

Handreiking bij Volwassenheidsmodel Informatiebeveiliging




NBA

Mei 2016

Deze uitgave is vervaardigd op initiatief van:

Ledengroep Intern en Overheidsaccountants (LIO) van de Koninklijke Nederlandse Beroepsorganisatie van Accountants (NBA).

Het concept model is op 8 december 2015 gepresenteerd en bediscussieerd tijdens de NBA rondetafelbijeenkomst “Volwassen Informatiebeveiliging”.

Samenstelling werkgroep Maturity Model Informatiebeveiliging:

- Mevrouw drs. R.I. Doerga RA, voorzitter LIO (tot oktober 2015)
- Mevrouw drs. K.T. van Gessel RE, Senior Auditor bij Audit Dienst Rijk
- De heer M.M. Buijs RE, Audit Manager bij Audit Dienst Rijk
- De heer R. van Hoeijen RE, Senior Internal Auditor bij Group Audit DeltaLloyd
- De heer ir. R.J.P.C. Warmoeskerken RE, Europese Practice Leader Security, Risk & Compliance bij Liquidhub

Versie 1.0, Mei 2016

Inhoudsopgave

Voorwoord	4
Inleiding	5
Doel van het volwassenheidsmodel	6
Toepassing van het volwassenheidsmodel	7
Uitleg van het volwassenheidsmodel	8
- Algemeen	8
- Control en risicobeschrijving	8
- Volwassenheidsniveaus	11
- Referenties	12
- Rapportage en communicatie naar stakeholders	13
Tips & Tricks	16
Bijlage - Volwassenheidsmodel Informatiebeveiliging	17

Voorwoord

“Informatiebeveiliging vergt gerichte aandacht”

Al sinds de opkomst van de informatietechnologie is de beveiliging van de informatie een belangrijk onderwerp. Wij hebben onderzocht hoe functiescheidingen in ICT-systemen worden geïmplementeerd, om te kunnen beoordelen of mensen toegangsrechten hebben op een 'need to know'-basis. Om als accountants te kunnen toezien op de kwaliteit van deze toegangsrechten, hebben we ICT-hulpmiddelen ingezet. We hebben speciale controledoelstellingen, -metingen en -instrumenten ontwikkeld, om dit deel van het algemene ICT-management mogelijk te maken. Het klinkt u wellicht heel bekend in de oren: we opereren tegenwoordig in een volledig digitaal verbonden wereld. Mensen delen voortdurend informatie met elkaar, waar ze zich ook bevinden. Dit stelt ons voor enorme uitdagingen als het gaat om cybersecurity en we hebben allemaal te maken met zaken als hackpogingen, DoS-aanvallen en andere verstoringen. Informatietechnologie is inmiddels zodanig geïntegreerd in bedrijfsstrategieën, dat problemen met de beveiliging rechtstreeks van invloed zijn op de dagelijkse bedrijfsactiviteiten. Daarnaast worden bedrijven geconfronteerd met toenemende druk van wet- en regelgeving ten aanzien van informatiebeveiliging en de bescherming van persoonsgegevens.

Directies merken dat besprekingen van nieuwe business-strategieën automatisch uitlopen op het bespreken van de digitale strategie. Over het algemeen voelen directies zich onzeker over het potentieel van informatietechnologie en de impact van cybersecurity. Ze zoeken houvast en antwoorden. Informatiebeveiliging is een boardroom topic geworden en moet zonder angst, onzekerheid en twijfel kunnen worden behandeld. Recente onderzoeken tonen aan dat het onderwerp cybersecurity en informatiebeveiliging absoluut thuishoort op de agenda van directievergaderingen.

In samenwerking met risicomanagement kan de accountant een belangrijke rol spelen in het begeleiden van organisaties op dit gebied. Accountants moeten inzicht kunnen geven in nieuwe controlemechanismen op het gebied van veiligheid. Accountants moeten ook in staat zijn het beheer van de informatiebeveiliging te beoordelen, alsmede hoe volwassen deze is georganiseerd.

Als professor in ICT auditing aan de Universiteit Tilburg heb ik goed zicht op de ontwikkelingen binnen de accountants-opleiding. We hebben veel nieuwe componenten op het gebied van informatiebeveiliging toegevoegd om de competenties van (ICT) auditors up-to-date te houden. Het is een onderwerp dat steeds belangrijker wordt en ook steeds ingewikkelder. Onze werkwijze beperkt zich niet tot het vaststellen van preventieve controles, maar omvat ook het bespreken van hoe we slagvaardig kunnen omgaan met beveiligingsincidenten. De richtlijnen voor informatiebeveiliging in deze handreiking sluiten daarbij aan. Het is een geweldig hulpmiddel voor accountants, dat ze ondersteunt bij uitdagingen op het gebied van informatiebeveiliging. Het biedt inzicht in bestaande veiligheidskaders, gebaseerd op gedefinieerde volwassenheidsniveau's. Het motiveert u een actieve rol te spelen en uw inzichten als accountant zowel met veiligheidsexperts als met directieleden te bespreken. Daarnaast kunnen operationele managers, controllers en risk managers het gebruiken als handleiding bij de keuze van maatregelen voor implementatiedoelinden en het stellen van prioriteiten daarbij. Ik hoop dat u de basisprincipes in uw eigen organisatie kunt omarmen en sterke auditvaardigheden kan opbouwen op het gebied van informatiebeveiliging.

Het is een uitstekend initiatief van de NBA Ledengroep Intern en Overheidsaccountants, dat inmiddels waardevolle resultaten heeft opgeleverd. Mijn welgemeende complimenten voor deze publicatie.

Professor Rob Fijneman RE RA, Universiteit Tilburg en TIAS School for Business and Society

Inleiding

De afgelopen decennia is onomstreden gebleken dat de ontwikkelingen van informatie- en communicatietechnologie (ICT) grote sprongen maakt en niet meer weg te denken is uit onze samenleving. Ieder individu, elke organisatie en elke staat maakt op een of andere manier gebruik van ICT. De toepassingsgebieden van ICT worden als maar groter en meer divers.

De primaire processen van organisaties zijn al geruime tijd afhankelijk van ICT. Door ontwikkelingen als Cloud Computing, Internet of Things, Mobile, Social Media en Big Data blijft de afhankelijkheid van en de verbondenheid met ICT steeds groeien. Hierdoor onderkennen veel organisaties dat zaken als informatiebeveiliging en bedrijfscontinuïteit cruciaal zijn, maar is het op orde krijgen en het in stand houden hiervan steeds complexer en lastiger.

De (deels latente) dreigingen met betrekking tot informatiebeveiliging c.q. cyber security zijn de afgelopen jaren namelijk flink toegenomen. Zowel de kans van optreden alsmede de impact van (cyber) security incidenten zijn dusdanig dat een organisatie tegenwoordig een behoorlijk volwassenheidsniveau voor informatiebeveiliging moet hebben, wil de organisatie geen onacceptabele risico's lopen.

Een belangrijke vraag in dit kader is: In hoeverre volstaat het huidige volwassenheidsniveau van informatiebeveiliging voor uw organisatie? Om deze vraag te kunnen beantwoorden, zal onder andere antwoord moeten worden gegeven op de onderliggende (sub)vragen:

- Op welk volwassenheidsniveau zou uw organisatie gelet op de risico's zich moeten bevinden?
- Op welk volwassenheidsniveau bevindt uw organisatie zich momenteel?
- En wat moet er nog gebeuren om dat volwassenheidsniveau te bereiken?

Het beantwoorden van deze vragen is niet evident. Het blijkt dat veel organisaties het lastig vinden om deze vragen op een adequate, consistente en snelle wijze te beantwoorden. In het bijzonder voor organisaties die periodiek door haar toezichthouder worden geconfronteerd met vragen over de stand van zaken aangaande de inrichting en effectiviteit van hun informatiebeveiliging. Om op deze vragen adequaat antwoord te kunnen geven blijkt dit vaak voor organisaties een lastige, intensieve en tijdrovende exercitie te zijn. Het ontbreekt aan een overzicht om op een consistente en efficiënte wijze de informatiebeveiligingsmaatregelen in te schalen op een bijbehorend volwassenheidsniveau.

Dit signaal is opgepikt door de Ledengroep Interne en Overheidsaccountantsdiensten (LIO) van de Nederlandse Beroepsorganisatie voor Accountants (NBA) en heeft daarom in het jaarplan 2015 van LIO een activiteit opgenomen om tot een handreiking aangaande een volwassenheidsmodel van informatiebeveiliging te komen. Dit heeft geresulteerd in de voorliggende handreiking en het bijbehorend volwassenheidsmodel voor informatiebeveiliging, waarmee een groot deel van de bovenstaande vragen door de organisatie beantwoord kunnen worden.

Het volwassenheidsmodel is overigens niet opgesteld met de intentie om een nieuw normenkader te introduceren en derhalve is gebruik gemaakt van en verwezen naar bestaande "good practices". In het geval er zaken zijn die verbetering of aanpassing behoeven in het model of bijbehorende aanpak verzoeken wij u om contact op te nemen met de NBA. Op deze manier wordt de kwaliteit en actualiteit van ons model vanuit het werkveld gewaarborgd. De NBA zal het model ook periodiek evalueren en waar nodig bijstellen.

Doel van het volwassenheidsmodel

Het volwassenheidsmodel heeft tot doel de interne audit afdelingen alsmede de directies van organisaties een leidraad en handvaten te geven waarmee zij doelgericht en op pragmatische wijze hun organisaties kunnen ondersteunen bij het meten, bepalen en verbeteren van het volwassenheidsniveau van informatiebeveiliging.

Het model geeft op conceptueel niveau inzicht in welke informatiebeveiligingsmaatregelen genomen moeten worden en welke maatregelen op welke volwassenheidsniveau redelijkerwijs verwacht mogen worden. Daarmee geeft het model de interne audit afdeling, de RvB en/of directie goed inzicht in welke stappen hun organisatie nog moet nemen om tot het gewenste¹ volwassenheidsniveau te komen.

In eerste instantie kan het model door het verantwoordelijk management en/of de interne audit afdeling gebruikt worden voor het toetsen van het volwassenheidsniveau van informatiebeveiliging op basis van de geïmplementeerde beheersmaatregelen.

Om tot het gewenste volwassenheidsniveau te komen, moeten er vanuit de organisatie specifieke situatie (kansen en risico's) onderbouwde keuzes worden gemaakt om bepaalde maatregelen wel of niet te treffen ("comply or explain"). Het model geeft aan welke beheersmaatregelen (per volwassenheidsniveau) aanwezig zouden moeten zijn die het vervolgens mogelijk maken om tot een dergelijke juiste afweging te komen. Afwegingen met betrekking tot kosten en baten zijn dermate situationeel dat deze niet zijn opgenomen in deze handreiking (en model).

Het model kan ook als basis dienen voor aanbevelingen, verbeterplannen of projectbrieven met betrekking tot een gerichte implementatie van beheersmaatregelen om het vereiste volwassenheidsniveau van informatiebeveiliging te bewerkstelligen.

Het model is in elektronische vorm beschikbaar en te downloaden via de website van NBA (www.nba.nl). Het model bestaat uit een spreadsheet (Excel) met verschillende tabbladen. De tabbladen hebben tot doel het model inhoudelijk te presenteren, ondersteuning te bieden bij het scoren van de volwassenheidsniveaus en uiteindelijk de resultaten door middel van grafieken te presenteren aan stakeholders. In het hiernavolgende hoofdstuk zal het volwassenheidsmodel nader worden uitgelegd.

Waar voorheen "impliciete" richtlijnen binnen een organisatie werden afgesproken om tot een uniforme uitvoering en vaststelling te komen, kan nu organisatiebreed, organisatieoverstijgend en/of sectorbreed het aangereikte volwassenheidsmodel worden gebruikt. Dit laatste maakt vergelijkingen tussen "industry peers" eenvoudiger.

¹ In sommige situaties kan er ook sprake zijn van vereist volwassenheidsniveau, bijv. opgelegd door de toezichthouder.

Toepassing van het volwassenheidsmodel

Zoals eerder beschreven geeft het model op conceptueel niveau inzicht in welke informatiebeveiligingsmaatregelen per volwassenheidsniveau redelijkerwijs verwacht mogen worden. Het geeft hiermee een handreiking om het volwassenheidsniveau te meten, bepalen en verbeteren, maar natuurlijk blijven de genoemde maatregelen altijd een enigszins subjectief karakter hebben. Het volwassenheidsmodel is richtinggevend en daarmee een goed instrument om de dialoog met het verantwoordelijk management te houden.

Ten behoeve van een succesvolle toepassing van het volwassenheidsmodel dient een aantal (rand)voorwaarden in ogenschouw te worden genomen:

- Het vaststellen van het gewenste volwassenheidsniveau wordt in belangrijke mate bepaald door de aard van de business c.q. processen, soort gegevens van de organisatie en de beschikbare applicaties en infrastructuur. Deze zaken alsmede de specifieke risico's en risicobereidheid van de organisatie zijn bepalend hoe hoog de lat voor de organisatie moeten liggen.
- Doordat vele organisaties delen van hun informatievoorziening en/of -verwerking hebben uitbesteed, dient er expliciet aandacht worden besteed aan de afhankelijkheden van en samenwerking met partners in de keten. Dit vergt ook een goede afstemming van de verschillende volwassenheidsniveau's binnen de keten.
- Bedenk dat per organisatie de van toepassing zijnde wet & regelgevingen verschillend zijn. Het model wijst op de compliance met verplichte wet & regelgevingen (b.v. WBP), echter deze zijn niet specifiek uitgewerkt en kunnen op onderdelen bepalend zijn voor de hoogte van de meetlat.
- Het model voorziet ook in de grafische presentaties van de uitkomsten. Dit verbetert de leesbaarheid van uitkomsten voor stakeholders, zoals RvB en toezichthouders. Echter de toegevoegde waarde zit hem vooral in de periodieke dialoog met deze stakeholders over uitkomsten, het bespreken van impact en risico's en de opvolging van mitigerende activiteiten.

Tenslotte verwijzen we nog naar laatste hoofdstuk waar nog enkele "Tips en Trics" ten behoeve van een succesvolle toepassing van het model zijn beschreven.

Uitleg van het volwassenheidsmodel

Algemeen

Het volwassenheidsmodel is opgesteld in een spreadsheet waarbij diverse kolommen zijn onderscheiden. Deze kolommen worden nader toegelicht in de hiernavolgende paragrafen.

Zoals eerder aangegeven is het volwassenheidsmodel niet opgesteld met de intentie om een nieuw normenkader te introduceren. Gebruikmakend van bestaande normen c.q. referentiekaders, zijnde CobIT, ISO27002, DNB, BIR en BIG, is een consistente verzameling van beheersdoelstellingen samengesteld waar per beheersdoelstelling vijf volwassenheidsniveaus zijn beschreven. De individuele beheersdoelstellingen wegen allen even zwaar.

Per beheersdoelstelling kan op basis van de beschrijving van het volwassenheidsniveau alsmede de verwijzing naar één of meerdere “good practices” een inschatting van het betreffende volwassenheidsniveau worden gemaakt. Hierbij dient in alle gevallen de organisatiespecifieke context bepalend te zijn voor verdere explicitering van de gewenste beheersmaatregelen en de waardering van de geïmplementeerde beheersmaatregelen.

Control en risicobeschrijving

De eerste kolommen van het volwassenheidsmodel beschrijven het aandachtsgebied, de unieke identificatie, de naam van beheersmaatregel, de beschrijving van het risico, het gewenste volwassenheidsniveau (ingeschat op basis van het inherente risico) en de beschrijving van de beheersmaatregel. De getallen in de oranje vierkanten verwijzen naar de paragrafen hieronder.

Afbeelding 1: Een voorbeeld van de control- en risicobeschrijving (Incident/problem management)

Area	ID	Control name	Risk description	Required maturity level based on inherent risk estimation	Control description
Incident / Problem Management	IM.01	Incident management	Incidents are not properly classified and are treated incorrectly in the incident and problem management process, ultimately decreasing the performance (e.g. integrity and availability) of IT.		A formal incident management process is communicated and implemented. Procedures are in place to ensure that all incidents and failures are recorded, analyzed, categorized and prioritized according to impact. All incidents are tracked and periodically reviewed to ensure they are resolved in a timely manner.
1	2	3	4	5	6

1 Area

De eerste kolom beschrijft het generieke aandachtsgebied. Binnen het model zijn 15 aandachtsgebieden onderscheiden, waarbij tevens de generieke doelstelling van het betreffende aandachtsgebied is beschreven²:

- **Bestuur (Governance, GO)**
Geeft richting en ondersteuning aan informatiebeveiliging in lijn met bedrijfsdoelstellingen, risicobereidheid en van toepassing zijnde wet- en regelgeving en vergewist zich van de effectieve naleving ervan.
- **Organisatie (Organisation, OR)**
Informatiebeveiliging is op het hoogst mogelijk organisatieniveau geadresseerd en het beheer van informatiebeveiliging in lijn is met de bedrijfsdoelstellingen en van toepassing zijnde risico's en compliance eisen.
- **Risicobeheer (Risk Management, RM)**
Draagt zorg voor het op gestructureerde wijze identificeren en beheersen van informatiebeveiligingsrisico's zodanig dat de risico's in lijn zijn met de risicobereidheid en risicoraamwerk van de organisatie.
- **Personeelsbeheer (Human Resources, HR)**
Draagt zorg voor dat alle medewerkers, inhuurkrachten en derde partijen zich bewust zijn van informatiebeveiligingsrisico's en voldoende geschoold zijn om in lijn met het beveiligingsbeleid hun werkzaamheden te kunnen verrichten.
- **Configuratiebeheer (Configuration Management, CO)**
Draagt zorg voor de vastlegging en ontsluiting van gegevens over de IT-middelen en IT-diensten.
- **Incident/probleembeheer (Incident/Problem Management, IM)**
Draagt zorg voor het afhandelen van verstoringen in IT-dienstverlening en voor tijdig herstel van afgesproken dienstenniveau's. Probleembeheer draagt zorg voor het wegnemen of voorkomen van structurele fouten in de IT-dienstverlening.
- **Wijzigingsbeheer (Change Management, CH)**
Draagt zorg voor het beheerst doorvoeren van wijzigingen in IT-middelen en IT-diensten (o.a. applicaties).
- **Systeemontwikkeling (System Development, SD)**
Draagt zorg voor het ontwikkelen van geautomatiseerde oplossingen in lijn met ontwerpspecificaties, ontwikkel- en documentatiestandaarden en kwaliteits- en acceptatiecriteria.
- **Gegevensbeheer (Data Management, DM)**
Draagt zorg voor het onderhouden van de volledigheid, juistheid, beschikbaarheid en bescherming van gegevens.
- **Identiteits- en toegangsbeheer (Identity & Access Management, ID)**
Draagt draagt zorg voor het beheren van de logische toegang tot informatie en informatiediensten (o.a. applicaties).
- **Beveiligingsbeheer (Security Management, SM)**
Draagt zorg voor het in kaart brengen en adresseren van de risico's van beschikbaarheid, integriteit en vertrouwelijkheid die van toepassing zijn op de informatievoorziening.
- **Fysieke beveiliging (Physical Security, PH)**
Draagt draagt zorg voor het toegangsbeheer tot ruimtes en de bescherming van personen en objecten tegen incidenten die een fysieke schade aan personen of objecten tot gevolg kunnen hebben.
- **Computer operatie (Computer Operations, OP)**
Draagt zorg voor het operationeel houden van de IT-diensten.
- **Bedrijfscontinuïteitbeheer (Business Continuity Management, BC)**
Draagt zorg voor het herstellen en voorzetten van de bedrijfsvoering na het optreden van een calamiteit in overeenstemming met de hiervoor afgesproken dienstenniveau's.

² Diverse definities komen uit het studierapport "Algemene beheersing van IT-diensten" (NOREA en PvlB, 2015)

- Ketenbeheer (Supply Chain Management, SC)
Draagt zorg voor het bewaken van de levering van de afgesproken dienstverlening door (interne en externe) leveranciers.

Per aandachtsgebied zijn twee of meer beheersdoelstellingen gedefinieerd die hun bijdrage leveren aan het bewerkstelligen van de generieke doelstelling van het aandachtsgebied.

2 ID

Elke beheersdoelstelling heeft een unieke identificatie (ID), welke bestaat uit een twee-letterig prefix gevolgd door een volgnummer. De twee-letterige prefixen zijn in de voorgaande paragraaf per aandachtsgebied weergegeven.

3 Control name

De korte c.q. summiere beschrijving van de beheersdoelstelling. De beschrijving geeft in enkele steekwoorden de kern en essentie van de beheersdoelstelling aan.

4 Risk description

De beschrijving van het (inherente) risico in het geval de betreffende beheersmaatregel niet of in onvoldoende mate effectief is. De risicobeschrijving is generiek van aard en indicatief.

5 Required maturity level based on inherent risk estimation

Op basis van het ingeschatte risico is een bepaald volwassenheidsniveau vereist dat het inherente risico waaraan de organisatie wordt blootgesteld binnen de risicobereidheid (risk appetite) van de organisatie terugbrengt c.q. het risico afdoende mitigeert.

