volledige bedrijfskritische applicatie- en infrastructuurlandschap, d.w.z. een volledige failover-test inclusief het herstel van bedrijfsspecifieke activiteiten en werkplekken. (b) Bewezen hersteltools zijn aanwezig voor alle applicaties, en infrastructuurcomponenten, applicaties en services voor alle lagen zijn ondergebracht. (c) Er zijn succesvolle tests op meerdere niveaus voor applicaties en infrastructuurcomponenten. (d*) De testplannen voor bedrijfs- en IT-continuïteit worden periodiek herzien.
5	Aanvullend: (a) De organisatie slaagt standaard voor haar BC/DR-tests zonder grote tekortkomingen/uitzonderingen omdat haar procedures en capaciteiten over de duur van een paar jaar zijn gefinetuned. (b) Periodieke rapporten over de "geteste" effectiviteit van de continuïteitsplannen worden naar het senior management gestuurd.

Referenties:

Normenkader Informatie-beveiliging HO 2015 ***04 Continuïteit***	5.1 5.3 5.4 5.5 5.6 5.9 5.12 6.1 6.3
COBIT 4.1	DS5.4
COBIT 5	DSS05.04
ISO 27K 2013	A.9.1.1 A.9.2.1 A.9.2.2 A.9.2.3 A.9.2.4 A.9.2.5 A.9.4.2 A.12.4.2 A.12.4.3
DNB 2014/2017	17.2
BIO 2019	9.1.1 9.2.1 9.2.1.1 9.2.1.2 9.2.2 9.2.2.1 9.2.2.2 9.2.2.3 9.2.3 9.2.3.1 9.2.4 9.2.5 9.2.5.1 9.2.5.2 9.2.5.3 9.4.2 9.4.2.1 9.4.2.2 12.4.2 12.4.2.1 12.4.2.2 12.4.2.3 12.4.2.4 12.4.3
NIST Cybersecurity Framework	PR.AC-1 PR.AC-3

Bedrijfscontinuïteitsmanagement

14.3 (BC.03) Offsite back-upopslag

Risico:

Kritieke media worden niet offsite opgeslagen, waardoor back-upgegevens niet beschikbaar zijn in geval van een calamiteit in het datacenter. Back-ups van kritieke media worden niet periodiek getest, met als mogelijk gevolg dat gegevens niet kunnen worden hersteld omdat ze niet compatibel zijn met de huidige software en hardware systemen en -configuratie.

Doelstelling:

Alle kritieke back-upmedia, documentatie en andere IT-resources die nodig zijn in het kader van IT-herstel- en bedrijfscontinuïteitsplannen worden offsite opgeslagen. De inhoud van back-upopslag wordt bepaald in samenspraak met de eigenaren van bedrijfsprocessen en IT-personeel. Het beheer op de externe opslagfaciliteit werkt op basis van het beleid voor dataclassificatie en de gebruikelijk manier van mediaopslag van de organisatie. IT-management zorgt ervoor dat offsite-arrangementen periodiek, ten minste jaarlijks, worden beoordeeld op inhoud, bescherming tegen omgevingsfactoren en beveiliging. De compatibiliteit van hardware en software voor het herstellen van gearchiveerde gegevens is gewaarborgd en gearchiveerde gegevens worden periodiek getest en ververst.

Volwassenheidsniveaus:

1	(a) Back-upmedia worden niet, of slechts gedeeltelijk, offsite opgeslagen. (b) Er worden geen extra maatregelen genomen om verlies van data te voorkomen in geval van nood bij het primaire datacenter.
2	(a) De organisatie heeft een beknopte inventarisatie gedaan van kritieke media die offsite opgeslagen moeten worden. (b) De inhoud van back-ups wordt bepaald in onderling overleg tussen proceseigenaren en IT-personeel. (c) Er zijn maatregelen genomen om offsite back-upopslag van kritieke media te garanderen.
3	(a) Er is een gedetailleerd overzicht van alle kritieke media die offsite moeten worden opgeslagen. Dit overzicht is goedgekeurd door het senior management. (b) Er is een duidelijke omschrijving van benodigde maatregelen voor dataopslag gegeven aan management. Dit betreft offsite opslagfaciliteiten, transport, herstelinstructies, labeling en inventarisatie van back-upmedia. (c) De offsite faciliteiten zijn in lijn met de continuity eisen en worden periodiek geëvalueerd.
4	Aanvullend: (a) Het beheer van de offsite opslagfaciliteiten handelt op basis van dataclassificatiebeleid en de procedures voor mediaopslag van de organisatie. (b) Het IT-management evalueert periodiek de offsite faciliteiten, in het bijzonder inhoud, beveiliging en bescherming tegen omgevingsfactoren. (c) Back-updata wordt regelmatig getest en hersteld om de kwaliteit van de data te waarborgen. (d) De compatibiliteit van hardware en software betrokken bij het herstel van gearchiveerde data wordt periodiek getest.
5	Aanvullend: (a) De offsite faciliteiten worden voortdurend verbeterd. (b) Mirroring van kritieke media door middel van cloudoplossingen wordt toegepast wanneer real-time back-ups van kritieke media nodig zijn.

Referenties:

Normenkader Informatie-beveiliging HO 2015 ***04 Continuïteit***	5.5
COBIT 4.1	DS5.4
COBIT 5	DSS05.04
ISO 27K 2013	A.9.2.3
DNB 2014/2017	17.2
BIO 2019	9.2.3 9.2.3.1
NIST Cybersecurity Framework	PR.AC-1 PR.AC-3

Bedrijfscontinuïteitsmanagement

14.4 (BC.04) Gegevensreplicatie

Risico:

Afwezigheid van of verkeerd geconfigureerde datareplicatie kan betekenen dat kritische financiële en/of operationele gegevens niet (tijdig) beschikbaar zijn in geval van een incident.

Doelstelling:

Gegevensreplicatie is opgezet tussen de productiefaciliteit van de organisatie en de disaster-recoveryfaciliteit, zodat kritieke financiële en operationele gegevens op korte termijn beschikbaar zijn. Replicatiestatus wordt bewaakt als onderdeel van het bewakingsproces voor systeemtaken.

Volwassenheidsniveaus:

1	(a) Er is geen mogelijkheid tot datareplicatie.
2	(a) In geval van nood kan er datareplicatie plaatsvinden door middel van (extern opgeslagen) back-ups. (b) De organisatie accepteert het verlies van data tussen de laatste back-up en het moment van het incident.
3	(a) Er is een datareplicatieproces geïmplementeerd in de faciliteiten voor productie- en disaster recovery van de organisatie. (b) De organisatie heeft inzicht in welke financiële en operationele data essentieel is en dus gerepliceerd moeten worden. Dit is goedgekeurd door het senior management. (c) In het geval van een incident is data op korte termijn beschikbaar.
4	Aanvullend: (a) Er wordt toegezien op de status van replicatie, als onderdeel van het system jobs monitoring proces. (b) De kwaliteit van datareplicatie wordt minstens jaarlijks (gedeeltelijk) getoetst.
5	Aanvullend: (a) Er vinden wekelijks geautomatiseerde gedeeltelijke datareplicatietesten plaats. (b) Volledig herstel d.m.v. gerepliceerde data is een integraal onderdeel van jaarlijkse calamiteiten- en hersteltesten.

