Confidentieel

Onderwerp: Toelichting op Toetsingskader Informatiebeveiliging 2014

1. INLEIDING

Sinds 2010 onderzoekt DNB de kwaliteit van informatiebeveiliging als thema binnen de financiële sector. Onderdeel van dit thema zijn periodieke self assessments, die bij banken, verzekeraars en pensioenfondsen worden uitgezet. Voor deze self assessment is in 2010 het Toetsingskader Informatiebeveiliging opgesteld dat bestaat uit 54 COBIT controls. Door DNB is gesteld dat deze controls in het kader van beheerste bedrijfsvoering allen een volwassenheidsniveau van minimaal "3" dienen te hebben (de controls dienen aantoonbaar werkend te zijn).

Naar aanleiding van reacties uit de sector en de toenemende dreiging van cybercrime is het Toetsingskader op twee onderdelen aangepast. Ten eerste is het kader geactualiseerd, met als doel de volwassenheidsniveau's te verduidelijken. Ten tweede verwacht DNB dat drie controls in de categorie "Assess and manage (IT) risks" op een hoger minimaal volwassenheidsniveau ("4") worden gebracht. Het doel hiervan is de weerbaarheid van de financiële sector tegen de continu veranderende cybercrime dreigingen verder te versterken.

1.1 **Verduidelijking en toelichting**

De belangrijkste aanpassingen ter verduidelijking van het Toetsingskader zijn:
- Een nadere toelichting op de definities van de volwassenheidsniveau's (de interpretatie van de criteria door DNB is niet veranderd), zie hoofdstuk 2.1,
- Een uitbreiding van de 'Points to consider' (aandachtspunten) voor het scoren van de controls zie hoofdstuk 2.2,
- Een opsplitsing van in twee documenten: de vragenlijst en de 'Points to consider'.

1.2 **Hoger minimaal volwassenheidsniveau**

De drie controls die minimaal op een volwassenheidsniveau "4" gebracht moeten worden (hoofdstuk 3), zijn:
4.1: IT risk management framework,
4.2: Risk assessment,
4.3: Maintenance and monitoring of a risk action plan.
Ten opzichte van niveau "3" houdt dit in dat deze controls periodiek aantoonbaar geëvalueerd worden.

1.3 **Planning/fasering**

DNB verwacht dat de drie controls in de categorie "Assess and manage (IT) risks" voor 1 juni 2015 op volwassenheidsniveau "4" functioneren. Als onderdeel hiervan verwacht DNB dat de instellingen voor 1 juni 2015 zelf bepaald hebben voor welke andere controls zij op basis van de (IT) risk assessments een hoger volwassenheidsniveau dan "3" noodzakelijk achten. Voor het op een hoger niveau brengen van deze andere controls dient een verbeterplan beschikbaar te zijn waarin is onderbouwd op welk moment de desbetreffende controls op niveau "4" zullen zijn

gebracht. De overige beheersmaatregelen binnen het Toetsingskader moeten nog steeds een volwassenheidsniveau van minimaal "3" behouden.

DNB zal bovenstaande gefaseerd en risico gebaseerd toetsen bij een selectie van instellingen. Deze zullen via een brief hiervan op de hoogte worden gesteld. In de brief zal ondermeer verzocht worden om het Toetsingskader in te vullen en binnen twee maanden terug te sturen.

2. AANPASSINGEN TOETSINGSKADER

2.1 **Definities volwassenheidsniveau's**

Het accent van de aanpassing ligt op het verduidelijken van de tot nu toe gehanteerde definities van de volwassenheidsniveau's. De interpretatie van de criteria door DNB is niet veranderd. Voor het volwassenheidsniveau "3" geldt nog steeds dat hier sprake moet zijn van een aantoonbare opzet, bestaan en werking van de betreffende control.

De definities van volwassenheidsniveau's wil DNB zo dicht mogelijk bij Cobit 4.1[1] laten aansluiten. Dat is ook de reden dat de Engelse terminologie gebruik wordt.

In onderstaande tabel staat in de tweede kolom de definitie zoals die in het Toetsingskader uit 2010 is opgenomen, in de derde kolom staan de aangepaste definities en in de vierde kolom zijn criteria opgenomen ter verdere verduidelijking van het volwassenheidsniveau. De belangrijkste tekstuele wijzigingen zijn in *italics* weergegeven.