De volgende volwassenheidsniveaus zijn van toepassing:

Score	Risico-inschatting	Vereist volwassenheidsniveau
N/A	Niet van toepassing	Niet van toepassing
1	Nihil	Laag
2	Beperkt Ruim binnen risicobereidheid	Beperkt
3	Gemiddeld Net binnen of net buiten risicobereidheid	Gemiddeld
4	Aanzienlijk Buiten risicobereidheid	Meer dan gemiddeld
5	Hoog Ruim buiten risicobereidheid	Hoog

Volwassenheidsniveaus

Om een handreiking te geven bij de consistente toetsing van het actuele volwassenheidsniveau zijn vijf volwassenheidsniveaus gedefinieerd en nader uitgewerkt. Op basis van vijf beschrijvingen (van redelijkerwijs te verwachten beheersmaatregelen) kan worden bepaald welk volwassenheidsniveau voor de betreffende beheersdoelstelling van toepassing is. Daarnaast helpt de indicatieve beschrijving van de (redelijkerwijs) te realiseren beheersmaatregelen ook om richting te geven aan het implementatie- c.q. verbetertraject, welke bijvoorbeeld in de vorm van een aanbeveling in een rapport kan worden opgenomen.

Afbeelding 2: Een voorbeeld van een nadere beschrijving van vijf volwassenheidsniveaus (change management)

Initial Controls are only partly defined and/or executed in an inconsistent manner and rely heavily on individuals.	Repeatable Controls are in place and executed in a structured and consistent, but informal manner.	Defined Controls are documented and executed in a structured, formal and proven manner.	Managed and measurable Effectiveness of controls is periodically assessed and checked for quality.	Continuous improvement An ecosystem has been established to provide continuous and effective control, and to resolve risks.	Actual maturity level indication
- An incident management policy has not been defined. - Roles and responsibilities are not defined. - There are no procedures to ensure that all incidents and failures are recorded and analyzed. - Incidents are tracked and reviewed on an individual basis. - Responses to information security incidents are ad hoc.	- An informal incident management process has been defined to address critical aspects. - Roles and responsibilities have been partially defined. - The majority of incidents is recorded and analyzed, but deviations from established norms or standards are likely to be undetected. - Criteria have not been defined for categorizing and prioritizing incidents according to impact. - Incidents are dispatched on ad-hoc basis. - Incidents are tracked on an individual basis and monitored individually. - No formal training standard procedures.	- The formalized incident management policy is documented and communicated. - Roles and responsibilities of the organization and suppliers are clearly defined. - Legal and criminal investigative issues are defined and addressed. - There is a formal and accessible function which registers, communicates, dispatches and analyzes reported incidents and problems. - Incidents are categorized and prioritized according to impact. - Security incidents are reported or detected and there is a process to ensure in a timely and effective manner. - Information is shared among staff in a proactive and formal manner. - Monitoring implemented to see if incidents are resolved in a timely manner.	- Incidents are proactively analyzed to identify causes. - A function (response team) is implemented which recognizes and manages security emergencies. - The security incident management process interfaces with key organization functions and external service providers (if applicable). - The timely resolution of incidents is strictly monitored. Unresolved incidents (known errors and workarounds) are recorded and reported as input for problem management. - The quality and openness of the incident management process is periodically reviewed.	- The registration, reporting and analysis of incidents and resolutions are automated and fully integrated with configuration and problem management. - Most systems have been equipped with automatic detection and warning mechanisms, which are continuously tracked and evaluated. - Incident and problem management are analyzed for continuous improvement.	7 8 9 10 11 12

7 - 11 Maturity Indication Level

Per beheersdoelstelling zijn de vijf indicaties van volwassenheidsniveaus op basis van een aantal criteria nader uitgewerkt. De volgende vijf niveaus als mede de volgende bijbehorende leidende criteria zijn hierbij onderkend:

Niveau	Naam	Omschrijving	Criteria
1	Initieel	Beheersmaatregelen zijn niet of gedeeltelijk gedefinieerd en/of worden op inconsistente wijze uitgevoerd. Grote afhankelijkheid van individuen.	• Geen of beperkte controls geïmplementeerd • Niet of ad-hoc uitgevoerd • Niet/deels gedocumenteerd • Wijze van uitvoering afhankelijk van individu
2	Herhaalbaar	Beheersmaatregelen zijn aanwezig en worden op consistente en gestructureerde, maar op informele wijze uitgevoerd.	• Control is geïmplementeerd • Uitvoering is consistent en standaard • Informeel en grotendeels gedocumenteerd
3	Gedefinieerd	Beheersmaatregelen zijn gedocumenteerd en worden op gestructureerde en geformaliseerde wijze uitgevoerd. De uitvoering is aantoonbaar.	• Control gedefinieerd o.b.v. risico assessment • Gedocumenteerd en geformaliseerd • Verantwoordelijkheden en taken eenduidig toegewezen • Opzet, bestaan en effectieve werking aantoonbaar
4	Beheerst en meetbaar	De effectiviteit van de beheersmaatregelen wordt periodiek geëvalueerd en kwalitatief gecontroleerd.	• Periodieke (control) evaluatie en opvolging vindt plaats • Rapportage management vindt plaats

Niveau	Naam	Omschrijving	Criteria
5	Continu verbeteren	Een ECO systeem is verankerd en draagt zorg voor een continue en effectieve controle en risico beheersing	- Self-assessment, gap en root cause analyses - Real time monitoring - Inzet automated tooling

Er wordt opgemerkt dat in tegenstelling tot andere volwassenheidsmodellen niveau 0 ("non existent") niet is uitgewerkt. Niveau 0 maakt onderdeel uit van niveau 1 ("initial").

12 Actual maturity level indication

Op basis van de gedefinieerde volwassenheidsniveaus kan een inschatting c.q. indicatie van het actuele volwassenheidsniveau worden gegeven.

Score	Actueel volwassenheidsniveau	Omschrijving
N/A	Niet van toepassing	Niet van toepassing
1	Laag	Initieel
2	Beperkt	Herhaalbaar
3	Gemiddeld	Gedefinieerd
4	Meer dan gemiddeld	Beheerst en meetbaar
5	Hoog	Continu verbeteren

Referenties

Ieder organisatie heeft veelal een keuze gemaakt welk model en/of "good practice" zij gebruikt voor informatiebeveiliging en/of risicomanagement. Het volwassenheidsmodel is zodanig opgesteld dat op basis van "good practices" de relevante controledoelstellingen en de bijbehorende volwassenheidsniveaus voor informatiebeveiliging zijn gedefinieerd. Deze zijn zoveel mogelijk conceptueel beschreven en waar mogelijk losgekoppeld van specifiek in te richten en uit te voeren beheersmaatregelen. De meer specifieke en meer gedetailleerde implementatie richtlijnen zijn derhalve terug te vinden in de betreffende "good practice" (standaard, raamwerk of baseline).

Hiertoe zijn de verwijzingen naar de volgende "good practices" opgenomen (de oranje nummers verwijzen naar de kolommen):

- 13** CobIT 4.1 - IT Governance Institute framework for control objectives for IT, 2007
- 14** COBIT 5.0 - ISACA framework for control objectives for IT, 2012
- 15** ISO/IEC 27001:2013 - Code of practice for information security controls (oktober 2013)³
- 16** DNB Standard Framework Information Security (ref. 50-230771, mei 2014)
- 17** BIR - Baseline Informatiebeveiliging Rijksdienst (tactisch, december 2012)⁴
- 17** BIG - Baseline Informatiebeveiliging Nederlandse Gemeenten (tactisch, juli 2015)⁴

³ De prefix "A." verwijst naar de bijlage van ISO/IEC 27001:2013, zijnde de control objectives en controls (uit ISO/IEC 27002:2013).

⁴ De overheid is verplicht om aan ISO27001 en ISO27002 te voldoen. De BIR beschrijft de invulling hiervan voor de rijksoverheid. De rijksspecifieke aanvullingen/invullingen zijn in de BIR met een [R] aangeduid. De BIG beschrijft de invulling hiervan voor de gemeenten. De gemeentespecifieke aanvullingen/invullingen zijn in de BIG met een [A] aangeduid.

In de onderstaande afbeelding is een voorbeeld van verwijzingen naar de “good practices” opgenomen.

Afbeelding 3: Een voorbeeld van de verwijzing naar “good practices” (change management)

References				
COBIT 4.1	COBIT 5	ISO 27K 2013	DNB 2014	BIR 2012 / BIG 2015
DS5.6, DS8.1, DS8.2, DS8.4, DS8.5	DSS02.01, DSS02.02, DSS02.03, DSS02.05, DSS02.06, DSS02.07	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	15.1, 15.2	8.2.3, 12.6.1, 13.1.1, 13.1.1.1, 13.1.1.2 [R], 13.1.1.3 [A], 13.1.1.4 [R], 13.1.2, 13.2.1, 13.2.3, 13.2.2
13	14	15	16	17

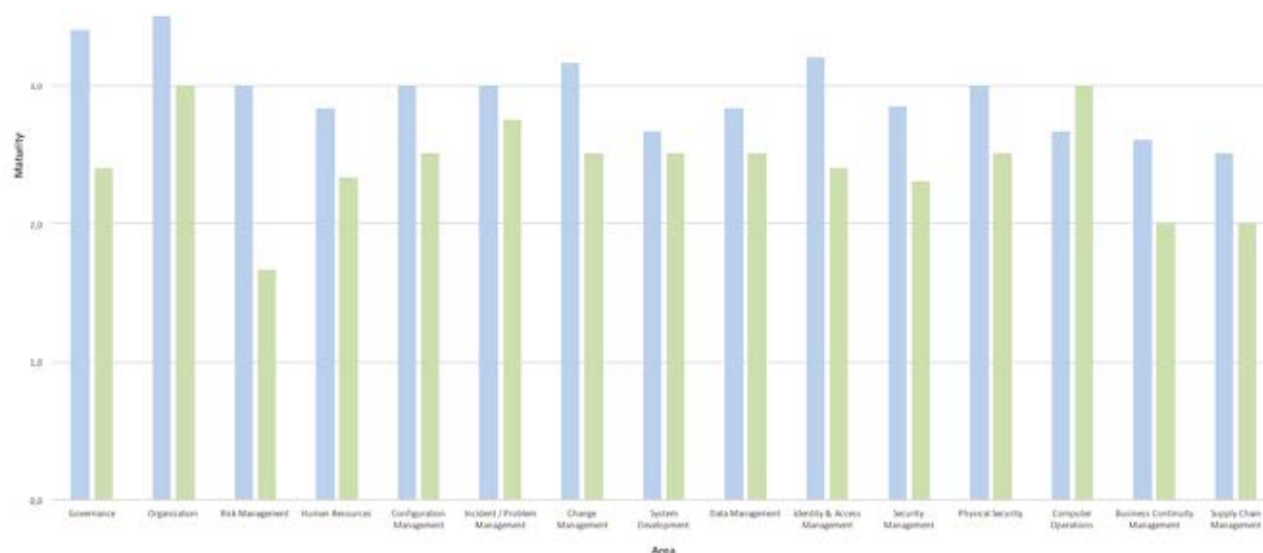
Rapportage en communicatie naar stakeholders

Op het moment dat de indicaties of scores van de volwassenheidsniveaus zijn getoetst en ingevuld, kunnen in de spreadsheet door middel van twee tabbladen de resultaten op grafische wijze worden gepresenteerd en gecommuniceerd aan de stakeholders. Het tabblad “Summary” in de Excel spreadsheet geeft een tweetal grafieken weer.

Summary of Required vs Actual Maturity Level Indications per Area

Deze grafiek geeft per aandachtsgebied het vereiste volwassenheidsniveau (ingeschat op basis van het inherente risico) afgezet tegen het actuele volwassenheidsniveau weer. Hierbij is het gemiddelde berekend van de volwassenheidsniveaus van de onderliggende beheersdoelstellingen behorende tot het betreffende aandachtsgebied (Area). In de hierna volgende grafiek is een voorbeeld weergegeven.

Afbeelding 4: Voorbeeld van grafiek met samenvatting van gemiddelde volwassenheidsniveaus per aandachtsgebied

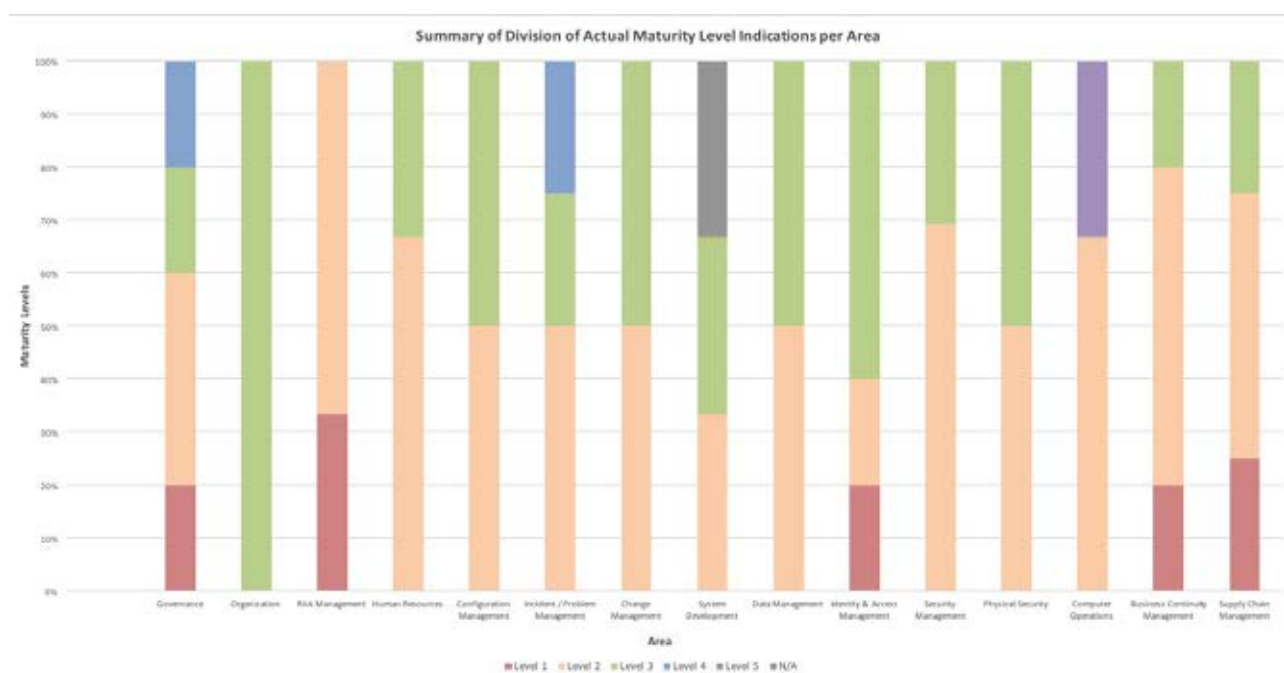


Summary of Division of Actual Maturity Level Indications per Area

Deze grafiek geeft per aandachtsgebied de procentuele verdeling van de volwassenheidsniveaus weer. Op basis van deze grafiek is eenvoudig te bepalen welk percentage van de beheersdoelstellingen zich bijvoorbeeld onder het volwassenheidsniveau 3 bevinden.

In de hiernavolgende grafiek (afbeelding 5) is een voorbeeld weergegeven waar uit de staafdiagram blijkt dat bijvoorbeeld alleen het aandachtsgebied “Organisatie” een volwassenheidsniveau 3 of hoger scoort omdat er geen rode (niveau 1) of lichtoranje (niveau 2) kleuren in de betreffende staaf voorkomen.

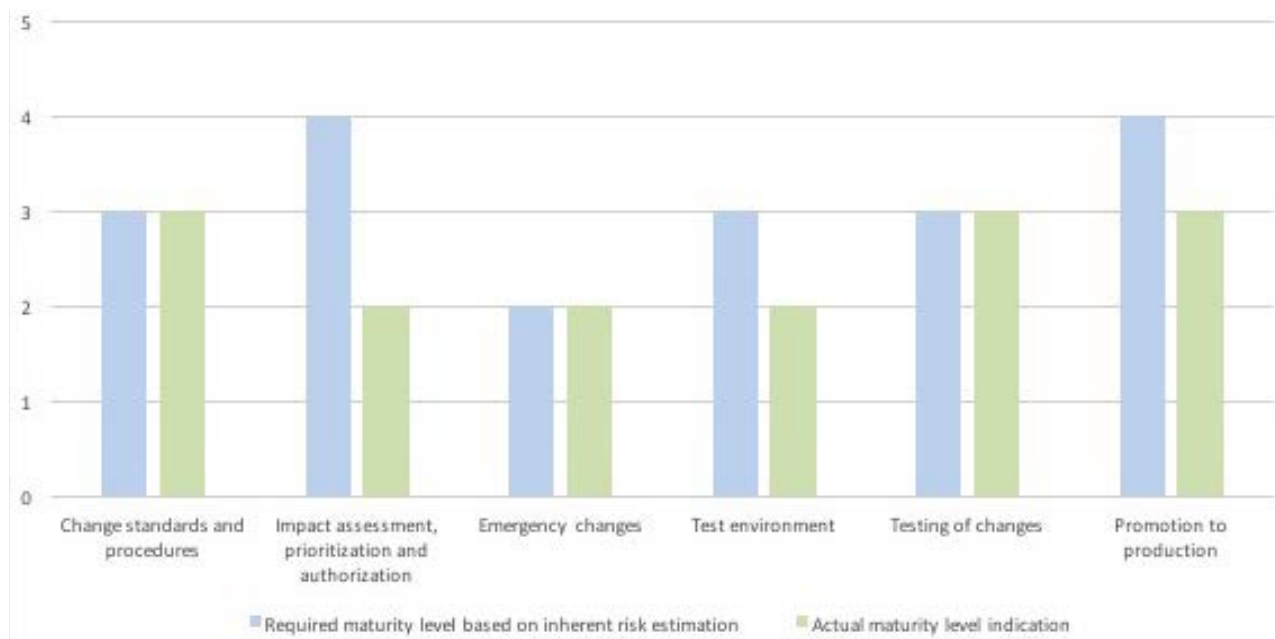
Afbeelding 5: Voorbeeld van grafiek met verdeling van volwassenheidsniveaus per aandachtsgebied



Door middel van het tabblad “Overview” kan een gedetailleerd inzicht worden verkregen van de volwassenheidsniveaus van individuele beheersdoelstellingen behorende tot de onderkende aandachtsgebieden. Per grafiek c.q. per aandachtsgebied (aantal = 15) wordt voor elke beheersdoelstelling de vereiste en actuele volwassenheidsniveaus tegen elkaar afgezet.

In de onderstaande grafiek (afbeelding 6) is ingezoomd op de volwassenheidsniveaus binnen het aandachtsgebied “Change Management”. Op basis hiervan is vast te stellen dat voor de actuele volwassenheidsniveaus (groen) 50% op niveau 2 en de andere 50% op niveau 3 (en bijvoorbeeld voldoet aan minimumniveau voor DNB) is gescoord. Hetgeen ook eenvoudig is af te leiden uit afbeelding 5. Het gemiddelde actuele volwassenheidsniveau komt hiermee op 2½, wat ook is af te leiden uit afbeelding 4.

Afbeelding 6: Voorbeeld van een “ingezoomde” grafiek (Change Management)



Tips & Tricks

- Het voorliggende model betreft een handreiking, die richtinggevend is voor een bepaalde aanpak en eventuele prioritering. De interne en externe context van een organisatie alsmede de bijbehorende bedreigingen, kwetsbaarheden en risico's zijn te allen tijde lijdend voor het implementeren en uitvoeren van de beheersmaatregelen. Denk bijvoorbeeld aan het feit dat elke organisatie een onderdeel uitmaakt van een (waarde)keten en dat bij risicomitigatie en -acceptatie ook altijd een kosten-baten afweging plaatsvindt. Beiden zaken zijn voor elke organisatie specifiek c.q. anders.
- Het verdient aanbeveling om de risico indicatie (5) organisatiespecifiek te maken door hier herkenbare kengetallen en/of criteria aan te koppelen. Denk aan financiële impact (kosten / verliezen in Euro's), operationele impact (kosten herstelwerk, aantal uren productieverstoring, organisatorisch omvang van verstoring) en reputationele impact (in regionaal of landelijke pers, intrekking van licentie).
- Betrek interne audit afdeling in de vorm van facilitator of laat ze een plausibiliteitstoets op de scores en bijbehorende documentatie (evidence) uitvoeren. Een plausibiliteitstoets heeft zeker meerwaarde als de scores en bijbehorende documentatie richting externe stakeholders of een toezichthouder moeten worden gepresenteerd en/of verdedigd.
- Informatiebeveiliging is integraal onderdeel van de bedrijfsvoering en het verantwoordelijke management is eigenaar van de betreffende risico's. Organiseer daarom een "challenge" sessie, waarbij de verantwoordelijke directie wordt uitgedaagd over de geïmplementeerde en uitgevoerde maatregelen en bijbehorende restrisico's in relatie tot het toegekende volwassenheidsniveau. Op basis van het opgeleverde documentatie c.q. onderbouwing dient de verantwoordelijke directie zich te vergewissen dat deze passend is voor het toegekende volwassenheidsniveau.
- In geval dat de volwassenheidsscore worden gebruikt voor externe verantwoording verdient het aanbeveling om de verantwoordelijke directie af te laten tekenen voor de volwassenheidsniveaus (en bijbehorende documentatie) behorende bij de aandachtsgebieden waar hij/zij verantwoordelijk voor is.
- In de gevallen waar het volwassenheidsniveau achterblijft bij het gewenste niveau verdient het aanbeveling de aandachtsgebieden (area's) te prioriteren. Bedenk dat er afhankelijkheden en/of randvoorwaardelijke aandachtsgebieden zijn. Voorbeelden hiervan zijn: uitkomsten uit risicomanagement proces of dataclassificatie proces zijn bepalend en richtinggevend voor diverse andere beveiligingsmaatregelen.
- Het verdient aanbeveling te identificeren waar het nemen van onmiddellijke actie het meeste rendement oplevert om managementbetrokkenheid en ondersteuning voor het gebruik van deze handreiking (en het model) te krijgen voor hun eigen gemak en/of management control.
- Evalueer jaarlijks het model en het gebruik en de toepassing ervan. Informeer NBA in het geval er zaken zijn die verbetering of aanpassing behoeven in het model of bijbehorende aanpak.