Referenties:

Normenkader Informatie-beveiliging HO 2015 ***04 Continuïteit***	1.14 2.4 5.13 5.14
COBIT 4.1	DS5.3
COBIT 5	DSS05.04 DSS06.02
ISO 27K 2013	A.9.4.1 A.11.2.9 A.13.1.1 A.13.1.2 A.14.1.1
DNB 2014/2017	17.1
BIO 2019	9.4.1 9.4.1.1 9.4.1.2 11.2.9 11.2.9.1 11.2.9.2 11.2.9.3 11.2.9.4 13.1.1 13.1.2 13.1.2.1 13.1.2.2 13.1.2.3 14.1.1 14.1.1.1
NIST Cybersecurity Framework	

Bedrijfscontinuïteitsmanagement

14.5 (BC.05) Crisismanagement

Risico:

Inadequaat crisismanagement kan leiden tot een inadequaat antwoord op calamiteiten met uiteindelijk tot gevolg dat business verloren gaat.

Doelstelling:

De organisatie heeft crisismanagement ingericht om snel, grondig en gecoördineerd op incidenten te reageren, de gevolgen te verminderen en de dienstverlening binnen een redelijke tijd te herstellen.

Volwassenheidsniveaus:

1	(a) Er zijn geen crisismanagementplannen of -procedures.
2	(a) Er is een proces voor crisismanagement, maar deze is slechts gedeeltelijk geïmplementeerd. (b) Er is een crisismanagamentteam, maar de verantwoordelijkheden, taken en benodigde acties zijn informeel en ad hoc.
3	(a) Er is een crisismanagementplan dat onderdeel is van het Business Continuïteit Plan (BCP), waardoor de organisatie de essentiële bedrijfsvoering weer kan oppakken, terwijl het crisismanagementteam zich op de crisis richt. (b) Alle betrokkenen zijn op de hoogte van de verantwoordelijkheden tijdens een crisis. (c) Er zijn periodiek crisisoefeningen voor crisismanagementteams.
4	Aanvullend: (a) Er zijn specifieke herstelscenario's gedefinieerd, waarbij voor elk scenario is bepaald hoe wordt omgegaan met de media en wat gecommuniceerd wordt. (b) Periodiek vindt een algehele oefening van het crisismanagement plaats om het hele proces, inclusief rampverklaring en escalatieprocedures, te valideren.
5	Aanvullend: (a) Er worden verbeteringen bepaald en geïmplementeerd op basis van de oefeningen van het crisismanagementteam. (b) Resultaten en verbeteringen worden gerapporteerd aan het senior management.

Referenties:

Normenkader Informatie-beveiliging HO 2015 ***04 Continuïteit***	1.9 1.10 5.10 5.11 5.16
COBIT 4.1	DS5.8
COBIT 5	DSS05.02 DSS05.03
ISO 27K 2013	A.10.1.1 A.10.1.2 A.13.2.3 A.18.1.5
DNB 2014/2017	18.3
BIO 2019	10.1.1 10.1.1.1 10.1.1.2 10.1.2 10.1.2.1 10.1.2.2 13.2.3 13.2.3.1 13.2.3.2 13.2.3.3 13.2.3.4 18.1.5 18.1.5.1
NIST Cybersecurity Framework	PR.IP-1 PR.IP-2 PR.IP-7, PR.IP-8, RS.CO-5, RS.AN-5

Ketenbeheer

15.1 (SC.01) Service level overeenkomst

Risico:

Overeengekomen serviceniveaus voldoen niet aan bedrijfsdoelstellingen of wettelijke eisen.

Doelstelling:

IT-services die aan de organisatie worden geleverd, worden gedefinieerd in het contract en bijhorende SLA. Er zijn maatregelen genomen om ervoor te zorgen dat diensten voldoen aan de huidige en toekomstige behoeften van de organisatie.

Volwassenheidsniveaus:

1	(a) Er is geen contract met bijbehorend service level agreement (SLA).
2	(b) Er zijn enkele afspraken gemaakt over service levels. (c) Er zijn geen afspraken gemaakt over periodieke rapportage over geleverde diensten.
3	(a) Service levels van IT-diensten zijn gebaseerd op business requirements. (b) SLA bevat afspraken over periodieke rapportage van geleverde diensten en performance. (c) De gedefinieerde serviceniveaus zijn gedocumenteerd in een SLA en formeel goedgekeurd door het (senior) management en de IT-service provider. (d*) Kopie procesbeschrijving van het controleren en beoordelen van dienstverlening door een derde partij (bv TPM, ISAE3402 of ISO27001).
4	Aanvullend: (a) Specifieke afspraken over informatiebeveiliging zijn in de SLA opgenomen. (b) Afspraken over het beëindigen van diensten (bijv. exit clausule, escrow, dataoverdracht/-vernietiging) zijn onderdeel van de SLA.
5	Aanvullend: (a) Criteria voor beveiligingsincidenten zijn gedefinieerd en beveiligingsincidenten worden separaat inzichtelijk gemaakt, naast incidenten veroorzaakt door gebreken of defecten.

Referenties:

Normenkader Informatie-beveiliging HO 2015 ***01 Beleid en Organisatie***	5.13 5.14 5.15
COBIT 4.1	DS5.10
COBIT 5	DSS05.02
ISO 27K 2013	A.13.1.1 A.13.1.2 A.13.1.3
DNB 2014/2017	18.4
BIO 2019	13.1.1 13.1.2 13.1.2.1 13.1.2.2 13.1.2.3 13.1.3 13.1.3.1
NIST Cybersecurity Framework	PR.AC-3 PR.AC-5 PR.IP-1 PR.IP-2 PR.IP-7 PR.IP-8 PR.IP-12 RS.CO-5 RS.AN-5 DE.CM-8 RS.MI-3

Ketenbeheer

15.2 (SC.02) Service Level Management

Risico:

Gebrek aan beheer en monitoring van de levering van diensten waardoor afwijkingen in de prestaties van leveranciers niet op tijd worden gedetecteerd. Trends in prestatiestatistieken voor specifieke en algemene diensten worden niet geïdentificeerd en niet opgevolgd, wat kan leiden tot een afname van de algemene bedrijfsprestaties.

Doelstelling:

Business requirements en de manier waarop IT-services en serviceniveaus bedrijfsprocessen ondersteunen, worden periodiek geanalyseerd. Services en serviceniveaus worden besproken en overeengekomen met de organisatie en vergeleken met het huidige serviceportfolio om nieuwe of gewijzigde services of serviceniveau-opties te identificeren.

Volwassenheidsniveaus:

1	(a) Er is geen proces voor Service Level Management.
2	(a) Er is een proces voor Service Level Management gedefinieerd, maar beheer en rapportage van service levels zijn niet formeel vastgelegd en/of organisatiebreed geïmplementeerd.
3	(a) Er is een proces voor Service Level Management gedefinieerd, geïmplementeerd en goedgekeurd door het (senior) management. (b) De performance van de services worden periodiek gerapporteerd in een service level rapport (SLR), en indien nodig besproken met de leverancier.
4	Aanvullend: (a) De requirements voor service-onderdelen worden periodiek vergeleken met de daadwerkelijke prestaties van de geleverde onderdelen, en wanneer deze niet voldoen aan de formele SLA levels/requirements wordt actie ondernomen. (b) De operationele effectiviteit van het Service Level Management proces wordt minstens één keer per jaar geëvalueerd. Indien nodig worden verbeteringen aangebracht.
5	Aanvullend: (a) Veranderende business requirements worden bekeken in de context van het huidige service portfolio om eventuele behoefte aan nieuwe of verbeterde services en service level mogelijkheden te identificeren.