Bijlage |

Volwassenheidsmodel

Informatiebeveiliging

Omwille van de leesbaarheid zijn twee kolommen (5 en 12), waarbij het gewenste en het actuele volwassenheidsniveau kan worden in gevuld, weggelaten.

Area	ID	Control name	Risk description	Control description	Maturity Indication Level 1	Maturity Indication Level 2
					Initial Controls are only partly defined and/or executed in an inconsistent manner and rely heavily on individuals.	Repeatable Controls are in place and executed in a structured and consistent, but informal, manner.
Governance	GO.01	Strategy	An absence of strategy can lead to poor business and security decisions or inappropriate response to changes in the business environment.	An information security strategy and vision is leading for all activities and measures concerning information security.	- Security activities or measures are implemented and/or executed on an ad-hoc basis.	- A strategy and vision has been defined, but has not been formally accepted.
	GO.02	Policy	Inability to comply with legislative, regulatory and/or internal IT (security) requirements due to an ineffective policy framework which supports the IT strategy and information security.	The organization has adopted a security policy which is communicated to employees (and contractors) via a written policy document or intranet. If applicable, the policy is also actively communicated to suppliers/vendors. The policy is regularly updated, reviewed and approved by senior management.	- No policy defined. - Some policy statements drafted.G3	- A security policy has been defined and covers most relevant aspects of information security. F5
	GO.03	Plan / Roadmap	Guidance and support for information security in accordance with business objectives, risks and compliance requirements is not provided by the organization.	Business objectives, risks and compliance requirements are translated into an overall information security plan, taking into consideration IT infrastructure and the security culture.	- No information security plan or roadmap defined. - A few individual IT security projects have been defined and/or in progress.	- An IT security plan or roadmap has been defined and covers all relevant business objectives, risks and compliance requirements.
	GO.04	Architecture	Incomplete overview of current and target architecture can lead to increase in costs, complexity and inability to timely respond to challenges driven by business changes.	An enterprise information architecture model (EIAM) has been established and maintained to enable application development and decision-supporting activities, consistent with IT plans. The model should make it possible to effectively create, use and share information, in a secure and resilient manner, as required by business objectives.	- No EIAM defined.	- Baseline (as-is) architecture has been defined. - EIAM-specific processes have been established to enable system and/or application development.
	GO.05	Independent assurance	Compliance and performance are not reviewed and confirmed by an independent party, leading to possible unknown and unaddressed deviations in compliance and/or performance.	Independent assurance (internal or external) is obtained about conformity of IT with relevant laws and regulations; the organization's policies, standards and procedures; generally accepted practices; and the effective and efficient performance of IT.	- Independent assurance is not obtained.	- The internal audit function has been defined and includes the task of reviewing compliance with relevant IT laws and regulations, the organization's IT policies, IT standards and IT procedures.
Organization	OR.01	Ownership, roles, accountability and responsibilities	Unclear or ambiguous ownership, roles, accountability or responsibilities can jeopardize effective decision-making, management and reporting on information security concerning business requirements/risks.	Information security is managed at all appropriate organizational levels and security actions are managed in line with business requirements / risks. Ownership, roles, accountability and responsibilities have been formally assigned and embedded into the organization.	- No ownership, roles and responsibilities formally assigned. - A few roles identified and informally performed.	- Roles critical for managing information risks have been defined and assigned, including specific accountability and responsibility for information security, physical security and compliance.
	OR.02	Segregation of duties	Unilateral actions (e.g. unauthorized access to data) could occur in key IT processes, which could result in a negative impact on business processes, e.g. risk of negligent or deliberate system misuse.	Roles and responsibilities are segregated to reduce the likelihood of single individuals compromising critical processes. Personnel are only performing authorized duties relevant to their respective jobs and positions.	- Roles and responsibilities are not segregated or are segregated on an ad-hoc basis.	- Roles and responsibilities are segregated. - How roles and responsibilities are segregated has not been formalized and/or agreed upon by (senior) management.

Maturity Indication Level 3	Maturity Indication Level 4	Maturity Indication Level 5	References				
			COBIT 4.1	COBIT 5	ISO 27K 2013	DNB 2014	BIR 2012 / BIG 2015
Defined Controls are documented and executed in a structured, formal and proven manner. - Strategy and vision has been approved by senior management. - Strategy and mission is actively communicated to employees, contractors and business partners.	Managed and measurable Effectiveness of controls is periodically assessed and checked for quality. - Strategy and vision are acknowledged as leading for all activities and measures regarding information security. - Alignment with strategy and vision is documented where applicable.	Continuous improvement An eco system has been established to provide continuous and effective control, and to resolve risks. - Strategy also addresses how IT will help business objectives to be realized. - The validity and feasibility of the strategy and vision is periodically verified. - If necessary, the strategy or vision is adjusted to keep pace with business objectives and external developments.	PO1.4, ME4.2	APO02.03, APO02.04, APO02.05	5.1, A.5.1.1	1.2	5.1.1
- Policy has been approved by senior management. - Security policy is actively communicated to employees, contractors and business partners (suppliers) and is made available as hard copy or digital document via intranet. - Policy is part of the security awareness program.	- The security policy has been embedded into / adopted by the organization and translated into underlying procedures, baselines and instructions. - Compliance with policy is assessed on ad-hoc basis.	- Compliance with security policy is periodically reported to senior management. - Policy is reviewed, updated and reaproved by senior management on an annual basis.	PO6.3, PO6.4, PO6.5	APO01.03, APO01.04, APO01.08	5.2, A.5.1.1, A.5.1.2, A.6.1.1, A.7.2.2, A.18.2.2	1.2	5.1.1, 5.1.2, 5.1.2.1 [R.A], 6.1.1.1 [R.A], 6.1.3, 6.1.8, 6.2.2
- The information security plan or roadmap has been approved by senior management. - The plan has been translated into required security policies and procedures together with appropriate investments in services, personnel, software and hardware. - Security policies and procedures are communicated to stakeholders and users.	- The information security plan is implemented via enforced security policies, procedures, required services, personnel, software and hardware. - There is a process for periodically updating the information security plan and for forcing appropriate levels of management review and approval of changes.	- The information security plan and related project portfolio are periodically monitored for e.g. progress, feasibility and extent to which business requirements are met, including benefit tracking. - Reports submitted to senior management.	DS5.2	APO13.02	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	1.1	5.1.1, 5.1.2, 6.2.2, 10.8.1, 11.1.1, 11.7.1, 11.7.2, 12.3.1, 15.1.1, 15.1.2, 15.1.3, 15.1.4, 15.1.5, 15.1.6
- A baseline for current (as-is) and target (to-be) architecture has been defined. - Target architecture is in line with organization-wide goals (including compliance with regulations) and organizational responsibilities. - The EIAM and relevant processes have been established and maintained to enable application development and decision-supporting activities, consistent with IT plans. - The EIAM has been approved by (senior) management.	In addition: - The model should facilitate, in a secure and resilient manner, effectively creation, use and sharing of information as required by business objectives. - Target architecture addresses the priorities and performance objectives identified in the enterprise business plan.	In addition: - The EIAM should facilitate effective creation, use and sharing of information by the business in a manner that improves (at least maintains) integrity and is flexible, functional, cost-effective and timely. - The EIAM and relevant processes are reviewed on a periodic basis.	PO2.1	APO03.02	A.14.2.5	2.1	
- Independent assurance (internal or external) is obtained about the compliance of IT with relevant laws and regulations, the organization's policies, standards and procedures, and generally accepted practices. - The assurance activities have been described in an Audit Plan that is agreed by (senior) management and audit committee. - The outcomes of assurance activities are reported to (senior) management and audit committee.	In addition: - Performance of the independent assurance function is periodically assessed by the audit committee.	In addition: - Independent assurance (internal or external) is also obtained about the effectiveness and efficiency of IT.	ME4.7	MEA02.05, MEA02.06, MEA02.07, MEA02.08	A.5.1.2, A.12.4.1, A.18.2.1, A.18.2.2, A.18.2.3	18.5	5.1.2, 6.1.8, 6.1.8.1 [R.A], 6.1.8.2 [R.A], 10.10.2, 15.2.1, 15.2.1.1, 15.2.1.2 [R.A]
- All roles for managing information risks have been defined and assigned. - The accountability (and responsibility) for risk and security management has been established at business level to deal with organization-wide issues. - There is a statement of intent by senior management, which supports the goals and principles of information security in line with business strategy and objectives.	- Ownership and accountability (and responsibility) have been embedded for IT-related risks within the business at an appropriate senior level. - Additional security management responsibilities may be assigned at a system-specific level to deal with related security issues (e.g. by means of RACI matrices).	In addition: - Senior management gives formal guidance about appetite for information risk and approves any residual information risks.	PO4.8, DS5.1	APO13.01, APO13.03	5.3, A.6.1.1, A.7.2.1	5.1, 5.2	6.1.1, 6.1.1.1 [R.A], 6.1.2, 6.1.2.1 [R.A], 6.1.3, 6.1.3.1 [R.A], 6.1.1, 6.1.1.1, 6.1.1.2 [R.A], 6.1.1.3 [R.A], 6.1.1.4, 6.2.1, 15.1.1, 15.2.1.1 Supplement BIG: 3.1 1
- Segregation of roles and responsibilities has been defined and implemented, which reduces the likelihood of single individuals compromising critical processes. - The segregation of duties (SoD) has been approved by (senior) management.	- Approved segregation of duties (SoD) is implemented so personnel are only performing authorized duties relevant to their respective jobs and positions. - The implementation and execution of relevant procedures is periodically assessed.	In addition: - A SoD conflict-matrix has been defined and is reviewed periodically (by means of GRC tooling) against actual implementation of processes and systems. - The SoD conflict-matrix is at least reviewed after major changes in processes or systems have been implemented.	PO4.11	APO01.02	A.6.1.2, A.7.2.1, A.12.1.4	7.1	6.2.1, 10.1.3, 10.1.3.1, 10.1.3.2 [R.A], 10.1.3.3 [R.A], 10.1.3.4 [R.A], 10.1.4

Area	ID	Control name	Risk description	Control description	Maturity Indication Level 1	Maturity Indication Level 2
					Initial Controls are only partly defined and/or executed in an inconsistent manner and rely heavily on individuals.	Repeatable Controls are in place and executed in a structured and consistent, but informal, manner.
Risk Management	RM.01	Information risk management framework	Information risk & control management framework is not in line with the organization-wide model for risk management, resulting in misinterpretations of risks and/or failure to meet IT and business objectives.	An information risk management framework has been established and aligned to the organization's objectives and (enterprise) risk management framework.	- Information risks are not assessed or are assessed/considered in an ad-hoc manner. - There is no (information) risk framework and management process.	- An information risk management policy and process has been defined; is usually executed at a high level and is mostly applied for major projects or in response to problems. - A concise information risk framework and a high level risk appetite have been drafted with limited alignment with business objectives and business risks.
	RM.02	Risk assessment	Inherent and residual risks are not (timely) identified and assessed. Likelihood and impact are not determined, resulting in failure to implement action plans and mitigating controls or risk initiatives.	Risk assessments are executed to determine actual risk profiles regarding business objectives. The likelihood and impact of all identified risks are assessed on a recurrent basis, using qualitative and quantitative methods. The likelihood and impact associated with inherent and residual risks are determined per category, on a portfolio basis.	- Information risk assessments are rarely carried out and rely heavily on individuals. - In some cases, risk assessments are executed as part of the project plan.	- Risk assessments are executed as part of the risk management process and risks are identified qualitatively and/or quantitatively. - The likelihood and/or impact are determined based on general criteria and not fully aligned with the organization's business objectives. - Risk assessments (as part of project) are documented concisely.
	RM.03	Risk action and mitigation plan (including risk acceptance)	Risk responses are not identified and implemented. Required actions are not communicated and executed, leading to possible manifestation of risks. High costs/low benefits related to moderate or low risks. Failure to prioritize risks can lead to higher costs or lower benefits.	Control activities are prioritized and planned at all levels to implement the necessary risk responses, including identification of costs, benefits and responsibility for execution. Approval is obtained for recommended actions and acceptance of residual risks, and ensures that committed actions are owned by the affected process owner(s). The execution of plans is monitored and any deviations are reported to senior management.	- A risk action and mitigation plan is not in place. - If risks are identified, risk mitigation is inconsistently applied and/or relies heavily on individual competencies.	- Risk action and mitigation plans are defined using a non formalized approach. - Risk actions/responses are incomplete, have not been formalized/agreed and risk owners are only partly assigned to risk actions or accepted risks.
Human Resources	HR.01	Recruitment	If the recruitment process is inadequate, the organization runs the risk of inappropriately qualified or unscreened IT workers being employed.	Recruitment processes for IT personnel are maintained in line with the organization's general personnel policies and procedures (e.g. hiring, positive work environment, orientation, etc.). Processes are implemented to ensure that the organization has an appropriately deployed IT workforce, with the skills needed to achieve organizational objectives. Background checks are part of the IT recruitment process. The extent and frequency with which periodic reviews on these checks are carried out, is determined by the sensitivity and/or criticality of the function and are implemented for employees, contractors and vendors.	- Activities or measures for recruiting IT personnel are implemented and/or executed on an ad-hoc basis.	- Recruitment processes for IT personnel have been defined and implemented. - Processes are implemented to ensure that the organization has an appropriately deployed IT workforce. - Background checks are sometimes included in the IT recruitment process, but are not yet formalized.
	HR.02	Certification, training and education	Lack of professional training offered to IT staff could cause lack of competency among IT staff, e.g. unnecessary overtime costs, incorrect operational procedures, inefficient project management, IT security breaches, major incidents and business disruptions.	Education, training and/or experience are regularly verified to see whether personnel have the competencies needed to fulfil their roles. Qualification and certification programs Core IT competence requirements are defined and, wherever appropriate, qualification and certification programs are used to verify whether they are being maintained.	- Training and education is implemented on an ad-hoc basis. - Certification of personnel is not in place.	- Processes regarding certification, training and education are being implemented. - Individual personal development plans are available.

Maturity Indication Level 3	Maturity Indication Level 4	Maturity Indication Level 5	References				
Defined Controls are documented and executed in a structured, formal and proven manner	Managed and measurable Effectiveness of controls is periodically assessed and checked for quality	Continuous improvement An eco system has been established to provide continuous and effective control, and to resolve risks.	COBIT 4.1	COBIT 5	ISO 27K 2013	DNB 2014	BIR 2012 / BIG 2015
- An organization wide (information) risk management policy has been defined and agreed by (senior) management. - The policy and process description jointly defines how to deal with the essential elements of risk management (risk appetite/profile, risk ownership, risk process, risk assessment, risk mitigation and risk acceptance). - The information risk management framework is in line with the organization's risk management framework and includes business-driven components for strategy, programs, projects and operations. - Information risk classifications are based on a common set of characteristics from the enterprise risk management framework and information risk measurements have been standardized and prioritized, which includes signing impact, acceptability of residual risk and probabilities with the enterprise risk management framework (and business or IT objectives / risks). - Training for the framework is implemented.	In addition: - The information risk management framework and the operating effectiveness of the information risk management process are assessed on a periodic basis. - Reporting about information risk management (framework) is done on a periodic basis, thus allowing management to monitor the risk position and make informed decisions about the risk exposure it is willing to accept.	In addition: - The information risk management framework also focuses on efficiency-related aspects in primary business operations. - Information risk management is truly integrated into all business and IT operations; is well accepted and extensively involves the (IT) organization's employees and suppliers. - The information risk management framework and process is subject to continuous improvement.	PO6.2, PO9.1	EDM03.02, APO01.03	4.4, 6.1.1, 6.1.2, A.5.1.1, A.17.1.1, A.17.1.2, A.18.2.2	4.1	4, 5.1.1, 14.1.1, 14.1.2, 14.1.3, 14.1.4, 15.2.1
- Consistent and recurrent execution of risk assessments is enforced by clear and appropriate instructions, as part of the information risk management process and related information risk framework. - The risk assessment methodology is in line with the business and ensures that key business risks are identified. - The identified information risks are qualitatively and/or quantitatively assessed by the risk management process / framework or good practice sources. - Deviations in risk appetite / profile regarding risk mitigation are reported to (senior) management.	In addition: - The correlations between identified risks are (cross-functional) analyzed and documented. - Risk assessment methodology is reassessed on a periodic basis.	In addition: - Information risk assessment methodology is fully supported via automated tooling, automatic workflow processing and integrated dashboards.	PO9.4	AP012.02, APO12.04	4.4, 6.1.2, 6.1.3, A.5.1.2, A.6.1.5, A.17.1.1, A.18.2.2	4.2	4, 5.1.2, 6.2.2, 14.1.2, 15.2.1
- A process has been implemented so risks are formally recognized and recorded in a risk action plan. - Residual risks and mitigating controls are identified, analyzed and documented (in a risk register or risk action plan). - The identified risk response or acceptance/tolerance of residual risks are documented and approved by (senior) management and clearly assigned to business (risk) owners. - Progress in risk actions / responses as well as deviations are monitored. - The risk action plan is maintained and adjusted if necessary.	In addition: - If applicable, the priorities of risk mitigation actions or arguments for risk acceptance are reassessed. - Identified risk responses include explicitly identifying costs and benefits and monitoring budget utilization. - Operating effectiveness of the information risk management process is assessed on a periodic basis.	In addition: - Capturing, analyzing, monitoring and reporting of information risk management data are highly automated. - Senior management continuously assesses risk mitigation strategies.	PO9.6	AP012.04, APO12.05, APO12.06	6.1.3, A.6.2.1, A.6.1.5, A.6.1.3, A.11.2.1, A.11.2.8, A.12.1.4, A.12.6.1, A.14.1.1, A.15.1.1, A.15.1.3, A.15.2.2	4.3	6.2.1, 6.2.2, 7.1.3, 7.1.3.1 [R.A], 7.1.3.2, 7.1.3.3, 7.1.3.4 [R.A], 9.1.1.1, 9.1.1.3, 9.2.1, 9.2.5, 10.1.1, 10.1.4, 10.2.3, 10.3.1.1 [R.A], 10.7.4.2 [R.A], 10.8.5, 11.2.1.3 [R.A], 11.2.4.1, 11.7.1, 12.1.1.1, 12.3.1.2, 12.6.1
- Recruitment processes for IT personnel have been defined and implemented in line with the organization's general personnel policies and procedures (e.g. hiring, positive work environment, orientation). - Processes are implemented to ensure that the organization has an appropriately deployed IT workforce with the skills needed to achieve organizational objectives. - Background checks are part of the IT recruitment process. The extent and frequency with which periodic reviews on these checks are carried out, is determined by the sensitivity and/or criticality of the function and are implemented for employees, contractors and vendors. - Process designs are approved by (senior) management.	In addition: - The implementation and operational effectiveness of relevant recruitment procedures and job descriptions are periodically assessed.	In addition: - Based on the outcomes of periodic (self)assessments or risk assessments, the design and/or implementation of recruitment processes are adapted (improved). - Shortcomings in the recruitment process are reported to (senior) management.	POT.1, POT.6	AP007.01, APO07.05, APO07.06	A.6.1.1, A.7.1.1, A.7.1.2, A.13.2.4	8.1, 8.4	6.1.5, 6.1.5.1 [R.A], 8.1.1, 8.1.1.1, 8.1.1.2 [R.A], 8.1.1.3 [R.A], 8.1.1.4, 8.1.2, 8.1.2.1 [R.A], 8.1.2.2, 8.1.3, Supplement BIG: 8.1.2.3
- Processes for certification, training and education are implemented and executed. - Individual personal development plans (PDP's) are available. - Education, training and/or experience are used to regularly verify whether personnel have the competencies needed to fulfill their roles. - The corresponding processes are approved by (senior) management.	In addition: - Core IT competence requirements are defined and, wherever appropriate, qualification and certification programs are used to verify whether they are being maintained. - Monitoring implemented for the realization of PDP's.	In addition: - The implementation of processes for certification, training and education are reviewed on a yearly basis, and involves assessing education and training content for relevance, quality, effectiveness.	POT.2, DST.1, DST.2	AP007.03	7.2, A.7.2.2	8.2	8.2.1.1, 8.2.2, 8.2.2.1, Supplement BIG: 8.2.2.2 [A]

Area	ID	Control name	Risk description	Control description	Maturity Indication Level 1	Maturity Indication Level 2
					Initial Controls are only partly defined and/or executed in an inconsistent manner and rely heavily on individuals.	Repeatable Controls are in place and executed in a structured and consistent, but informal, manner.
	HR.03	Dependence on individuals	Critical dependency on key individuals will cause risks in case of departure or extended unavailability of key IT staff, if key development team leaves the organization or if it is not possible to recruit IT staff.	There is an absence of succession planning and staff backup for key/critical individuals and/or departments.	- Succession planning and staff back-up is not implemented. - Single points of failure regarding staffing are not identified.	- Back-up and replacement of key staff / positions is arranged at departmental level.
	HR.04	Job change and/or termination	User access is not timely disabled after employees have left the team or should no longer have access for any reason. Continuity of the function is endangered due to lack of knowledge transfer.	Expedient actions are taken regarding job changes, especially job terminations. Knowledge transfer is arranged, responsibilities are reassigned and access rights are removed so risks are minimized and continuity of the function is safeguarded.	- No or ad-hoc actions are taken regarding job changes or job terminations.	- Access rights of employees are changed, reassigned and/or removed based on job changes and/or job terminations.
	HR.05	Knowledge sharing	The absence of procedures and work instructions for enabling transfer of knowledge is resulting in ineffective and inefficient use of systems for supporting business processes. It also can lead to ineffective and inefficient delivery, maintenance and support of the system and associated infrastructure.	Transfer of knowledge and skills so end users can effectively and efficiently use the system to support business processes. Knowledge and skills are transferred so operations and technical support staff can effectively and efficiently deliver, support and maintain the system and associated infrastructure.	- Knowledge sharing is not implemented or knowledge is shared on ad-hoc basis.	- Decentralized informal processes are implemented for knowledge sharing. - Knowledge and skills often transferred on an individual basis.
	HR.06	Security awareness	People that are insufficiently aware about security risks do not understand potential consequences of their actions and are not able to bear this responsibility as part of their duties.	A security awareness program is implemented to educate users about their responsibility to protect the confidentiality, availability and integrity of information (assets).	- No security awareness activities are defined or performed.	- Security awareness activities are performed at departmental level.
Configuration Management	CO.01	Identification and Maintenance of Configuration Items	Business disruptions due to unauthorized and undocumented configuration changes in IT environment, lack of traceable sources during root cause analysis, ineffective alignment with other processes and inability to track responsible stakeholders.	Configuration procedures have been established to support management and logging of all changes to the configuration repository. These procedures are aligned with (and preconditional for) change management, incident management and problem management procedures.	- A configuration procedure has not been formalized. - Working practices are only established on an individual level and differ across platforms.	- A configuration procedure to identify and maintain configuration items has been defined but not formalized. - Data content of recorded items is not used by interrelated processes such as change management, incident management and problem management.
	CO.02	Configuration repository and baseline	The organization's system reliability is compromised without rapid detection and correction of improper configurations that can negatively impact performance or integrity.	A support tool and a central repository have been established for all relevant information about configuration items. All assets and changes to assets are monitored and recorded. A baseline of configuration items for every system and service is implemented as a benchmark after changes.	- Basic configuration management tasks, such as identifying and maintaining inventories of configuration items, are performed on an ad hoc basis. - Configuration documentation is incomplete and unreliable.	- Configuration management tools are partially used, but there is no standard. - Installed software, configurations and documentation are recorded but data content of recorded items is limited.

Maturity Indication Level 3	Maturity Indication Level 4	Maturity Indication Level 5	References				
			COBIT 4.1	COBIT 5	ISO 27K 2013	DNB 2014	BIR 2012 / BIG 2016
Defined Controls are documented and executed in a structured, formal and proven manner. Succession planning, job rotation and staff back-up are implemented. Training programs are in place to mitigate the risk of overdependence on key individuals. Key functions / positions are formally defined by senior management.	Managed and measurable Effectiveness of controls is periodically assessed and checked for quality. In addition: - Key/critical individuals and/or departments are identified throughout the organization and/or reassessed on a yearly basis.	Continuous improvement An eco system has been established to provide continuous and effective control, and to resolve risks. In addition: - Effectiveness of the process for succession planning and staff back-up is periodically reviewed. - Succession planning is in line with IT and business strategy.	PO7.5	APO07.02		8.3	
Approved processes are implemented to transfer knowledge and reassign or withdraw access rights. Knowledge transfer is arranged, responsibilities are reassigned and access rights are removed so risks are minimized and continuity of the function is safeguarded. Job hand-over steps have been described.	In addition: - Exit interviews are conducted and the correctness and timeliness of changes, reassignment or withdrawal of access rights is periodically reviewed.	In addition: - Effectiveness of the processes for job change and/or termination is periodically reviewed and adequate improvements are implemented.	PO7.8	APO07.01	A.7.2.3, A.7.3.1, A.8.1.4, A.9.2.6	8.5	8.2.3, 8.3.1, 8.3.2, 8.3.3
Approved processes are implemented organization-wide to transfer knowledge and establish and maintain adequate documentation, training and implementation materials so systems can be effectively used to support business processes. This involves end users as well as operations and technical support staff.	In addition: - Adequacy of support documentation is assessed on a periodic basis.	In addition: - Knowledge and skills are transferred so end users can efficiently use the system to business processes. - Knowledge and skills are transferred to enable operations and technical support staff to efficiently deliver, support and maintain the system and associated infrastructure.	PO7.5, A14.3, A14.4	APO07.02, BAI08.01, BAI08.02, BAI08.03, BAI08.04	A.8.1.4, A.7.2.2, A.12.1.1, A.14.2.9, A.15.1.6	8.3, 9.1, 9.2	6.1.7, 10.1.1, 10.3.2, 13.2.2 Supplement BIG 6.1.7.2
A security awareness program has been included in an information security plan and is executed accordingly organization-wide. There is alignment with security policies.	In addition: - Activities about security awareness include a mandatory e-learning program which has to be successfully completed with an on-line examination.	In addition: - The effects of security awareness activities are monitored. - Correlation of security incidents, due to lack of awareness, leads to adjustments in security awareness activities.	PO7.4, DS7.1, DS7.2	APO01.04, APO07.03, APO13.02	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	9.1, 9.2	6.1.5, 6.1.5.1 [R.A], 7.1.3, 8.1.1.2 [R.A], 8.1.1.3 [R.A], 8.2.1.2, 8.2.2, 8.2.3, 8.2.3.1 [R.A], 10.7.3, 11.3.1, 11.3.2, 11.3.3, 14.1.1.1 [R.A] Supplement BIG 8.2.2.2 [A]
Formalized configuration procedure and working practices are in place to identify and maintain all configuration items and their attributes. The procedure is aligned with change management, incident management and problem management procedures. The procedure is documented, standardized and communicated. There is a policy for physical asset tagging and new assets are registered in procurement procedures. Processes are implemented to maintain compliance with, and control over, purchased, deployed, archived and expired licenses.	In addition: - There is a process for periodically reviewing relevant documentation, timely execution and integrity of the repository (including licenses). - The implementation and execution of relevant procedures regarding configuration management are periodically assessed. - Management receives regular reports which lead to improvement plans. - Procedures and standards are incorporated into training.	In addition: - Exception analysis is performed on a continuous basis and exceptions are investigated. - Any shortcomings or trends are reported to management. - There is full integration of interrelated processes, and configuration data is used and updated in an automated manner.	DS9.2, DS9.3	BAI10.03, BAI10.04, BAI10.05, DSS02.05	A.8.1.1, A.8.1.2, A.8.2.2, A.12.5.1, A.14.3.1	13.1	7.1.1, 7.1.2, 7.2.2, 12.4.1.3
All assets and changes to assets are monitored and recorded in a central repository. The relationships amongst configuration items are identified and maintained. A configuration management tool (or similar tools) is (being) implemented across platforms. Some automation is used to assist in tracking equipment and software changes. Configuration baselines for components are defined and documented as a benchmark after changes. Changes to the configuration repository (CMDB) are logged.	- Automated tools, to assist in tracking equipment and software changes, are utilized to enforce standards and improve stability. - There are mechanisms to monitor changes against the defined repository and baseline. - Physical verifications are periodically performed. - Changes logged in the configuration repository are periodically analyzed. - Management receives reports periodically.	- All IT assets are managed within a central configuration management system that contains all necessary information about components and their interrelationships as well as data for repair, service, warranty, upgrade and technical assessments. - Processes and automation implemented for software and hardware asset management (including licenses). - Management receives automated reports periodically.	DS9.1	BAI10.01, BAI10.02, BAI10.04, DSS02.01	A.8.1.1, A.8.1.2, A.8.1.3, A.12.6.1	13.2	7.1.1, 7.1.2, 12.6.1

Area	ID	Control name	Risk description	Control description	Maturity Indication Level 1	Maturity Indication Level 2
					Initial Controls are only partly defined and/or executed in an inconsistent manner and rely heavily on individuals.	Repeatable Controls are in place and executed in a structured and consistent, but informal, manner.
Incident / Problem Management	IM.01	Incident management	Incidents are not properly classified and are treated incorrectly in the incident and problem management process, ultimately decreasing the performance (e.g. integrity and availability) of IT.	A formal incident management process is communicated and implemented. Procedures are in place to ensure that all incidents and failures are recorded, analyzed, categorized and prioritized according to impact. All incidents are tracked and periodically reviewed to ensure they are resolved in a timely manner.	- An incident management policy has not been defined. - Roles and responsibilities are not defined. - There are no procedures to ensure that all incidents and failures are recorded and analyzed. - Incidents are tracked and reviewed on an individual basis. - Responses to information security incidents are ad hoc.	- An informal incident management process has been defined to address critical aspects. - Roles and responsibilities have been partially defined. - The majority of incidents is recorded and analyzed, but deviations from established norms or standards are likely to be undetected. - Criteria have not been defined for categorizing and prioritizing incidents according to impact. - Incidents are dispatched on ad-hoc basis. Incidents are tracked on a manual basis and monitored individually. - No formal training and communication about standard procedures.
	IM.02	Incident escalation	Incidents are not identified, resolved, reviewed, escalated and analyzed in a timely manner, ultimately leading to decreased performance (e.g. integrity and availability) of IT.	Incident management (or service desk) procedures are established so, if incidents cannot be resolved within the agreed period, service levels are appropriately escalated and, if appropriate, workarounds are provided. Incident ownership and life cycle monitoring remain with the service desk for user-based incidents, regardless which IT group is working on resolution activities.	- There is an absence of policy to ensure that incidents which cannot be resolved timely are escalated. - Incidents are tracked and reviewed on an individual basis. - Responses to information security breaches are unpredictable. - Incident ownership is not defined.	- There is an informal incident escalation process. - Incidents that cannot be timely resolved are escalated. - No criteria defined for prioritization of incidents. - Absence of centralized knowledge base. - Response teams are not trained and rely on key individuals.
	IM.03	Incident response on (cyber) security incidents	Absence of effective and timely response or follow up of (cyber) security incidents.	The organization needs to have an incident response capability to detect (cyber) security incidents quickly, contain them, mitigate impact, and restore and reconstitute services in a trusted manner.	- No plans / procedures to ensure that (cyber) security incidents are adequately handled. - Responses to (cyber) security incidents often occur on an individual basis.	- The need to respond to cyber incidents is recognized by management. - There is an informal procedure for responding to (cyber) security incidents. - Prevention, mitigation, preparation for and recovery from (cyber) security incidents are in the early stages of development.
	IM.04	Problem management	Incidents are not properly classified and treated incorrectly by the incident and problem management process, ultimately reducing the performance of IT.	A formal problem management process has been defined and implemented. Procedures are in place to identify (proactively & reactively) causes of (potential) incidents and problems, and to control known errors until they are resolved. Structural errors in IT-services are minimized, whereby reducing the number and impact of potential problems.	- Absence of problem management policy. - Roles and responsibilities for problem management are not defined. - No procedures have been defined to identify causes of incidents and failures. - Problems are unlikely to be detected.	- There is an informal problem management process. - Key knowledgeable individuals provide some assistance with problems relating to their area of expertise, but the responsibility for problem management is not assigned. - The registration and tracking of problems and their resolutions is fragmented within the response teams.
Change Management	CH.01	Change standards and procedures	The lack of a formal IT change management process, which ensures that proposed changes are reviewed, authorized, tested, implemented, documented and released in a controlled manner, could lead to business disruptions and/or loss of confidential data.	Formal change management procedures have been set up to handle all requests (including maintenance and patches) for changes to applications, procedures, processes, system and service parameters, and the underlying platforms, in a standardized manner.	- Absence of change management policy and change management procedure. - Changes and requests for changes are not handled in a standardized or consistent manner. - Roles and responsibilities are not defined. - Formal approval (authorization) of changes does not take place. - There is poor or non-existent documentation of changes.	- A change management policy has been defined to cover critical aspects. - A consistent change management process is in place and most changes are executed in accordance with this process. - Roles and responsibilities are partially defined. - The process is informal and unauthorized changes may occur. - Version control is implemented for critical system parameters.

Maturity Indication Level 3	Maturity Indication Level 4	Maturity Indication Level 5	References				
Defined Controls are documented and executed in a structured, formal and proven manner.	Managed and measurable Effectiveness of controls is periodically assessed and checked for quality.	Continuous improvement An eco system has been established to provide continuous and effective control, and to resolve risks.	COBIT 4.1	COBIT 5	ISO 27K 2013	DNB 2014	BIR 2012 / BIG 2016
The formalized incident management policy is documented and communicated. Roles and responsibilities of the organization and suppliers are clearly defined. Legal and criminal investigative issues are defined and addressed. There is a formal and accessible function which registers, communicates, dispatches and analyzes reported incidents and problems. Incidents are categorized and prioritized according to impact. Security incidents are prevented or detected and here is a process to deal with them in a timely and effective manner. Information is shared among staff in a proactive and formal manner. Monitoring implemented to see if incidents are resolved in a timely manner. There are limited management reviews for incidents and resolution analysis.	In addition: - Incidents are proactively analyzed to identify causes. - A function (response team) is implemented which recognizes and manages security emergencies. - The security incident management process interfaces with key organization functions and external service providers (if applicable). - The timely resolution of incidents is strictly monitored. Unresolved incidents (known errors and workarounds) are recorded and reported as input for problem management. - The quality and operating effectiveness of the incident management process is periodically reviewed.	In addition: - The registration, reporting and analysis of incidents and resolutions are automated and fully integrated with configuration and problem management. - Most systems have been equipped with automatic detection and warning mechanisms, which are continuously tracked and evaluated. - Incident and problem management are analyzed for continuous improvement.	DS8.6, DS8.1, DS8.2, DS8.4, DS8.5	DSS02.01, DSS02.02, DSS02.03, DSS02.05, DSS02.06, DSS02.07	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	15.1, 15.2	8.2.3, 12.6.1, 13.1.1, 13.1.1.1, 13.1.1.2 [R], 13.1.1.3 [A], 13.1.1.4 [R], 13.1.2, 13.2.1, 13.2.3, 13.2.2 Supplement BIG: 13.1.1.5 13.1.1.6 [A]
The formalized incident management policy includes an escalation procedure. Escalation criteria have been defined. The escalation procedure is based on agreed service levels for incidents which cannot be resolved immediately. Categorization and prioritization is done based on impact analysis, defined criteria and service levels. The response teams receive necessary training. Incident ownership is defined.	In addition: - Advice is consistent and incidents are resolved in a timely fashion with a structured escalation process. - Significant incidents are reported to management. - Escalation procedures are understood and thoroughly enforced. - Response teams receive regular training. - The escalation process is periodically evaluated.	In addition: - The escalation process is evaluated on a continuous basis. - Incident resolution is regularly analyzed to improve the process, and shortcomings and trends are reported to management.	DS8.3	DSS02.04	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	15.2	13.1.1, 13.2.1, 13.2.3, 14.1.1, 14.1.2
In addition to the regular incident and problem management procedures, plans are in place to address the prevention and mitigation of, preparation for, response to, and recovery from (cyber) security incidents. Roles and responsibilities are defined and assigned. The organization can quickly respond to a breach at the appropriate scale or escalation level based on the possible impact.	In addition: - Incident response coordination plans include all business functions such as regulatory affairs, legal, compliance and audit, and business operations. - Relevant relationships with third parties are maintained (such as law enforcement, specialist firms, CERT). - All (cyber) security incidents are reported to management and appropriate authorities. - Response plans are based on risk analysis on the type of data (assets) being compromised and/or a threat and vulnerability analysis.	In addition: - Continuous improvement for prevention and mitigation, preparation for, response to, and recovery from (cyber) security incidents by identifying risks and developments. - (Cyber) Security incident resolution is regularly analyzed to improve the process and shortcomings are reported to management.		AP012.06, DSS04.03, DSS05.07	A.16.1.5	15.1, 15.2	
A formalized problem management policy has been documented and communicated. Procedures are in place to identify causes of problems. The roles and responsibilities of the organization and suppliers are clearly defined. There is a function which registers, communicates, dispatches and analyzes reported problems. Problems are prioritized and assigned to response teams in accordance with the policy. Information is shared among response teams in a proactive and formal manner. Management analysis of problem identification and resolution is limited and informal. Known errors are registered and controlled until they are resolved.	In addition: - Problems are proactively analyzed to identify causes. - External sources (such as suppliers, user groups, conferences) are systematically consulted to proactively identify problems. - Progress in problem diagnosis and resolutions monitored and structural errors are minimized. - The majority of problems are identified, recorded and reported, and resolutions are initiated. - Problem management is periodically reviewed.	In addition: - Tools are used for recording, reporting and analyzing problems and resolutions. - Problem management processes are integrated with configuration and change management. - Most systems have been equipped with automatic detection and warning mechanisms, which are continuously tracked and evaluated. - Problem management is analyzed for continuous improvement.	DS10.1, DS10.2, DS10.3, DS10.4	DS03.01, DS03.02, DS03.03, DS03.04, DS03.05	A.7.2.3, A.12.6.1, A.16.1.1, A.16.1.2, A.16.1.3	15.1, 15.2	8.2.3, 12.6.1, 13.1.1, 13.1.1.1, 13.1.1.2 [R], 13.1.1.3 [A], 13.1.1.4 [R], 13.1.2, 13.2.1, 13.2.3, 13.2.2 Supplement BIG: 13.1.1.5 13.1.1.6 [A]
The change management policy and working practices are documented, standardized and communicated. A formal change management process is in place for changes to applications, procedures, processes, systems and service parameters and the underlying platforms. The process includes all elements from promotion to production, including change authorization, impact analysis, release management, tracking of changes and roll back procedures. Roles and responsibilities are defined and assigned. Change requests and changes are executed in a standardized manner. Changes are documented and documentation is current and correct. A version control system (VCS) for applications, procedures, system parameters, platforms etcetera is (being) implemented.	In addition: - The change management policy has been fully embedded into the organization and implemented consistently for all changes. - The quality and effectiveness of the change management process is periodically reviewed. - Reports are sent to senior management for review. - Tools are used to detect unauthorized changes.	In addition: - The change management policy is regularly reviewed and updated. - Roles and responsibilities are reviewed on an ongoing basis. - Exception analysis is performed and exceptions are investigated. - Management receives regular reports on shortcomings and trends, which lead to improvement plans. - Reporting requirements are regularly reviewed and updated.	A16.1, A16.4, A16.5	BAI06.01, BAI06.02, BAI06.03, BAI06.04	8.1, A.12.1.2, A.14.2.2, A.14.2.4	10.1	10.1.2, 10.1.2.1, 10.1.2.2 [R,A], 12.5.1

Area	ID	Control name	Risk description	Control description	Maturity Indication Level 1	Maturity Indication Level 2
					Initial Controls are only partly defined and/or executed in an inconsistent manner and rely heavily on individuals.	Repeatable Controls are in place and executed in a structured and consistent, but informal, manner.
	CH.02	Impact assessment, prioritization and authorization	Inadequate impact assessment, prioritization or authorization could lead to business disruptions, corruption and/or loss of confidential data.	All change requests are assessed in a structured manner to determine impact on the operational system and its functionality. All changes are categorized, prioritized and authorized.	- There is no procedure for the assessment, prioritization and authorization of changes. - Roles and responsibilities are not defined. - Impact assessments for change requests are executed on an ad hoc basis and unauthorized changes can take place. - The process for categorizing and prioritizing changes is not standardized.	- Analysis is carried out into the impact of IT changes on business operations. - Criteria for the analysis are being developed. - An informal process is in place to categorize, prioritize and authorize changes. - Roles and responsibilities are partially defined. - Business process owners are mainly involved in the approval process.
	CH.03	Emergency changes	Critical disruption of business processes cannot be fixed in a timely manner because additional lead time is needed during a standard change management procedure. Unauthorized changes have been made during an emergency situation which remain unnoticed.	Emergency changes requiring immediate implementation are properly handled to ensure minimal impact to systems and IT applications. The emergency change is registered, evaluated and tested after implementation and approved by senior management.	- Absence of emergency change management procedure. - Requests for emergency changes and emergency changes are not handled in a standardized manner. - Poor or non-existent documentation of emergency changes. - Roles and responsibilities are not defined. - Formal approval (authorization) of emergency changes does not take place.	- An (informal) emergency change management process is in place, which covers critical aspects of the process. - Roles and responsibilities are partially defined. - After the emergency change, control steps are not always consistently completed.
	CH.04	Test environment	Absence of a secure, controlled and representative test environment could lead to insufficient/unreliable testing before changes are introduced to the production environment of a critical application, which could cause negative impact on application's functionality, performance and security.	A secure test environment has been defined and established, which represents the planned production environment in terms of security, internal controls, operational practices, data quality, privacy requirements and workloads.	- A test environment has not been structurally defined and established for use when developing and testing changes. - Policy for using a test environment has not been defined. - Errors are likely to occur, together with interruptions in the production environment, because of poor change management.	- An informal policy is in place for using a test environment when developing and testing changes. - Changes are developed and tested outside the production environment. - The test environment is representative of the production environment for critical aspects.
	CH.05	Testing of changes	Inadequate or incomplete testing could lead to business disruption or unreliable data processing.	Changes are tested independently in accordance with the defined test plan prior to migration to the operational environment. It is ensured that the plan considers security and performance.	- Absence of policy for the testing changes. - Roles and responsibilities for testing changes are not defined. - Testing is done on an individual / ad hoc basis. - Test plans are not drawn up prior to testing.	- An informal procedure is implemented for testing changes. - Roles and responsibilities have been partially defined. - Test plans have been made, but there are no formal criteria regarding content of test plans. - Controls are partially implemented to ensure that changes are tested in accordance with the defined test plan. - Test results are partially documented. - No criteria for retaining or disposing of test results.
	CH.06	Promotion to production	Business disruptions or unauthorized changes due to insecure handing over of changes into the production system.	After testing, handover of the changed system to operations is controlled, keeping it in line with the implementation plan. Approval is obtained from key stakeholders, such as users, system owner and operational management. Wherever appropriate, the system is run parallel to the old system for a while, and behavior and results are compared.	- Policy has not been defined for the handover of changed systems to operations. - Implementation plans are drawn up on an ad hoc basis. - Roles and responsibilities are not defined.	- An informal handover policy is in place, which covers critical aspects, including the approval of the process. - Roles and responsibilities are partially defined. - Implementation plans are made, but there are no formal criteria regarding the content of implementation plans. - Controls are partially implemented to ensure that the handover occurs in accordance with the defined implementation plan. - Acceptance tests are normally executed.