Referenties:

Normenkader Informatie-beveiliging HO 2015 *06 Controle en Logging*	1.6 2.4 2.6 3.1 3.8 3.9 3.11 3.15 4.7 4.8 4.12 4.13 5.9 5.12 5.13 5.14 6.2 6.3 6.8 6.10
COBIT 4.1	DS5.7
COBIT 5	DSS05.05
ISO 27K 2013	A.6.2.1 A.6.2.2, A.9.4.2, A.9.4.4, A.11.1.6 A.11.2.1 A.11.2.3 A.11.2.8 A.11.2.9 A.12.4.1 A.12.4.2 A.12.4.3 A.12.4.4 A.12.5.1 A.12.6.1 A.13.1.2 A.16.1.3 A.16.1.4 A.16.1.5 A.16.1.7 A.18.2.3
DNB 2014/2017	20.1
BIO 2019	6.2.1; 6.2.1.1; 6.2.1.2; 6.2.2 9.4.2; 9.4.2.1 9.4.2.2; 9.4.4; 9.4.4.1; 9.4.4.2; 11.1.6; 11.2.1; 11.2.3; 11.2.8; 11.2.9; 12.4.1; 12.4.1.1; 12.4.1.2; 12.4.1.3; 12.4.1.4; 12.4.1.5; 12.4.2; 12.4.2.1; 12.4.2.2; 12.4.2.3; 12.4.2.4; 12.4.3; 12.4.4; 12.5.1; 12.6.1; 12.6.1.1; 13.1.2; 13.1.2.1; 13.1.2.2; 13.1.2.3; 16.1.3; 16.1.3.1; 16.1.4; 16.1.4.1; 16.1.5; 16.1.7; 16.1.7.1; 18.2.3; 18.2.3.1;
NIST Cybersecurity Framework	PR.DS-4 PR.DS-6 PR.DS-8 PR.IP-1 PR.IP-2 PR.IP-7 PR.IP-8 PR.IP-12 PR.PT-2 PR.PT-4 DE.CM-8 RS.CO-5 RS.AN-5 RS.MI-3

Ketenbeheer

15.3 (SC.03) Supplier Risk Management

Risico:

Geen op risico gebaseerd toezicht die non-disclosure agreements (NDA's), aanbetalingsovereenkomsten, blijvende levensvatbaarheid van de leverancier, naleving van beveiligingseisen, alternatieve leveranciers, conventionele vergoedingen en bonussen in overweging nemen.
Gebrek aan juridisch toezicht waardoor contracten niet worden opgesteld in overeenstemming met de eisen van de organisatie of wet- en regelgeving.

Doelstelling:

Risico's met betrekking tot het vermogen van leveranciers om effectieve dienstverlening op een veilige en efficiënte manier voort te zetten worden voortdurend geïdentificeerd en beperkt. Contracten voldoen aan universele zakelijke standaarden in overeenstemming met wet- en regelgeving. Risk Management neemt aspecten als niet-openbaarmakingsovereenkomsten (NDA's), escrow-contracten, voortdurende levensvatbaarheid van de leverancier, conformiteit met beveiligingseisen, alternatieve leveranciers, boetes en beloningen, enz. in overweging.

Volwassenheidsniveaus:

1	(a) Er is geen proces voor Supplier Risk Management. (b) Contracten en/of SLA's worden getekend zonder een gedegen risicoanalyse van de externe partij.
2	(a) Er is een proces voor risicomanagement van leveranciers gedefinieerd, maar deze is slechts gedeeltelijk geïmplementeerd. (b) Voor cloud computing wordt een checklist gebruikt voor een snelle analyse van de provider. (c) De geïdentificeerde risico's worden zelden gedocumenteerd en/of gerapporteerd.
3	(a) Er is een proces voor leveranciersrisicomanagement gedefinieerd, geïmplementeerd en goedgekeurd door het (senior) management. (b) Risico's betreffende het vermogen van de leverancier om effectief en veilig (cloud)diensten te leveren worden voortdurend geanalyseerd en beperkt. (c) In het proces voor Supplier Risk Management wordt rekening gehouden met non-disclosure agreements (NDA's), escrow contracten, levensvatbaarheid van leveranciers, compliance met beveiligingseisen, alternatieve leveranciers, boetes en beloningen, etc. (d) Over niet-gemitigeerde of geaccepteerde risico's wordt periodiek aan het (senior) management gerapporteerd. (e) Contracten zijn conform algemene bedrijfsstandaarden en voldoen aan wet- en regelgeving (e.g. data privacy). (f) Voordat de contracten worden ondertekend wordt een assurance verkregen, die aantoont dat de levering van diensten voldoet aan wet- en regelgeving en ook aan het eigen (beveiligings)beleid). (g*) Eisenset(s) zijn gedocumenteerd.
4	Aanvullend: (a) De operationele effectiviteit van het proces voor Supplier Risk Management wordt jaarlijks geëvalueerd. Eventuele verbeteringen worden aangebracht en geëvalueerd. (b) Als onderdeel van het proces voor Supplier Risk Management worden interne beheersmaatregelen (zoals beveiligingsmaatregelen) bij de externe partij of provider regelmatig geëvalueerd.
5	Aanvullend: De risico's met betrekking tot het vermogen van de leverancier om effectieve dienstverlening op een veilige en efficiënte manier voort te zetten, worden voortdurend onderzocht en beperkt.