Maturity Indication Level 3	Maturity Indication Level 4	Maturity Indication Level 5	References				
			COBIT 4.1	COBIT 5	ISO 27K 2013	DNB 2014	BIR 2012 / BIG 2015
Defined Controls are documented and executed in a structured, formal and proven manner. A formal procedure for the assessment, categorization, prioritization and authorization of changes has been formalized and communicated. Impact assessments take place prior to a change. Security, legal, contractual and compliance implications are considered in the assessment process. There is a formal procedure for the authorization of changes (Change Advisory Board). Each requested change is formally approved (via Change Advisory Board) by the business process owner and stakeholders. Prioritization and categorization are based on predefined criteria.	Managed and measurable Effectiveness of controls is periodically assessed and checked for quality. The procedure for the assessment, categorization, prioritization and authorization of changes is implemented consistently. - All changes are subject to thorough planning and impact assessment to minimize the likelihood and impact of post-production problems. - The number of disruptions or data errors caused by inaccurate specifications and/or an incomplete impact assessment is kept to a minimum. - The operational effectiveness of procedures is measured and reviewed periodically. - Senior management receives regular reports.	Continuous improvement An eco system has been established to provide continuous and effective control, and to resolve risks. The assessment procedure is regularly reviewed and updated. - The measurement criteria are regularly reviewed. - Management receives regular reports which lead to improvement plans. - Reporting requirements are regularly reviewed and updated.	A/5.2	BAI/05.01	8.1, A.12.1.2, A.12.5.1, A.14.2.2, A.14.2.4	10.2	10.1.2, 10.1.2.1, 10.1.2.2 [RA], 12.5.1, 12.8.1
The emergency change management procedure is formalized, documented and communicated. Emergency change requests and emergency changes are executed in a standardized manner. Roles and responsibilities are clearly defined and assigned. Emergency changes are authorized and documented. The control steps, including approval, are completed after the emergency change in accordance with the procedure. Critical deviations from the process are reviewed.	In addition: - The emergency change procedure, including post implementation review, is consistently followed for all emergency changes. - Documentation is current and correct. - There is a process for monitoring the quality and performance of the emergency change management process. - The quality and effectiveness of the emergency change process is periodically reviewed. - Reports are sent to senior management and reviewed.	In addition: - The emergency change management process is regularly reviewed and updated. - Exception analysis is performed and exceptions are investigated. - Management receives regular reports which lead to improvement plans. - Reporting requirements are regularly reviewed and updated. - Roles and responsibilities are reviewed regularly.	A/5.3	BAI/05.02	8.1, A.12.1.2	10.1	10.1.2
A formal test environment policy has been defined and implemented. A secure test environment has been defined and established. The test environment is representative of the production environment (factors include workload/stress, operating systems, application software, database management systems, network and computing infrastructure). The test environment cannot interact with production environments (in particular (pre) production). The test environment is protected against unauthorized access and use. Ownership of the test and production environments is clearly defined. There are guidelines for using data in the test environment to ensure compliance with applicable privacy laws.	In addition: - A process for monitoring the use of a test environment is in place, and incidents are reviewed and remedied. - The test and production environments are periodically reviewed to check whether the test environment is sufficiently representative of the production environment. - The security of the test environment and test data management is periodically reviewed. - Reports are sent to senior management for review.	In addition: - Policy is continuously reviewed and improved. - Roles and responsibilities are reviewed on an ongoing basis. - Management receives regular reports which lead to improvement plans. - Reporting requirements are regularly reviewed and updated. - Tooling for creating subsets and data anonymization is implemented.	A/7.4	BAI/07.04	8.1, A.9.4.5, A.12.1.4, A.14.2.6, A.14.3.1	10.3	10.1.4, 10.1.4.1, 10.1.4.2, 10.1.4.3 [RA], 12.4.2, 12.4.3, 12.4.3.1 Supplement BIG: 12.4.3.2
A formal policy for testing changes has been documented and communicated. Roles and responsibilities are defined and assigned. Test plans are made prior to testing. Criteria have been established to ensure that necessary elements, such as security and performance, are included in the test plan. Changes are tested independently in accordance with the test plans. A procedure is being implemented to manage retention or disposal of test results. Fallback or back out plans are prepared and tested prior to changes being promoted into production.	In addition: - All changes to critical applications are evaluated and tested to ensure that there will be no adverse consequences for the operations or security of the organization. - Changes are only tested in the test environment. - Security and performance requirements are validated. - The test procedures, test plan and execution of testing processes are periodically reviewed. - Reports are sent to senior management for review.	In addition: - Policy is continuously reviewed and improved. - Roles and responsibilities are reviewed on an ongoing basis. - All incidents with the change management / test process are reviewed and remedied. - Management receives regular reports which lead to improvement plans. - Reporting requirements are regularly reviewed and updated.	A/7.5	BAI/07.05, BAI/03.08	8.1, A.9.4.5, A.12.1.2, A.14.2.3, A.14.2.8, A.14.3.1	10.4	6.1.4, 10.1.2, 12.4.2, 12.4.3
A formalized policy for the handover of changed systems is documented and communicated. Procedures for the use of DTAP environments and an approval process are in place. The approval process includes a formal documented sign-off from (defined) key stakeholders. Roles and responsibilities are defined and assigned. Access rules to the various (DTAP) environments are defined to ensure necessary segregation of duties. Implementation plans are made prior to the handover and handovers are implemented in accordance with the plans. Wherever appropriate (identified in impact assessment), the system is run to parallel the old system for a while, and behavior and results are compared. Acceptance criteria are defined and acceptance tests are executed and logged. Controls are in place to ensure that accepted changes are actually part of the handover to operations (completeness).	In addition: - A procedure is in place for updating system documentation, relevant contingency plans, etc. - The handover policy is implemented consistently. - A change will only be closed after all activities and registrations are implemented and evaluated. - The handovers are periodically reviewed and reports are sent to senior management.	In addition: - Policy, roles and responsibilities are continuously reviewed and improved. - All incidents during testing and implementation are reviewed and remedied. - Management receives regular reports which lead to improvement plans. - Reporting requirements are regularly reviewed and updated.	A/7.8	BAI/07.08	A.14.2.9, A.14.2.3	10.5	6.1.4, 10.3.2, 10.3.2.1 [RA], 10.3.2.2, 12.5.2

Area	ID	Control name	Risk description	Control description	Maturity Indication Level 1	Maturity Indication Level 2
					Initial Controls are only partly defined and/or executed in an inconsistent manner and rely heavily on individuals.	Repeatable Controls are in place and executed in a structured and consistent, but informal, manner.
System Development	SD.01	Methodology for secure development and implementation of software	Software and/or system developments not designed and implemented according to agreed functional, technical and security requirements, approval standards, and the information architecture, which results in business requirements not being met.	A structured approach (secure software development life cycle process) to in-house development and acquisition of software is in place, which ensures that potential risks to internal controls are adequately assessed and mitigated, and that confidentiality, integrity and availability aspects are addressed. For each new development or acquisition, approval is required by an appropriate level of business and IT management.	- No structured approach in place. - Ad-hoc actions are taken regarding system and software development.	- Secure coding guidelines are defined and are applied on a irregular basis. - Reviews of security requirements and source codes are based on individual initiatives. - Formal "kill gates" not implemented regarding security in project management methodology and security testing.
	SD.02	Developer access to production	Developers with access to the production environment jeopardize segregation of duties, which could ultimately lead to unauthorized access or changes to programs and data.	Employees (developers) involved in the development and implementation of changes to in-scope applications and supporting operating systems and databases are restricted from having write-level access to the production environment. The employees (developers) responsible for releasing the source code to production do not have write-level access to the test or development environment.	There is no policy regarding restrictions to the production environment for developers.	- Limited policy and instructions defined for developer access to production. - Developers have no write-level access to the production environment. - In case of high priority incident resolution, write-level access to production is granted to developers.
	SD.03	Data conversion and/or migration	Anomalies during data conversion / migration are not detected (timely) leading to decreased integrity (e.g. accuracy and completeness) in (financial) data.	Management has controls in place to ensure that data conversion (relevant to financial reporting) is accurate and complete, and data conversion controls are designed by the entity to maintain the integrity of data throughout the conversion process.	No controls defined regarding data conversion and/or migration	- Limited controls are implemented to validate the accuracy and completeness of data conversion / migration. - The defined controls are documented.
Data Management	DM.01	Data (and system) ownership	Unclear or ambiguous ownership can jeopardize effective decision-making, protection of data and information systems, and control of data management.	The business is provided with procedures and tools, enabling it to address its responsibilities for ownership of data and information systems. Owners make decisions about classifying information and systems and protect them in line with this classification.	- There is no formal policy for data ownership and data classification. - System ownership is not, or is informally, addressed. - Roles and responsibilities for data ownership have not been formally assigned.	- There is a policy for system and data ownership. - The policy gives a clear description about roles, responsibilities and ownership. - Responsibility has not been formally assigned for all data and systems.
	DM.02	Classification	Decisions about classifying information and systems, as well as related level of protection, are not in line with the business requirements. Data may be compromised in various ways if sensitive data is not classified at the appropriate level.	Establish a classification scheme that applies throughout the organization, based on the criticality and sensitivity (e.g., public, confidential, top secret) of organization data. This scheme should include details about data ownership; definition of appropriate security levels and protection controls; and a brief description of data retention and destruction requirements, criticality and sensitivity. It should be used as the basis for applying controls such as access controls, archiving and encryption.	- A classification scheme has not been developed. - The organization makes no distinction between different levels of data criticality or sensitivity.	- Classification of data is informal and ad-hoc. - Local interpretations of data classification schemes are used. - Data owners (if assigned) decide for themselves if data is sensitive and if additional controls are needed.
	DM.03	Security requirements for data management	Inadequate security requirements for data management could lead to unmet business objectives and non-compliance with organization's security policy and regulatory requirements (fines).	Policies and procedures are defined and implemented to identify and apply security requirements applicable to the receipt, processing, storage and output of data in order to meet business objectives, the organization's security policy and regulatory requirements (e.g. data privacy).	No formal procedures or policy in place concerning security requirements for data management.	- Limited and informal security requirements for data management have been established. - There is no organization-wide policy or procedures to identify or apply security requirements for data management.

Maturity Indication Level 3	Maturity Indication Level 4	Maturity Indication Level 5	References				
			COBIT 4.1	COBIT 5	ISO 27K 2013	DNB 2014	BIR 2012 / BIG 2015
Defined Controls are documented and executed in a structured, formal and proven manner. The organization has implemented a structured approach to in-house development and acquisition of software. Mandatory secure coding standards are defined. For each new development or acquisition, approval by an appropriate level of business and IT management is required. Software quality assurance methodology ensures that mandatory "kill gates" (including risk assessment, source code review and testing) for information security cannot be bypassed and are documented. Security awareness training is attended on a voluntary basis.	Managed and measurable Effectiveness of controls is periodically assessed and checked for quality. In addition: - The effectiveness of a formal and structured approach is assessed periodically and, if applicable, actions for improvement are followed up. - A mandatory security & risk education program for developers is implemented.	Continuous improvement An eco system has been established to provide continuous and effective control, and to resolve risks. In addition: - Based on the evolving threat landscape, risk assessments are conducted periodically. The scope of the risk assessments includes the implemented software products as well as the development methodology itself. - Residual risk is reported to accountable (senior) IT management.	PO6.3, A12.5, A12.7, A12.8	APO11.02, APO11.05, BAI03.02, BAI03.03, BAI03.05, BAI03.06, BAI03.09	8.1, A.8.1.5, 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	10.5, 16.1	6.1.4, 10.3.2, 10.3.2.1 [RA], 10.3.2.2, 12.5.5, 12.5.1
Comprehensive policy and instructions are defined, implemented and approved by (senior) management. Developers have no write-level access to production, and system managers that promote software to production do not have write-level access to the development, test and acceptance environment. Exceptions to policy or instructions are approved beforehand by the system/process owner and strict logging and/or 4-eye principle is applied during the period that temporary write-level access is granted.	In addition: - Effectiveness of the implementation and execution of relevant policy and instructions are periodically assessed and documented. - Improvements are defined based on the assessments. - Samples of exception logs are assessed on a periodic basis.	In addition: - Real-time monitoring and detection of write-level access to production is implemented via automated detection and response technology, e.g. SIEM. - Exceptions are reported on a monthly basis to (senior) management.	D55.3, D55.4	DSS05.04	A.9.1.1, A.9.2.3, A.9.4.5, A.14.2.1	17.1	11.1.1, 11.2.2, 12.4.3, 12.4.3.1 Supplement BIG: 12.4.3.2
A risk and business impact analysis is performed as justification for the defined controls. The design of the controls is documented and formally accepted by the system/process owner. The controls ensure the accuracy and completeness of the data conversion/migration and also maintain the integrity of the data. Outcomes of the (manual and/or automated) performed integrity checks are documented and assessed by the system/process owner in order to formally accept the data conversion.	In addition: - An evaluation of the data conversion / migration process is conducted by the project team. - Lessons learned and improvement areas are identified and documented for future usage.	In addition: - The conversion / migration approach is embedded into the project management methodology. - Controls (for accuracy, completeness and integrity) are fully automated. Manual interventions are exceptional.	A17.5	BAI07.02			
A approved policy gives a clear description about roles, responsibilities and ownership. Policy and procedures support the classification and protection of information assets, enable efficient delivery and use of business applications, and facilitates effective security decision-making. Policy and procedures are communicated through the whole organization and have been applied to business-critical data and information systems	In addition: - Policy and procedures are implemented in the organization and have been applied to all application systems and enterprise architecture, as well as internal and external data communication.	In addition: - Compliance with data management policy is periodically reported to senior management. - The policy is yearly reviewed, updated and reapproved by senior management.	PO4.9	APO01.06	A.8.1.1, A.8.1.2, A.8.2.1, A.8.2.2, A.8.2.3	8.1	6.1.3, 6.1.3.1 [RA], 7.1.2, 7.2.1, 7.2.2, 10.7.3
A data classification scheme and related guidance are implemented and applied throughout the organization. Data ownership, definitions and requirements for different levels of data classification are explicitly described in the guidelines. The guidelines are used as a basis for applying the required controls for critical business processes and/or applications. The classification scheme is approved by senior management.	In addition: - The guidelines are used as a basis for applying the required controls for all business processes and applications organization-wide. - The implementation and execution of relevant procedures, as well as the correctness and completeness of classification schemes, are periodically assessed.	In addition: - (Changes in) Data classification is fully supported via automated tooling, automatic workflow processing and integrated dashboards. - Data classification is integrated into information/data lifecycle management.	PO2.3	APO03.02	8.2.1, 8.3.1, 9.1.1	2.2	7.2.1, 7.2.1.1 [RA], 10.7.1, 11.1.1 Supplement BIG: 7.2.1.2
A policy has been defined, implemented and communicated to protect sensitive data and messages from unauthorized access and incorrect transmission and transport. The policy has been approved by (senior) management. A formal process is in place, which identifies sensitive data and addresses the business needs or confidentiality of data and compliance with applicable laws and regulations (e.g. data privacy). Data classification has been agreed with business process owners. Requirements of business-critical systems are business aligned and have been established for physical and logical access to data output, and confidentiality of output is clearly defined and taken into consideration.	In addition: - Implementation and execution of relevant procedures regarding security requirements for data management are periodically assessed. - Requirements for all information systems have been established concerning e.g. physical protection, back-up of sensitive data and data storage in the cloud (at third parties). - Awareness programs have been established to create and maintain awareness about security when handling and processing of sensitive data.	In addition: - The definition and application of security requirements are integrated into information/data lifecycle management. - Efficiency and costs are also taken into account when specifying security requirements for data management.	DS11.6	DSS01.01, DSS05.08, DSS06.05	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	12.3	10.5.1, 10.7.1, 10.7.3, 10.8.3, 10.8.3.1, 10.8.3.2 [RA], 10.8.4, 10.8.4.1 [RA], 10.8.4.2 [R], 10.8.5, 10.9.2, 10.9.2.1, 10.9.2.2, 10.9.3, 11.3.3, 12.2.2, 12.2.3, 12.2.4.3 [R], 12.4.2, 15.1.3, 15.1.4

Area	ID	Control name	Risk description	Control description	Maturity Indication Level 1	Maturity Indication Level 2
					Initial Controls are only partly defined and/or executed in an inconsistent manner and rely heavily on individuals.	Repeatable Controls are in place and executed in a structured and consistent, but informal, manner.
	DM.04	Storage and retention arrangements	Absence of procedures regarding data storage, retention and archiving lead to failure to meet business objectives and non compliance with organization's security policy and regulatory requirements.	Procedures are defined and implemented for effective and efficient data storage, retention and archiving to meet business objectives, the organization's security policy and regulatory requirements.	- There are no procedures in place for data storage, retention and archiving. - Data storage is unstructured.	- Limited requirements defined for data storage techniques. - There are some informal guidelines for retention and archiving.
	DM.05	Exchange of (sensitive) data	Unauthorized access to resources (data) connected to a network or disclosure of sensitive information transmitted on a network. This could ultimately lead to theft, corruption, improper or unauthorized use of information assets.	Policies and procedures are defined and implemented to ensure that business requirements for the protection of data and software are met when data and software are exchanged within the organization or with any external entity. Sensitive transaction data is only exchanged via a trusted path or medium with controls to show authenticity of content, proof of submission, proof of receipt and non-repudiation of origin.	- There is no policy or guidelines for exchanging (sensitive) data within the organization or with an external entity. - The organization has the capability of making secure file and document transfers, but these capabilities are not consistently and widely used.	- There is an informal policy for data exchange. - The organization's secure file and document transfer mechanisms are used organization-wide.
	DM.06	Disposal	Inadequate disposal of information could lead to non compliance with regulatory requirements or unauthorized access to (confidential) information.	Procedures are defined and implemented to ensure that business requirements for protecting (sensitive) data and software are met when data and hardware are disposed of or transferred.	- Data is disposed of in an ad hoc manner. - There are no formal procedures for data removal and disposal.	- Informal procedures are implemented so equipment and media containing sensitive data are disposed via a central point in the organization. - Responsibilities for data disposal have been partly defined.
Identity & Access Management	ID.01	Access rules	Incorrect access rules and/or access groups could cause segregation of duty conflicts to have a negative impact on the business process and application performance.	The organization has defined access groups (or roles) based upon established business rules, including segregation of duties, in a SOLL authorization matrix. Procedures are in place to ensure timely initiation and update in the SOLL authorization matrices for all assets. Management authorizes changes to defined privileges for access groups (or roles).	- No policy to control access to information. - Absence of complete SOLL authorization matrix. - Not all user activities can be traced to uniquely identifiable users.	- Informal policy implemented about access to information. - A SOLL authorization matrix has been defined but not formalized. - Activities of high privilege users are traceable to uniquely identifiable users. - Defined roles and user access rights are in line with business needs. - Job requirements are attached to user identities.
	ID.02	Access rights administration	Unauthorized access to data, applications, operating systems and related resources (e.g. database tables, password tables, memory), caused by an inadequate process for assigning, monitoring, reviewing and terminating user access rights. Incorrect assignment of user access rights could lead to segregation of duty conflicts having a negative impact on business process and application performance.	Employee access rights are assigned commensurate with assigned job responsibilities (e.g. through role-based access). Administration procedures are available to define activities for requesting, issuing or closing an account and its associated user access rights. The procedure addresses the method used by senior management to appropriately authorize these activities.	- Absence of policy for user accounts and related privileges. - No administration procedure for users and access groups/roles. - Access rights are granted and revoked on an ad hoc basis, depending on individuals. - Users could access more information than based on 'need-to-know/have' principle.	- Informal policy in place on all accounts and access rights (internal, external, administrators), and all circumstances (normal, emergency). - An administration procedure for accounts and related privileges has been defined but not formalized. - Access to information is defined as a result of risk management, and complies with policy and security demands. - Accounts and related access rights are blocked/revoked if a user resigns or is fired.
	ID.03	Super users	Inadequate management of super users could lead to unauthorized access to programs and data, or disruption of IT services.	Management has controls in place which ensure that super user access is restricted to an appropriate (limited) group of individuals and that activities performed with super user accounts are monitored. Super user accounts need to be approved by responsible management.	- Policy has not been created for defining and using super user access. - No procedure is in place for the assignment of super user rights. - No defined group of individuals to which super user access is restricted	- Policy for the use of super user access, and a procedure for the assignment of super user rights, has been defined but not formalized. - Individuals authorized to assign super user rights are approved by management. - Super user activities are recorded and are analyzed in case of incidents.

Maturity Indication Level 3	Maturity Indication Level 4	Maturity Indication Level 5	References				
Defined Controls are documented and executed in a structured, formal and proven manner.	Managed and measurable Effectiveness of controls is periodically assessed and checked for quality.	Continuous improvement An eco system has been established to provide continuous and effective control, and to resolve risks.	COBIT 4.1	COBIT 5	ISO 27K 2013	DNB 2014	BIR 2012 / BIG 2015
Formal procedures and guidelines are defined for data storage, retention and archiving. Business aligned requirements for data storage, retention and archiving (techniques) are defined and implemented. It has also been ensured that requirements are in line with security policies and contractual, legal and regulatory requirements.	In addition: - Storage and retention arrangements are periodically reviewed to verify whether business objectives are still being met. - The implementation and execution of relevant procedures of data storage, retention and archiving are periodically assessed. - Data management techniques like Command Query Responsibility Segregation (CQRS, read actions are separated from the write actions) are observed or implemented.	In addition: - Data and retention arrangements are integrated into information/data lifecycle management. - Implementation and execution of the data life cycle management procedures and related costs are reviewed regularly and reported to senior management. - Data management technique like event sourcing (ES) is observed or used.	DS11.2	DSS04.08, DSS06.04	A.8.3.1, A.12.3.1, A.18.1.3	12.1	10.5.1, 10.5.1.4, 10.5.1.5, 10.7.1, 10.7.1.1 [RA], 10.7.1.2 [RA], 10.7.1.3, 10.7.1.4, 15.1.3
Policy and procedures are defined and implemented to ensure that business requirements are met for the protection and exchange of data and software. Policy and procedures are agreed by senior management and widely used. Corporate data is classified according to exposure level and classification diagram (e.g., confidential, sensitive). Data transmissions outside the organization must be encrypted prior to transmission. Review of business critical application logs, or processing stops for invalid or incomplete transactions, is in place.	In addition: - Sensitive data processing is controlled through application controls that validate the transaction prior to transmission. - Periodic review is carried out on all relevant application and system logs or processing stops for invalid or incomplete transactions. - Data exchange policy, and the operating effectiveness of the data exchange process, are assessed on a periodic basis.	In addition: - Data exchange methodology is fully supported via automated (real-time) tooling, automatic workflow processing and integrated dashboards. - Reporting about data exchange is done on a periodic basis.	DS5.11	DSS05.02	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	18.5	7.1.3.1 [RA], 10.6.1, 10.6.1.3 [RA], 10.8.2, 10.8.1, 10.8.1.1 [RA], 10.8.1.2, 10.8.1.3, 10.8.1.4, 10.8.1.5, 10.8.4, 10.8.4.1 [RA], 10.8.4.2 [RA], 10.9.1, 10.9.2, 11.4.1, 11.4.2, 11.4.3, 11.4.5, 11.4.6, 11.4.7
Formal procedures are defined and implemented to ensure that business and regulatory requirements for protecting (sensitive) data and software are met when data and hardware are disposed of or transferred. Equipment and media containing sensitive information are sanitized (as much as possible) prior reuse or disposal. Responsibility for disposal procedures has been clearly defined.	In addition: - Unsanitized equipment and media are transported in a secure manner throughout the disposal process. - Disposed equipment and media containing sensitive information have been logged to maintain an audit trail. - The implementation and execution of relevant procedures for disposing of data are periodically assessed.	In addition: - A procedure is in place to remove active media from the media inventory list upon disposal. - A procedure is in place to ensure that inventory is updated to reflect recent disposals in the log. - Data disposal is integrated into information/data lifecycle management.	DS11.4	DSS06.08	A.8.3.1, A.8.3.2, A.11.2.7	12.2	9.2.6, 9.2.6.1 [RA], 9.2.6.2 [RA], 10.7.1, 10.7.2, 10.7.2.1 [RA]
Policy and SOLL matrix for access rights/privileges of users and groups (roles) have been defined, documented, formalized, communicated and punctually updated. Identification, authentication and authorization of users implemented and enforced. Access rights derived from the SOLL matrix are frequently compared to the IST situation. Activities of users are traceable to uniquely identifiable users. User identities and access rights are maintained in a central repository.	In addition: - (Cost-effective) Technical and procedural measures for user identification, authentication and enforcement of user rights are kept current and are periodically assessed and documented. - Improvements are defined on the basis of assessments.	In addition: - The performance and improvements in the access rule administration procedure and practices are continuously monitored.	DS5.3	DSS05.04, DSS06.03	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	17.1	5.1.1, 10.1.3, 11.1.1, 11.2.3, 11.7.1.1 [RA], 11.7.2
Policy and procedures for all accounts and access rights/privileges are defined, documented, formalized and communicated. Includes approval procedure outlining the data/system owner granting access privileges. Adequate SoD in place for requesting, approving, implementing or revoking user access rights. Employee access rights are implemented through role-based access.	In addition: - Assigned employee access rights are periodically compared to job responsibilities. - Improvements are defined based on these assessments.	In addition: - Performance and improvement in managing accounts and related access rights are continuously monitored. - Tooling (e.g. provisioning) for Identity & Access Management is successfully implemented.	DS5.4	DSS05.04, DSS06.03	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	17.2	6.1.3, 6.2.1.2, 8.3.1, 8.3.3, 10.1.3, 11.2.1, 11.2.1.1, 11.2.1.2 [RA], 11.2.1.3 [RA], 11.2.2, 11.2.3, 11.3.1, 11.5.1, 11.5.2, 11.5.2.3 [RA], 11.5.3, 11.5.3.1, 11.5.3.3 [RA], 11.5.3.2 [RA], 11.5.3.4, 11.5.5, 11.5.6, 11.5.1
A formal super user procedure has been defined, documented and communicated. Individuals with super user access are defined and assignment is approved by responsible management. Activities performed with super user accounts are logged and reviewed.	In addition: - Activities performed with super user accounts are continuously monitored. - The super user procedure, and the super user access to systems, is periodically assessed.	In addition: - Based on periodic assessments, the super user procedure is reviewed and improved (as part of IAM). - Shortcomings or trends are reported to senior management.	DS5.4	DSS05.04	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	17.2	10.10.3, 10.10.4, 11.1.1, 11.2.1, 11.2.2, 11.2.4, 11.5.2, 11.2.3, 11.5.1

Area	ID	Control name	Risk description	Control description	Maturity Indication Level 1	Maturity Indication Level 2
					Initial Controls are only partly defined and/or executed in an inconsistent manner and rely heavily on individuals.	Repeatable Controls are in place and executed in a structured and consistent, but informal, manner.
	ID.04	Envelope procedure	Absence of an adequate envelop procedure could lead to unauthorized access to programs and data, or disruption of IT services.	An envelope procedure has been defined to control emergency access to accounts with super user rights and is followed by the organization.	- No envelope procedure defined. - Emergency access with super user rights is not monitored or monitored on an ad hoc basis.	- An envelope procedure has been defined but not formalized. - Individuals who are authorized to assign temporary super user rights have been defined. - Emergency actions are recorded. - Passwords are changed after every emergency access.
	ID.05	Periodic review of access rights	Unauthorized access to the operating system, data and applications (including programs, tables, and related resources) caused by inadequate access rights and monitoring of access violations. Incorrect assignment of user access rights could lead to segregation of duty conflicts having a negative impact on the business process and application performance.	Management periodically reviews user access implemented for the relevant applications (IST-situation) in order to confirm the correctness of implemented accounts and roles (the access rights), and validate that access rights are commensurate with assigned job responsibilities, as set out by the access rules (SOLL-situation). Any inappropriate access noted during the review process is revoked in a timely manner. This control involves SOLL and IST matrices being compared by responsible management.	- No defined procedure to control and manage system and application access rights. - No complete SOLL situation defined. - Ad hoc reviews by individuals.	- A procedure to control and manage system and application access rights has been defined but not formalized. - Systems, applications and data are classified by importance and risk. - Ad-hoc SOLL-IST evaluations are executed for high privileged users (including vendors, providers and business partners).
Security Management	SM.01	Security baselines	Absent or incorrect security baselines could lead to different or inconsistent implementation of security parameters, ultimately leading to unauthorized access or disruption of IT services.	Security baselines and guidelines for IT infrastructure are in place to limit the risk of unauthorized access to IT assets. Security baselines are formally defined, periodically updated and reviewed, approved by senior management, and communicated to responsible IT staff. Implemented security settings for IT assets are periodically reviewed for compliance with security baselines. Deviations from the baselines are documented and approved.	- No security baselines defined.	- Security baselines are defined for core IT infrastructure components / assets. - Security baselines are implemented on an ad-hoc basis and deviations from the baselines are not documented.
	SM.02	Authentication mechanisms	Inappropriate authentication could lead to unauthorized access to programs / data by misusing identities of authorized users, and/or not all activities of users are traceable to unique identifiable users.	All users (internal, external and temporary) and their activity on IT systems should be uniquely identifiable. Management is responsible for periodically reviewing the list of active IDs in relevant applications, in order to validate whether unique User IDs are implemented to provide individual accountability and to ensure that generic or system level IDs are locked or otherwise protected. Any inappropriate or inactive IDs noted during the review process are disabled in a timely manner.	- No policy to control user authentication. - No procedure for user ID management. - Authentication not enforced before granting access. - Not all user activities and system processes are traceable to unique identifiable users. - Ad hoc measures depend on individuals.	- Informal policy for user authentication is in place. - An administration procedure for establishing identification, authentication and authorization of users has been defined but are informal. - Authentication is enforced before granting access. - All user activities are traceable to uniquely identifiable users. - Defined roles utilized for granting access are in line with business needs and based on minimum privileges and approved by process owner. - Job requirements are attached to user identities. - System or generic user ID's are protected.
	SM.03	Mobile devices and teleworking	Lost or stolen mobile devices, eavesdropping or interception of wireless communication, unsecured personal (mobile) systems and transmission of malware could compromise business data.	Ensuring information security when using mobile devices and teleworking facilities. Mobile device management, encryption and malware protection are in place to limit the risks.	- Absence of policy for using and securing mobile devices or teleworking facilities. - Absence of procedure for requesting, approving, distributing and accepting mobile devices or teleworking facilities. - Business data possibly stored in clear text on mobile devices.	- Informal policy implemented for securing mobile devices or teleworking facilities. - Access to a mobile device is only granted after using a (strong) password. - No business data is stored on mobile devices (zero footprint), or else only encrypted data is stored on a mobile device.
	SM.04	Logging	Absence of logging and/or absence of periodic review of logging could lead to inappropriate or unusual activities not being noticed on time or failure to execute adequate follow-up actions. Log retention and access rights to logs are not in line with business or regulatory requirements.	Logging requirements are defined based on monitoring and reporting needs, and implemented in systems, databases and network components. Logs are periodically reviewed for indications of inappropriate or unusual activities, and adequate follow-up actions are defined. Log retention and access rights are in line with business requirements.	- Logging requirements are partially defined and documented. - Logging is not structured and only reviewed on an ad hoc basis, depending on individuals.	- Requirements are documented but informal. - A procedure to review logging has been defined but not formalized. - Logging is implemented on relevant IT components and periodically reviewed. - Actions performed by administrators and operators are also logged and periodically reviewed. - Internal system clocks are synchronized. - Log retention periods and access rights are in place.

Maturity Indication Level 3	Maturity Indication Level 4	Maturity Indication Level 5	References				
Defined Controls are documented and executed in a structured, formal and proven manner.	Managed and measurable Effectiveness of controls is periodically assessed and checked for quality.	Continuous improvement An eco system has been established to provide continuous and effective control, and to resolve risks.	COBIT 4.1	COBIT 5	ISO 27K 2013	DNB 2014	BIR 2012 / BIG 2015
A formal envelope procedure has been defined, documented and communicated. Use of the envelope procedure is logged. Use of the envelope procedure is reviewed, along with executed emergency actions with super user rights and changes to envelope passwords.	In addition: - Implementation and execution of the envelope procedure is periodically assessed.	In addition: - Automated Privileged Access Management (PAM) tooling is implemented. - Based on periodic assessments, the envelope procedure and implementation thereof is reviewed and improved. - Shortcomings and trends are reported to senior management.	DSS.4	DSS05.04	A.9.2.3	17.2	11.2.2
Procedures for controlling and managing access rights and SOLL-IST evaluations have been defined, documented and formalized. For all users, SOLL and IST matrices are periodically compared, reviewed and signed off by management. Inappropriate access is revoked.	In addition: - The procedures for controlling and managing access rights and SOLL-IST evaluations are periodically assessed.	In addition: - Based on periodic assessments, the procedures for controlling and managing access rights and SOLL-IST evaluations are reviewed and improved (as part of IAM). - Shortcomings and trends are automatically reported to senior management (and if applicable access rights are automatically deactivated in accordance with reported exceptions).	DSS.4	DSS05.04	A.5.1.2, A.9.2.5	17.2	5.1.2, 11.2.4
Security baselines are defined, approved by senior management and communicated to responsible IT staff. Implemented security settings for IT assets are periodically reviewed for compliance with security baselines. Outcomes are documented and deviations from the baselines are also documented and approved.	In addition: - Mandatory implementation of security baselines for new IT infrastructure components is enforced by system and project management processes. - Security baselines are periodically reviewed and updated (if necessary). - The level of compliance with baselines is periodically reported to senior management.	In addition: - Compliance monitoring for security baselines is done via continuous monitoring / auditing tooling. - Exceptions to baselines are reported in real-time.	DSS.5	APO01.04, DSS05.07, MEA03.02	A.6.1.5, A.18.2.2	1.1, 3.2	15.2.1
Policy and procedure for user authentication and user ID management are defined, documented, formalized and communicated. Includes approval procedure outlining the data/ system owner who grants access privileges. Access provision and authentication controls for all users (internal, external) are utilized for logical access to all systems and resources. Adequate SoD in place for requesting, approving, implementing or revoking user access rights. User identities and access rights are maintained in a central repository. Inappropriate or inactive user ID's rights are timely disabled. Dual factor authentication is enforced for untrusted environments or critical systems.	In addition: - Implementation and execution of relevant procedures are periodically assessed and documented. Improvements are defined based on assessments.	In addition: - Performance and improvement of user ID management, authentication mechanisms and controls are continuously monitored.	DSS.3	DSS05.04, DSS08.02	A.9.4.1, A.11.2.9, A.13.1.1, A.13.1.2, A.14.1.1	17.1	10.8.1, 10.8.2, 11.6.1, 11.6.1.2 [R,A], 11.6.1.3 [R,A], 11.6.1.4 [R,A], 12.1.1
Formalized policy and procedures for securing mobile devices and/or teleworking facilities are documented and communicated (mobile device management). Anti-malware software on mobile devices is kept up-to-date. In case of loss or theft, communication with centralized applications is shut off. No business data is stored on teleworking facilities at home or elsewhere (zero footprint). The trusted (logical) workplace is protected from malware. Business data in untrusted environments only printed after a risk assessment.	In addition: - The implementation and execution of mobile device management is periodically assessed and documented. Improvements are defined on the basis of assessments.	In addition: - Performance and improvements in secure mobile devices and teleworking facilities are continuously monitored.		DSS01.04, DSS05.03, DSS06.06	A.6.2.1, A.6.2.2	16.1	11.7.1, 11.7.1.1 [R,A], 11.7.1.2 [R,A], 11.7.1.3 [R,A], 11.7.2, 11.7.2.1, 11.7.2.2 [R], Supplement BIG: 10.4.1.6, 11.7.2.3 [A]
Logging requirements are formalized; a procedure and working practices for maintaining, storing and reviewing logging are documented, formalized and based upon risk assessments. The procedure is aligned with business requirements. Logging of unusual activities and malfunction of logging itself is documented, analyzed and met by follow-up actions.	In addition: - The implementation and execution of relevant procedures and practices are periodically assessed and documented. Improvements are defined based on assessments.	In addition: - Automated detection and response technology, e.g. SIEM, is fully implemented. - Performance and improvement of the logging procedure and practices are continuously monitored.	DSS.5	DSS05.04, DSS06.07	A.12.4.1, A.12.4.2, A.12.4.3	16.1	10.10.1, 10.10.1.1, 10.10.1.2 [R,A], 10.10.1.3 [R,A], 10.10.1.4 [R,A], 10.10.1.5, 10.10.2, 10.10.2.1, 10.10.3, 10.10.3.1, 10.10.3.2 [R,A], 10.10.3.3, 10.10.3.4, 10.10.3.5 [R,A], 10.10.3.6, 10.10.4, 10.10.5

Area	ID	Control name	Risk description	Control description	Maturity Indication Level 1	Maturity Indication Level 2
					Initial Controls are only partly defined and/or executed in an inconsistent manner and rely heavily on individuals.	Repeatable Controls are in place and executed in a structured and consistent, but informal, manner.
	SM.05	Security testing, surveillance and monitoring	Absence of security testing, surveillance and monitoring may lead to unusual and/or abnormal activities not being detected and/or addressed in a timely manner. Not maintaining the enterprise security baseline may lead to unsecured implementation of IT components.	Implementation of IT security is tested and monitored in a proactive way. IT security should be recredited in a timely manner to ensure that the organization's approved information security baseline is maintained. A logging and monitoring function will enable early prevention and/or detection and subsequent timely reporting of unusual and/or abnormal activities which may need to be addressed.	- IT security implementation is tested in an ad hoc manner. - Absence of procedures or policy.	- There is a procedure with guidelines for testing the security measures, but mainly focuses on unit or component testing. - Surveillance of unusual or abnormal activities is done by checking the logs afterwards.
	SM.06	Patch management	Absence of patches or security fixes could cause known vulnerabilities to be misused to gain unauthorized access to the IT infrastructure.	Available patches and/or security fixes are installed in compliance with set and approved policies (including those for operating systems, databases and installed applications) and recommendations of CERT and/or suppliers.	- No patch management policy defined. - Individual risk analysis for vulnerabilities and patches. - Ad hoc installation of patches and/or security fixes.	- Informal policy defined. - Risks of vulnerabilities and installation of patches/fixes are managed but not documented. - Patches are often implemented with little regard for information security.
	SM.07	Threat and vulnerability management	Less understanding about who will attack the organization, how the organization will be attacked and what vulnerabilities and attack paths can be exploited to reach critical assets, increases the risk of a damaging breach being encountered.	A threat and vulnerability management process is implemented to identify threats and timely detect and remedy vulnerabilities that may lead to a degradation in performance of, or an attack on, an enterprise resource. The number of attack vectors is also in scope, thus reducing the overall exposure.	- A vulnerability management process is non-existent. - Absence of automated vulnerability assessment (VA) solution. - Almost everything is done manually system by system.	- A basic and informal threat and vulnerability management process is being implemented. - A vulnerability scanner is in place, ideally covering both web and network vectors in addition to scanning for device misconfigurations. - Scanning is done on ad hoc basis.
	SM.08	Infrastructure resource protection and availability	Business disruptions due to insecure handover of changes into production infrastructure, system and routine maintenance. Due to lack of internal control, security and auditability measures, (sensitive) IT infrastructure is exposed to a decrease in integrity and availability.	Internal control, security and auditability measures are implemented during the configuration, integration and maintenance of hardware and infrastructure software to protect resources and ensure availability and integrity. Responsibilities for using sensitive infrastructure components are clearly defined and understood by those who develop and integrate infrastructure components. Their use is monitored and evaluated.	- No process defined for infrastructure resource protection and availability. - Although there awareness about the importance of IT infrastructure, there is no consistent overall approach. - There is no separate test environment for IT infrastructure.	- Infrastructure resource protection and availability is supported by some (formal) practices and the importance of IT infrastructure is understood. - For some environments, there is a separate test environment for IT infrastructure.
	SM.09	Infrastructure maintenance	Business disruptions due to insecure handover of changes in the production infrastructure, system and routine maintenance.	A strategy and plan for infrastructure maintenance has been developed, and ensures that changes are controlled in line with the organization's change management procedure. Include periodic reviews against business needs, patch management, upgrade strategies, risks, vulnerability assessment and security requirements.	- No process defined for infrastructure maintenance. - Changes to infrastructure for new applications are made without a formal strategy or overall plan. - Maintenance is done on the basis of incidents and/or short-term needs.	- An informal process for infrastructure maintenance is implemented. - Maintenance of IT infrastructure is not based on any defined strategy and does not consider the needs of supported business applications. - Some maintenance activities are scheduled and/or coordinated. - Documentation for critical system software is maintained.