Referenties:

Normenkader Informatie-beveiliging HO 2015 ***04 Continuïteit***	NVT
COBIT 4.1	AI7.5
COBIT 5	BAI07.02
ISO 27K 2013	
DNB 2014/2017	
BIO 2019	
NIST Cybersecurity Framework	

Ketenbeheer

15.4 (SC.04) Interne beheersing bij derden

Risico:

"De IT-beheersomgeving en het IT-beheersframework van derden voldoet niet aan de organisatiedoelstellingen. Externe dienstverleners voldoen niet aan wet- en regelgeving en contractuele verplichtingen.
Hierdoor voldoet de organisatie zelf ook niet aan relevante wet- en regelgeving of verliest vertrouwelijkheid, integriteit en/of beschikbaarheid van zijn data."

Doelstelling:

De status van de interne beheersmaatregelen van externe dienstverleners wordt beoordeeld. Er zijn procedures om te zorgen dat externe dienstverleners voldoen aan wet- en regelgeving en contractuele verplichtingen.

Volwassenheidsniveaus:

1	(a) Interne beheersing van externe partijen wordt niet geëvalueerd.
2	(a) Er zijn enkele procedures gedefinieerd voor adequate interne beheersing door externe partijen.
3	(a) Er is een formeel vastgelegd proces om te zorgen dat interne beheersing effectief toegepast wordt. (b) De status van de interne beheersmaatregelen van de externe dienstverleners wordt periodiek geëvalueerd. (c) Er zijn procedures om te garanderen dat externe dienstverleners zich aan de contractuele verplichtingen houden.
4	Aanvullend: (a) Er zijn procedures om te garanderen dat externe dienstverleners zich aan wet- en regelgeving houden (bijv. data privacy). "(b) Verdere inzicht in deze assurance wordt ook verkregen en opgevolgd door: • een extern audit rapport (bijv. SOC2, ISAE3402/SSAE16 of TPM), • te steunen op een intern audit rapport van de service provider (nadat de bekwaamheid van interne audit gevalideerd is). • door gebruikmaking van de ""recht op audit"" clausule."
5	Aanvullend: (a) Geautomatiseerde tooling en/of uitgebreide service level rapporten bieden de organisatie maandelijks inzicht in de ontwikkeling van interne beheersmaatregelen van externe partijen.

Referenties:

Normenkader Informatie-beveiliging HO 2015 ***06 Controle en Logging***	Vertrouwelijkheid en integriteit - cluster 5 NVT
COBIT 4.1	
COBIT 5	DSS01.04, DSS05.03, DSS06.06
ISO 27K 2013	A.6.2.1, A.6.2.2
DNB 2014/2017	18.1
BIO 2019	6.2.1 6.2.1.1 6.2.1.2 6.2.2
NIST Cybersecurity Framework	PR.DS-4 PR.IP-1 PR.IP-2 PR.IP-7 PR.IP-8 PR.PT-3 PR.PT-5 RS.CO-5 RS.AN-5