Maturity Indication Level 3	Maturity Indication Level 4	Maturity Indication Level 5	References				
			COBIT 4.1	COBIT 5	ISO 27K 2013	DNB 2014	BIR 2012 / BIG 2016
Defined Controls are documented and executed in a structured, formal and proven manner. Policy and related procedures for scanning, testing and monitoring IT security are defined and implemented. Both are approved by senior management. There are security baselines which are implemented for all business critical IT components utilized by the organization. A logging and monitoring function is implemented for early prevention and/or detection and subsequent timely reporting of unusual and/or abnormal activities. Special attention is given to cyber security threats.	Managed and measurable Effectiveness of controls is periodically assessed and checked for quality. In addition: - An inventory has been created for all IT components, network devices, services and applications and each component has been assigned a security risk rating and is scanned or tested accordingly. - All business critical IT components are (automatically) recorded in CMDB and monitored in real-time for security events in alignment with business needs.	Continuous improvement An ecosystem has been established to provide continuous and effective control, and to resolve risks. In addition: - IT security testing has been integrated into the organization's project management and software development methodologies to ensure that security is considered in development, design and testing requirements, to minimize the risk of new or existing systems introducing security vulnerabilities. - Information or cyber security threats are constantly monitored by automated detection and response technology, e.g. SIEM.	DSS.5	DSS05.04, DSS05.07	A.12.4.1, A.12.4.2, A.12.4.3, A.12.7.1, A.12.8.1, A.12.6.2, A.14.2.8, A.16.1.3, A.16.1.4, A.16.2.1, A.16.2.3	16.1	6.1.8, 10.10.1, 10.10.1.1, 10.10.1.2 [R,A], 10.10.1.3 [R,A], 10.10.1.4 [R,A], 10.10.1.5, 10.10.2, 10.10.3, 10.10.3.1, 10.10.3.2 [R,A], 10.10.3.3, 10.10.3.4, 10.10.3.5 [R,A], 10.10.3.6, 10.10.4, 10.10.5, 12.6.1, 13.1.2, 15.2.2, 16.3.1
Formal documented patch management policy defined. Organization-wide patch management is implemented, documented and aligned to change management. Patching is done basically and in cooperation with CERT. IT personnel perform manual checks on the patch levels of OS, databases and applications.	In addition: - The effectiveness of patch management is frequently assessed. Assessments are documented and improvement measures are defined. - Patch management is more likely to be driven by risks and moves away from being compliance-driven.	In addition: - Automatic checks on patch levels and alerts to IT personnel are in place (but no automatic installation of patches). - Reports are automatically generated for senior management.	A13.3, A16.1, DSS.9	BAI03.10, DSS05.01	A.12.6.1, A.12.6.2	16.2	9.1.2.7, 12.6.1, 12.6.1.1, 12.6.1.2, 12.6.1.3, 12.6.1.4 [R,A] Supplement BIG: 12.6.1.5
A formalized threat and vulnerability management process (including cooperation with CERT) is implemented and driven by regulatory compliance and known risks. A vulnerability assessment solution is solidly in place to feed scans, most likely from multiple types of scanners from several vendors.	- Threat and vulnerability management (and patching) is implemented as a complete ecosystem rather than separate entities. - A more advanced and thorough process is implemented with penetration testing being used for vulnerability validation. - Implementation of red team concept for formal penetration testing. - Periodic reporting for vulnerability management process is in place.	- The IT security and IT operations departments implement processes to jointly manage the lifecycle of vulnerabilities. - The established process is the key to establishing closed-loop vulnerability management, from threat identification to remediation and validation. - Data for vulnerability management is integrated into all other aspects of IT security and IT operations to enable near real time adjustment of security controls, and network and data center management. - Metrics focus on improving security instead of only reporting identified vulnerabilities.		DSS05.01, DSS05.02, DSS05.07	A.12.2.1, A.12.6.1	18.2, 20.1	10.4.1, 10.4.2, 12.6.1
A clear, defined and generally understood process for the protection and availability of IT infrastructure is in place. The process description is aligned with business requirements and approved by (senior) management. Responsibilities for using sensitive infrastructure components are clearly defined and understood by those who develop and integrate infrastructure components. Tests include functionality, security, availability and integrity condition, and any other vendor recommendations. There are separate IT infrastructure environments for test and production. All application software is tested prior to installation in an environment separate from, but sufficiently similar to, production. Installations of appropriately licensed software are in accordance with vendor guidelines.	In addition: - Maintenance activities on sensitive IT infrastructure components are logged and regularly reviewed by responsible senior staff member. - All infrastructure data and software are backed up prior to installation and/or maintenance tasks. - The implementation and execution of relevant procedures and practices are periodically assessed and documented.	In addition: - The protection and availability process for infrastructure is proactive and closely aligned with overall business security and availability measures (and requirements). - The infrastructure components are constantly monitored by automated detection and response technology, e.g. SIEM, as an integral part of the infrastructure.	A13.2, DSS.7	BAI03.03, DSS02.03, DSS05.05	A.14.1.1, A.17.2.1	18.1	12.1.1, 12.1.1.1, 12.1.1.2, 12.1.1.3, 12.1.1.4, 12.1.1.5 Supplement BIG: 12.1.1.6
A clear, defined and generally understood process for maintaining IT infrastructure is in place. The process description is aligned with change management and approved by (senior) management. The process supports the needs of critical business applications and is aligned with IT and business strategy, and is consistently applied. Maintenance is planned, scheduled and coordinated. Documentation for system software is maintained, kept up-to-date and is periodically updated with vendor documentation for all systems.	In addition: - The maintenance process for technology infrastructure is applied consistently for all IT components and is focused on reusability. - The process is well organized and proactive. - The IT infrastructure adequately supports the business applications. - The effectiveness of the infrastructure maintenance procedures is periodically assessed.	In addition: - The maintenance process for technology infrastructure is proactive and closely aligned with critical business applications and the technology architecture. - Periodic reviews are conducted against business needs, patch management, upgrade strategies, risks, vulnerabilities assessment and security requirements. - Good practices regarding technology solutions are followed, and the organization is aware of the latest platform developments and management tools. - Costs are reduced by rationalizing and standardizing infrastructure components and by using automation.	A13.3	BAI03.10	6.1, A.11.1.5, A.11.2.4, A.12.6.1, A.14.2.3, A.14.3.1, A.17.2.1	18.2	9.1.5, 9.2.4, 12.4.2, 12.5.2, 12.6.1

Area	ID	Control name	Risk description	Control description	Maturity Indication Level 1	Maturity Indication Level 2
					Initial Controls are only partly defined and/or executed in an inconsistent manner and rely heavily on individuals.	Repeatable Controls are in place and executed in a structured and consistent, but informal, manner.
	SM.10	Cryptographic key management	Protection for the confidentiality, authenticity or integrity of information fails due to inadequate cryptographic techniques. This could ultimately lead to theft, corruption, improper or unauthorized use of information assets.	Policies and procedures are in place to organize the generation, change, revocation, destruction, distribution, certification, storage, entry, use and archiving of cryptographic keys to protect keys against modification and unauthorized disclosure.	- No policy and procedure for key lifecycle management. - No information classification scheme available.	- Policy and procedure for key lifecycle management and information classification scheme are defined but not formalized.
	SM.11	Network security	Unauthorized access to resources connected to a network or disclosure of sensitive information transmitted on a network. This could ultimately lead to theft, corruption, improper or unauthorized use of information assets.	Security techniques and related management procedures (e.g., firewalls, security appliances, network segmentation and intrusion detection) are used to authorize access and control information flows from and to networks. Available best practices in this area (i.e. GovCert, ISO/IEC, ITSec) are considered.	- No network security policy in place. - No procedure or guidelines. - Ad hoc risk analysis and use of measures by individuals.	- Network security policy is defined, but informal. - Procedures for implementing network security are defined and executed but not formalized. - Best practices are used but not on a structured basis.
	SM.12	Manage malware attacks	Integrity of information systems (and data) can be compromised and damaged by unauthorized alterations by unauthorized users if inadequate measures are in place regarding malicious software and the use of up to date security patches. This could ultimately lead to theft, corruption, improper or unauthorized use of information assets.	Preventive, detective and corrective measures are in place (especially up-to-date security patches and virus control) across the organization to protect information systems and technology from malware (e.g., viruses, worms, spyware, spam).	- No policy for preventing malicious software. - No (full) automatic prevention software in place. - No (full) up-to-date virus definitions.	- Malicious software prevention policy is defined, but informal. - Virus protection, alert and corrective software is used. - Virus definitions are up-to-date. - Most incoming e-mail is filtered for malware.
	SM.13	Protection of security technology	Confidentiality of security documentation is compromised when information and information systems are available to unauthorized users and can be used for unauthorized purposes. Integrity of information systems can be compromised and damaged by unauthorized alterations by unauthorized users if inadequate measures are in place. This could ultimately lead to theft, corruption, improper or unauthorized use of information assets.	Security-related technology has been made resistant to tampering, and security documentation is not disclosed unnecessarily.	- No special measures are taken to protect security related technology. - There is no difference in storing regular documentation and security-related documentation.	- Policies and procedures have been established to address security breach consequences (specifically to address controls for configuration management, application access, data security and physical security requirements).

Maturity Indication Level 3	Maturity Indication Level 4	Maturity Indication Level 5	References				
			COBIT 4.1	COBIT 5	ISO 27K 2013	DNB 2014	BIR 2012 / BIG 2015
Defined Controls are documented and executed in a structured, formal and proven manner. Formal documented policy and procedure for key lifecycle management and information classification scheme has been defined. Information labeling according to the classification scheme. Protective controls implemented for information which covers need to share and protect information. Confidentiality and integrity of private keys is enforced.	Managed and measurable Effectiveness of controls is periodically assessed and checked for quality. In addition: - The effectiveness of cryptographic key management procedures is periodically assessed.	Continuous improvement An eco system has been established to provide continuous and effective control, and to resolve risks. In addition: - Based on the periodic assessments, the cryptographic key management procedures are reviewed and improved. Any shortcomings are reported to senior management.	DSS.8	DSS05.02, DSS05.03	A.10.1.1, A.10.1.2, A.13.2.3, A.18.1.5	18.3	10.8.4, 10.8.4.1 [R.A], 10.8.4.2 [R.A], 12.2.3, 12.3.1, 12.3.1.1, 12.3.1.2, 12.3.1.3 [R.A], 12.3.2, 12.3.2.1, 12.3.2.2, 12.3.2.3, 12.3.2.4, 12.3.2.5 [R.A], 15.1.6
Network security policy is defined and implemented: procedures, guidelines and documentation for administrating critical network components are established and updated. Security techniques are in place for the authorization of access, control of information flows and different security zones. Appropriate encryption is used when sensitive data is transported over untrusted networks.	In addition: - The actuality and execution of relevant procedures are periodically assessed and documented. - Improvements are defined based on these assessments.	In addition: - Based on the periodic assessments, procedures are reviewed and improved. Any shortcomings are reported to senior management.	DSS.10	DSS05.02	A.13.1.1, A.13.1.2, A.13.1.3	18.4	10.6.1, 10.6.1.1, 10.6.1.2 [R.A], 10.6.1.3 [R.A], 10.6.1.4, 10.6.2, 11.4.5, 11.4.5.1 [R.A], 11.4.5.2 [R.A], 11.4.5.3 [R.A], 11.4.5.4 [R.A], 11.4.5.5, 11.4.6, 11.4.7
A formal software prevention policy is defined, documented and communicated. Key staff members are aware of their responsibility to comply with policy. Automated virus protection, alert and corrective controls are in place and formalized. Centrally distributed protection software (version and patches) has up-to-date virus definitions. All (inbound and outbound) e-mail is filtered against unsolicited information and malware. Controls are in place to limit the spread of malware.	In addition: - The distribution process, regular evaluation of new threats and e-mail filtering are reviewed for effectiveness.	In addition: - Periodic assessments are used to review and improve the management of malware attacks. Any shortcomings are reported to senior management.	DSS.9	DSS05.01	A.9.1.2, A.12.2.1, A.13.1.1, A.13.1.2, A.13.1.3	19.1	10.4.1, 10.4.1.1 [R.A], 10.4.1.2 [R.A], 10.4.1.3, 10.4.1.4 [R.A], 10.4.1.5, 10.4.2, 10.4.2.1, 10.4.2.2, 10.6.1, 10.6.1.1, 10.6.1.2 [R.A], 10.6.1.3 [R.A], 10.6.1.4, 10.6.2, 11.4.1, 11.4.5, 11.4.5.1 [R.A], 11.4.5.2 [R.A], 11.4.5.3 [R.A], 11.4.5.4 [R.A], 11.4.5.5, Supplement BIG, 10.4.1.6
In addition: Security design features facilitate password rules (e.g., maximum length, characters, expiration and reuse). Access is authorized and appropriately approved.	In addition: - There are control records granting and approving access and logging unsuccessful attempts, lockouts, authorized access to sensitive files and/or data, and physical access to facilities.	In addition: - Security reports generated from system tools are used to prevent network penetration vulnerability attacks. - The controls are part of annual management reviews on security features for physical and logical access to files and data.	DSS.7	DSS05.05	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.11.2.6, 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	20.1	9.1.6, 9.2.1, 9.2.3, 10.7.4, 10.7.4.1, 10.7.4.2 [R.A], 10.8.2, 10.10.1, 10.10.2, 10.10.3, 10.10.4, 10.10.5, 10.10.6, 11.3.2, 11.3.3, 11.4.3, 11.4.4, 11.5.1, 11.5.4, 11.5.5, 11.5.6, 11.7.1, 11.7.2, 12.4.1, 12.6.1, 13.1.2, 13.2.3, 13.2.4

Area	ID	Control name	Risk description	Control description	Maturity Indication Level 1	Maturity Indication Level 2
					Initial Controls are only partly defined and/or executed in an inconsistent manner and rely heavily on individuals.	Repeatable Controls are in place and executed in a structured and consistent, but informal, manner.
Physical Security	PH.01	Physical security measures	Security measures at physical sites (for IT equipment) are not in line with business requirements. Unauthorized physical access can jeopardize the integrity and availability of IT components.	For workplaces, the organization has defined and implemented physical security measures in line with business requirements to ensure that access to information systems is appropriately restricted and is capable of effectively preventing, detecting and mitigating risks relating to theft, temperature, fire, smoke water vibration, terror, vandalism, power outages, chemicals or explosives. Access to premises, buildings and areas should be justified, authorized, logged and monitored. This applies to all persons entering the premises, including staff, temporary staff, clients, vendors, visitors or any other third party.	- No identifiable physical security policies or controls are in place. - The organization is not able to quickly detect the theft of, or attacks on, buildings and physical assets. - The management of facilities and equipment is dependent upon the skills and abilities of key individuals.	- Some physical security policy and framework elements are in place, but these may not be comprehensive and are not consistently followed; non-compliance is not identified. - Physical security is an informal process, but standards are not consistently applied across the organization.
	PH.02	Physical access rights management	Procedures are not defined and implemented to grant, limit and revoke access to premises, buildings and areas according to business needs, including emergencies. Access to premises, buildings and areas cannot be justified, authorized, logged or monitored.	Procedures are defined and followed to grant, limit and revoke access to IT-critical areas or data centers (e.g. premises, buildings and rooms) according to business needs, including emergency access. Adequate security measures (e.g., lock on door, card-key access system, cipher lock, etc.) are used to restrict physical access to computer facilities that house relevant applications.	- No procedures are defined for physical access administration. - Personnel is able to move within the premises without restriction. - Other procedures regarding management and protection of physical IT assets are not or concisely defined.	- Informal procedures are implemented to grant, limit and revoke access to specific areas in buildings. - Physical security objectives are not based on formal standards nor aligned with business (security) objectives. - Facility maintenance procedures are not well documented and mostly rely upon good practices of a few individuals.
Computer Operations	OP.01	Job processing	IT production (e.g. programs, jobs) is not executed as planned and deviations from scheduled processing are not identified and resolved in a timely manner.	The organization has procedures in place for automated job scheduling. Job operations are monitored and include: - the use of interfaces between relevant systems to confirm that data transmissions are complete, accurate and valid. - results of the backup job to confirm success Failures are recorded and resolved via the incident management procedure. The ability to modify job schedules, batch jobs and automated interfaces is restricted to authorized individuals.	- No procedures defined for job processing.	- Several runbooks for production jobs are available and generally describe jobs and interfaces for the most relevant systems. - Job processing is implemented locally (per department) and correlation across several systems is not in place. - Anomalies in (back-up) job scheduling are not centrally registered (via incident management).
	OP.02	Backup and recovery procedures	Loss of data supporting (financial) information in case of system outage or integrity issue due to inaccurate, incomplete, not timely back-up of critical data and monitoring thereof.	The organization has implemented a strategy for regularly backing up relevant data and programs. Backup and recovery procedures are formally defined and implemented for all in-scope systems. The backup schedule and retention requirements are in line with the risks accepted by the business for data loss and based on the criticality of the system and the cost of manual recovery. Periodic testing for restore procedures is executed and documented.	- No procedures defined for back up and recovery.	- Procedures for backup and restoration of systems, applications, data and documentation have been defined. - The backup schedule and retention requirements are not (fully) aligned with business requirements.
	OP.03	Capacity and performance management	Performance and capacity is not properly and timely managed leading to business disruptions when maximum capacity or minimum performance is reached.	The organization has procedures implemented to ensure that the performance and capacity of IT services and the IT infrastructure is able to deliver the agreed service level targets in a cost effective and timely manner. Performance and capacity management considers all resources required to deliver the IT service, and plans for short, medium and long term business requirements, including forecasting future needs based on workload, storage and contingency requirements.	- Capacity and performance management is not implemented.	- A process (and technology) has been defined and implemented to provide relatively simplistic tracking and manual reporting of "raw performance metrics" at (virtual) server level. - Reporting is manual and on an ad-hoc basis (mostly incident driven).

Maturity Indication Level 3	Maturity Indication Level 4	Maturity Indication Level 5	References				
			COBIT 4.1	COBIT 5	ISO 27K 2013	DNB 2014	BIR 2012 / BIG 2015
Defined Controls are documented and executed in a structured, formal and proven manner. A comprehensive risk-based physical security policy is documented, communicated, and supported by (access) systems for protecting and supporting people (temporary staff, clients, vendors, visitors or any other third party), and for incident response and reporting. The policy is approved by senior management. Effective measures are in place to prevent, detect and impede threats on, or the unauthorized access to premises, building and removal of physical assets. Physical security and safety measures are in line with business needs and are actively considered from the early stage of any premises relocation, refurbishment or construction; corresponding zone and control design and certification requirements are complied with. Responsibility and ownership are clearly addressed.	Managed and measurable Effectiveness of controls is periodically assessed and checked for quality. In addition: - The physical security policy addresses the safety and security of personnel and assets when offsite. The policy also prescribes that management monitors the effectiveness of controls and compliance with established standards and that the recoverability of premises and computing resources is incorporated into the risk management process. - Applicable standards are defined for all facilities, covering site selection, construction, guarding, personnel safety, mechanical and electrical systems, and protection against environmental factors (e.g., fire, lighting, flooding). - Compliance with the policy is assessed (by the 2nd line of defense) on an ad-hoc basis.	Continuous improvement An eco system has been established to provide continuous and effective control, and to resolve risks. In addition: - Based on the policy there is an agreed-upon, long-term plan for the facilities required to support the organization's premises and computing environment. - All facilities are inventoried and classified according to the organization's ongoing risk management process. - Compliance with the security policy is periodically reported to senior management. - The policy is yearly reviewed, updated and reapproved by senior management.	DS12.2	DSS01.04, DSS01.05, DSS06.05, DSS06.06	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	21.1	9.1.1, 9.1.1.1, 9.1.1.2, 9.1.1.3, 9.1.1.4 [A], 9.1.1.5 [R], 9.1.1.8 [A], 9.1.2, 9.1.3, 9.1.3.1, 9.1.3.2 [R,A], 9.1.3.3 [R,A], 9.1.4, 9.1.4.1, 9.1.4.2, 9.1.4.3 [R,A], 9.1.4.4 [R,A], 9.1.4.5, 9.1.4.6 [R,A], 9.2.1, 9.2.2, 9.2.3, 9.2.5, 9.2.7 Supplement BIG:
Formalized procedures are implemented for physical access administration. Perimeter security measures and access restrictions are applied to only authorized personnel is allowed to access buildings, IT-critical areas or data centers. Access to IT areas (server rooms, buildings, areas or zones) is based on job function and responsibilities. Employees are instructed to display visible identification. Visitors are logged and escorted. Procedures are in place to ensure that access profiles remain up-to-date. A process is implemented to log and monitor all entry points to IT sites, while registering all visitors, including contractors and vendors. Responsibility and ownership are clearly assigned and communicated.	In addition: - Access (violation) is strictly controlled and monitored periodically. - Standardized control mechanisms are in place for addressing environmental and safety factors regarding physical security. - Management reviews the accuracy of authorizations and compliance with applicable standards. - Management has established objectives and metrics for measuring the management of IT areas. - The operational effectiveness of physical security procedures is assessed on an ad-hoc basis.	In addition: - Access controls are monitored continuously. - The environment is monitored and controlled through specialized equipment, and equipment rooms have become 'unmanned'. - Preventive maintenance programs enforce strict adherence to schedules, and regular tests are performed for sensitive equipment. - Facility strategy and standards are aligned with IT service availability targets and integrated into business continuity planning and crisis management. - Management reviews and optimizes physical security facilities using objectives and metrics on a continual basis.	DS12.3	DSS06.05, DSS06.06	A.11.1.2, A.11.1.5, A.11.1.6, A.11.2.1, A.11.2.6	21.2	9.1.2.1, 9.1.2.2 [R,A], 9.1.2.3, 9.1.2.4, 9.1.2.5, 9.1.2.8, 9.1.2.7, 9.1.2.8 [R,A], 9.1.3, 9.1.5, 9.1.5.1, 9.1.5.2, 9.1.5.3, 9.1.6, 9.1.6.1 [R,A], 9.2.1, 9.2.4, 9.2.4.1 [R,A], 9.2.5
A runbook for job scheduling is available and is aligned with business objectives (agreed upon by system or process owner). The runbook contains detailed information and instructions. Job processing and interface monitoring are implemented centrally and are centrally managed including correlation across several systems. Exceptions or anomalies in job processing are registered via the incident management process.	In addition: - Reporting for job processing is part of service level reporting. - The operational effectiveness of the job processing process is assessed on a periodic basis.	In addition: - Dedicated tooling is used to automate job processing and follow-up of related anomalies (e.g. automatic restart) depending on criticality of jobs.	DS13.1, DS13.2	DSS01.01, DSS01.03	A.12.1.1		10.1.1
There is adequate policy and procedures for the backup of systems, applications, data and documentation, and consider business-related factors as well as security requirements. Policy and procedures are aligned with business needs and approved by (senior) management. Responsibilities have been clearly assigned for making, restoring and monitoring backups. The priority for data recovery has been based on business requirements and IT service continuity procedures.	In addition: - Critical data that affects business operations is periodically identified using the risk management model and IT service continuity plan. - Sufficient restoration tests have been periodically performed to ensure that all components of backups can be effectively and punctually restored. - The operational effectiveness of backup and recovery procedures is assessed on a periodic basis.	In addition: - Performance of the backup and recovery process is periodically reported to (senior) management and, if necessary, improvements are addressed. - The procedures are an integral part of the organization's disaster recovery planning. - Systems, applications, data and documentation maintained or processed by third parties are adequately backed up or otherwise secured. - The return of backups from third parties should be required and escrow or deposit arrangements considered.	DS11.5	DSS04.08	A.12.3.1	11.4	10.5.1
A process (and technologies) has been defined and implemented to provide comprehensive tracking and fully automated reporting for 'raw performance metrics' at (virtual) server or partition level. Automated generation of periodic reports based on metrics is done across most of the infrastructure. Periodic reports make it possible to spot trends or problems and give limited insight into future needs.	- A process (and technologies) is in place for fully automated tracking, analysis and reporting of metrics which closely relate to business services. - In addition to system and application workload data, additional performance and capacity metrics are factored which more closely relate to business or service metrics (e.g. configuration, costing, response times, transaction rates, etc.). - Automated generation of exception-oriented analysis and reports is done on a periodic basis. - Forecasting of future needs is based on periodic reporting. - Operational effectiveness of the performance and capacity management process is assessed periodically.	In addition: - Predictive analytics on key elements of the infrastructure and application landscape is in place and executed in a structured manner to support performance and capacity planning.	DS3.1, DS3.2, DS3.3, DS3.4, DS3.5	BAI04.01, BAI04.02, BAI04.03, BAI04.04, BAI04.05	A.12.1.3, A.17.2.1		10.3.1, 10.3.1.1 [R,A], 10.3.1.2 [R,A], 10.3.1.3 [R,A]

Area	ID	Control name	Risk description	Control description	Maturity Indication Level 1	Maturity Indication Level 2
					Initial Controls are only partly defined and/or executed in an inconsistent manner and rely heavily on individuals.	Repeatable Controls are in place and executed in a structured and consistent, but informal, manner.
Business Continuity Management	BC.01	Business continuity planning	Absence of risk-related understanding about potential business impact and requirements for resilience, alternative processing and recovery of all critical IT services. This could ultimately lead to a major disruption in key business functions.	Business and IT continuity plans are developed based on the framework and designed to reduce the impact of a major disruption on key business functions and processes. The plans are based on risk-related understanding about potential business impacts and address requirements concerning resilience, alternative processing and recovery capability in all critical IT services. The plans also cover usage guidelines, roles and responsibilities, procedures, communication processes and the testing method.	- No business-aligned IT continuity plan has been defined. - The IT organization has a limited and general recovery plan for its network and IT systems.	- IT (and eventually business) continuity plans are developed based on a informal (and concise) framework. These plans are incomplete and partly based on risk-related understanding about potential business impacts. - In case of a major interruption, the concerned key processes and systems could probably be recovered, but disaster recovery activities are likely to be insufficient. - If critical programs/data are lost and/or key personnel leave, some key business processes may be non-functional for extended periods of time.
	BC.02	Testing of Disaster recovery	Business disruptions due to inadequate IT continuity planning and testing thereof (including crisis management, roles and responsibilities, procedures, communication processes).	Business and IT continuity plans are tested on a regular basis to ensure that business critical systems and services can be effectively recovered, shortcomings are addressed and the plan remains relevant. This requires careful preparation, documentation, reporting of test results and, depending on the results, implementation of an action plan. The extent of testing recovery in single applications ranges from integrated testing scenarios to end-to-end testing and integrated vendor testing.	- Testing of IT continuity plans is not performed or is done on ad hoc basis. - There is a siloed test approach for some critical applications and some simple recovery testing for infrastructure components.	- The IT continuity plan is tested on a regular basis (once a year). - Limited consolidation of individual recovery test methods for critical applications. Most of the time, testing is done via isolated testing on individual applications and underlying infrastructure.
	BC.03	Off site backup storage	Critical media is not stored offsite, leading to backup data being unavailable in case of a disaster at the data center. Critical media backups are not tested periodically, possibly meaning that data cannot be restored due to data being incompatible with current software and hardware systems and configuration.	All critical backup media, documentation and other IT resources needed for IT recovery and business continuity plans are stored offsite. The content of backup storage is determined after collaboration between business process owners and IT personnel. Management at the offsite storage facility acts on the basis of data classification policy and the enterprise's media storage practices. IT management ensures that offsite arrangements are periodically assessed, at least annually, for content, environmental protection and security. Compatibility of hardware and software for restoring archived data is ensured, and archived data is periodically tested and refreshed.	- Backup tapes are not, or only partly, stored offsite. - No additional measures are taken to prevent data loss in case of a disaster at the primary data center.	- The organization has made an concise inventory for critical media which has to be stored offsite. - The content of backup storage is determined after collaboration between business process owners and IT personnel. - Controls are in place to ensure the offsite backup storage of critical media.
	BC.04	Data replication	Absence of or incorrectly configured data replication could mean that critical financial and/or operational data will not be (timely) available in case of incidents.	Data replication has been set up between the organization's production facility and its disaster recovery facility to help ensure that critical financial and operational data is available on short notice. Replication status is monitored as part of the system jobs monitoring process.	- The organization has no means of data replication.	- In case of incidents, data replication is safeguarded by restoring (externally stored) backups. - The organization accepts data loss for the time between last data back-up and moment when the incident occurred.
	BC.05	Crisis management	Inadequate crisis management could lead to inadequate responses to calamities, ultimately leading to loss of business.	The organization needs to have a crisis management capability to respond to accidents promptly, thoroughly and in a coordinated manner to mitigate impact and restore services in a timely fashion.	- Crisis management plans or procedures have not been defined.	- A process for crisis management has been defined, but only partially implemented. - A crisis management team has been appointed but responsibilities, tasks and required actions are informal and ad hoc.
Supply Chain Management	SC.01	Service level agreement	Agreed upon service levels do not meet business objectives or regulatory requirements.	IT services provided to the entity are defined in the SLA. Measures have been taken to ensure that services meet the organization's current and future needs.	- A service level agreement (SLA) has not been defined.	- Some agreements regarding service levels have been defined. - No agreements made about periodic reporting of delivered services.
	SC.02	Service level management	Lack of management and monitoring for service delivery, which means deviations in the performance of service providers are not detected on time. Trends in performance statistics for individual and overall services are not identified and acted upon, which can lead to a decrease in overall business performance.	Business requirements, and the way in which IT-enabled services and service levels support business processes, are periodically analyzed. Services and service levels are discussed and agreed with the business, and compared with the current service portfolio to identify new or changed services or service level options.	- Absence of service level management process.	- A process for service level management has been defined, but control and reporting about service levels is not formalized and/or implemented organization-wide.

Maturity Indication Level 3	Maturity Indication Level 4	Maturity Indication Level 5	References				
Defined Controls are documented and executed in a structured, formal and proven manner.	Managed and measurable Effectiveness of controls is periodically assessed and checked for quality.	Continuous improvement An eco system has been established to provide continuous and effective control, and to resolve risks.	COBIT 4.1	COBIT 5	ISO 27K 2013	DNB 2014	BIR 2012 / BIG 2015
Business and IT continuity plans are defined and approved by senior management. The organization has conducted a business impact analysis which defines recovery-time objectives and has fully documented IT disaster-recovery and business-continuity plans to meet these objectives. The plans cover usage guidelines, roles and responsibilities, procedures, crisis management and communication processes and the testing method. As a result, the organization would most likely be able to continue operations following a major disruption at any site.	In addition: - The continuity plans contain a rotating schedule of tabletop and live tests from its business continuity and crisis management plans, which include improvements based on the results of previous tests. - Shortcomings encountered when performing continuity plans are reported.	In addition: - Business continuity plans and related processes are periodically reviewed. Shortcomings in (the effectiveness or efficiency) of continuity plans, as well as (the follow-up of) improvement actions, are reported to senior management.	DS4.1, DS4.2	DSS04.01, DSS04.02, DSS04.03	A.6.1.3, A.6.1.4, A.17.1.1, A.17.1.2	11.1	6.1.6, 6.1.6.1 [R.A], 6.1.7, 14.1.1, 14.1.2, 14.1.3, 14.1.4
Business and IT continuity plans are tested via approved integrated test/recovery scenarios. Business and IT continuity plans are tested on a regular basis (at least once a year) to ensure that business critical systems can be effectively recovered, shortcomings are addressed and the plan remains up-to-date. Proven preparation, documentation, reporting of test results and, depending on the results, implementation of an action plan are in place.	- Integrated business continuity tests are performed for the complete business critical application and infrastructure landscape, i.e. a full fail-over test including the recovery of business specific activities and workplaces. - Proven recovery tools are in place for all applications, and infrastructure components, applications and services for all tiers are accommodated. - There is successful multi-level testing for applications and infrastructure components. - Business and IT continuity test plans are reviewed on an ad-hoc basis.	In addition: - The organization routinely passes its BC/DR tests without major shortcomings/exceptions because its procedures and capabilities have been refined over several years. - Periodic reports for "tested" effectiveness of continuity plans are sent to senior management.	DS4.4, DS4.5	DSS04.02, DSS04.04, DSS04.05, DSS04.06	17.1.3	11.2	14.1.5, 14.1.5.1 [R.A]
There is a detailed overview of all critical media which has to be stored off-site. The overview is approved by senior management. Clear descriptions of necessary data storage controls are given to management regarding the offsite storing facility, including transport, recovery instructions, labeling and inventory lists of backup media. Offsite arrangements are in line with the business continuity requirements and are periodically assessed.	In addition: - Management at the offsite storage facility act based on data classification policy and the enterprise's media storage practices. - IT management ensures that offsite arrangements are periodically assessed for content, environmental protection and security. - Backup data is regularly tested and restored to ensure the quality of data. - Compatibility of hardware and software to restore archived data is periodically tested.	In addition: - The offsite arrangements are subject to constant improvement. - Mirroring of critical media by means of cloud solutions are in place where real-time backups of critical media are required (see also data replication).	DS4.9	DSS04.07	A.12.3.1	11.3	10.5.1
A data replication process is implemented between the organization's production facility and its disaster recovery facility. The organization has a clear insight into critical financial and operational data which must be replicated, and is agreed upon by senior management. The data is available on a short notice in case of incidents (meeting the business requirements).	In addition: - The replication status is monitored as part of the system jobs monitoring process. - The quality of data replication is (partially) tested at least every year.	In addition: - Automated partial data replication tests are performed weekly. - A full restore of replicated data is an integral part of yearly disaster and recovery tests.	DS11.1	DSS01.01, DSS04.07	A.17.2.1	11.4	
An crisis management plan has been defined and is part of the Business Continuity Plan (BCP). The BCP allows the organization to recover critical business operations, and for the crisis management team to deal with the crisis at hand. Responsibilities during the crisis are clear for all parties involved. Exercises for crisis management teams are conducted periodically.	In addition: - Specific recovery scenarios are defined where each recovery scenario requires a specific media plan and notification plan. - An overall crisis management test is conducted to validate the overall process, including disaster declaration and escalation procedures.	In addition: - Improvement actions are identified and followed up based on conducted crisis management team exercises. - Results and improvement actions are reported to senior management.		DSS04.03, DSS04.04, DSS04.06	A.17.1.1, A.17.1.2	11.1	14.1.1, 14.1.2, 14.1.3, 14.1.4
Service levels regarding IT enabled services are derived from business requirements. SLA contains agreements regarding periodic reporting of service delivery and service performance. The defined service levels are documented in an SLA, and are formally agreed by (senior) management and IT service provider.	In addition: - Specific agreements regarding information security are defined in the SLA. - Agreements for the discontinuation of services (e.g. exit clause, escrow, data hand over and/or destruction of data) are part of the SLA or master agreement.	In addition: - "Security incident" criteria has been defined and checked to measure security incidents separately from incidents related to failures.	DS1.3, DS1.5	APO09.04, APO09.05	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	14.1	6.2.3, 6.2.1, 6.2.1.5 [R.A], 6.2.1.6, 10.2.1, 10.2.1.1, 10.2.1.2, 10.2.2, 10.2.3, 12.5.5, 10.8.2 Supplement B1G: 6.2.1.7
A service level management process has been defined, implemented and agreed by (senior) management. On a periodic basis, the performance of agreed services is reported in a service level report (SLR) and, if necessary, discussed with the service provider.	In addition: - Formal requirements for service components are periodically compared to the actual performance of delivered service components, and action is taken against non-compliance with formal SLA levels/requirements. - Operational effectiveness of the service level management process is assessed at least once a year. If applicable, improvements are addressed and followed up.	In addition: - Evolving business requirements are (re)assessed against the current service portfolio to identify the need for new or changed services or service level options.	DS1.5, DS1.6	APO09.05, APO09.06	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	14.1	6.2.3, 10.2.1, 10.2.2, 10.2.2.1, 10.2.2.3, 10.2.3, 12.5.5

Area	ID	Control name	Risk description	Control description	Maturity Indication Level 1	Maturity Indication Level 2
					Initial Controls are only partly defined and/or executed in an inconsistent manner and rely heavily on individuals.	Repeatable Controls are in place and executed in a structured and consistent, but informal, manner.
	SC.03	Supplier risk management	Lack of risk oversight to consider non-disclosure agreements (NDAs), deposit contracts, enduring provider's viability, compliance with security expectations, alternative providers, conventional fees and bonuses. Also lack of legal oversight to ensure contracts are established in accordance with organization requirements or legal regulatory requirements.	Risks are continuously identified and mitigated relating to suppliers' ability to continue effective service delivery in a secure and efficient manner. Contracts comply with universal business standards in accordance with legal and regulatory requirements. Risk management considers non-disclosure agreements (NDAs), escrow contracts, continued supplier viability, conformance with security requirements, alternative suppliers, penalties and rewards, etc.	- A supplier risk management process is not in place. - Contractual agreements and/or SLA's are signed without conducting a proper risk assessment on the third party (service).	- A process for managing risks regarding suppliers has been defined, but only partly implemented. - In terms of cloud computing, a checklist is used to quickly assess the cloud service provider. - Identified risks are rarely documented and/or reported.
	SC.04	Internal control at third parties	The IT control environment and framework of third parties does not meet organizational objectives. Third party service providers do not comply with legal and regulatory requirements and contractual obligations.	The status of external service providers' internal controls is assessed. Procedures are in place to ensure that external service providers comply with legal and regulatory requirements and contractual obligations.	- Internal controls for third parties are not assessed.	- Few procedures have been defined to ensure that adequate internal controls are implemented by third parties.

Maturity Indication Level 3	Maturity Indication Level 4	Maturity Indication Level 5	References				
			COBIT 4.1	COBIT 5	ISO 27K 2013	DNB 2014	BIR 2012 / BIG 2015
Defined Controls are documented and executed in a structured, formal and proven manner. Risks are continuously identified and mitigated relating to suppliers' ability to continue effective cloud service delivery in a secure manner. The supplier risk management process considers non-disclosure agreements (NDAs), escrow contracts, continued supplier viability, conformance with security requirements, alternative suppliers, penalties and rewards, etc. Non-mitigated or accepted risks are reported to senior management on a periodic basis. Contracts comply with universal business standards in accordance with legal and regulatory requirements (e.g. data privacy). Assurance, showing service delivery complies with legal and regulatory requirements, as well as own (security) policies, is obtained before contractual agreements are signed.	Managed and measurable Effectiveness of controls is periodically assessed and checked for quality. In addition: - Operational effectiveness of the supplier risk management process is assessed yearly. If applicable, improvements are addressed and followed up. - Periodic assessments on internal controls (including security measures) at the third party and/or cloud service provider are part of the supplier risk management process.	Continuous improvement An eco system has been established to provide continuous and effective control, and to resolve risks. In addition: - Risks are continuously identified and mitigated relating to suppliers' ability to continue effective service delivery in an efficient manner.	DS2.3	APO10.04	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	14.2	6.2.1, 6.2.1.1, 6.2.1.2, 6.2.1.3 (R.A), 6.2.1.4, 6.2.3, 8.1.2, 8.1.3, 10.2.3, 10.4.1, 10.4.2, 10.8.2
A formal process is implemented to ensure that adequate internal controls are operating effectively. The statuses of external service providers' internal controls are periodically assessed. Procedures are in place to ensure that external service providers comply with contractual obligations.	In addition: - Procedures are in place to ensure that external service providers comply with legal and regulatory requirements (e.g. data privacy). - Furthermore, third party assurance is provided by an external auditor (e.g. ISAE3402).	In addition: - Automated tooling (portal) and/or extended service level reporting offers the organization a monthly insight into the maturity of internal controls at third parties.	ME2.6	MEA02.01	8.1, A.15.1.2, A.15.2.1, A.18.2.2	16.3	6.2.1.5, 6.2.3, 10.2.2, 15.2.1

Koninklijke Nederlandse
Beroepsorganisatie
van Accountants



Antonio Vivaldistraat 2 - 8
1083 HP Amsterdam
Postbus 7984
1008 AD Amsterdam

T 020 301 03 01
E nba@nba.nl
I www.nba.nl