Aanpassingen:

	Was (2010):	**Wordt (2014):**	
Lvl	Control is:	Control is:	Criteria:
0	**Non-existent** - No documentation. There is no awareness or attention for certain control.	**Non-existent** - No documentation. There is no awareness or attention for certain control.	
1	**Ad-hoc, initial** - Control is (partly) defined, but performed in an inconsistent way. The way of execution is depending on individuals.	***Initial/ad hoc*** - Control is (partly) defined, but performed in an inconsistent way. The way of execution is depending on individuals.	
2	**Repeatable, informal** - Control is defined and executed in a structured and consistent, but informal way.	**Repeatable *but intuitive*** - Control is in place and executed in a structured and consistent, but informal way.	The control execution is based on an informal, unwritten though standard practice.

[1] Binnen Cobit 4.1 worden echter op verschillende plaatsen verschillende definities gehanteerd. DNB gaat uit van de definities zoals opgenomen in "Cobit 4.1 Research, 2007, Appendix III—Maturity Model for Internal Control, page 175"

3	**Structured and formalized** - Control is documented, executed *organization wide* in a structured and formalized way. Execution of control can be proved.	***Defined*** **-** Control is documented, executed in a structured and formalized way. Execution of control can be proved.	* Formal control is available for any critical process. * Critical processes and controls are identified based on risk assessments. * There is evidence of implementation of the control * Formal "test of design effectiveness" constitutes evidence for level 3. * Formal "test of operating effectiveness" constitutes evidence for level 3. *The test of operating effectiveness should be done over an appropriate period which fits the risk profile.
4	**Implemented and periodically assessed** - Control is executed in a structured and formalized way *organizational wide*. The *efficiency* and effectiveness of the control is also assessed and improved when necessary.	***Managed and measurable*** **-** The effectiveness of the control is periodically assessed and improved when necessary. *This assessment is documented.*	Criteria for level 3 plus the following: * The periodic evaluation of the control is documented, including any identified action for improvement. *The frequency of the periodic evaluation should be based on the risk profile. * The frequency of this assessment should be at least annually.
5	-	***Optimised*** *- An enterprisewide risk and control programme provides continuous and effective control and risk issues resolution. Internal control and risk management are integrated with enterprise practices, supported with automated real-time monitoring with full accountability for control monitoring, risk management and compliance enforcement. Control evaluation is continuous, based on self-assessments and gap and root cause analyses. Employees are proactively involved in control improvements.*	Distinguishing criteria are: * Continuous improvement. * Comparing control performance with market data of other enterprises. * Advanced IT-support as workflow processing and integration.

Generic remarks:

- For all controls, management may vary control and process implementation across the organization based on the situational risk profile and business context including local requirements by law and regulators. Processes (business and IT) are not equally critical in every situation. The need to demonstrate the required maturity level pertains only to key financial processes and assets and to essential supporting processes.
- Based on a risk assessment management may choose to differentiate control objectives and strictness of control measures.
- Control objectives are aimed to define WHAT has to be managed on a mature level. The 'Point to consider' are provided to give guidance. Financial institutions should determine HOW they implement procedures and measures to achieve the objectives stated in the assessment framework.

2.2 **Indeling van het Toetsingskader**

Het aangepaste Toetsingskader Informatiebeveiliging is opgesplitst in twee documenten:

- Document 1 (getiteld 'Questionnaire') bevat de 54 COBIT controls die beoordeeld moeten worden door de instelling. In het document is de omschrijving van de control en de mapping naar Cobit V5 en ISO27000 vermeld. Dit document moet door de instelling weer teruggestuurd worden aan DNB.
- Document 2 (getiteld 'Points to consider') bevat de 'Points to consider' voor alle controls en is bedoeld als 'guidance' voor de instelling. Deze 'Points to consider' zijn ten opzichte van de vorige versie van het Toetsingskader uitgebreid met elementen uit:
    - SANS Top 20 Critical Security Controls for Effective Cyber Defense (www.sans.org)
    - ISO 27032:2012 Guidelines for Cyber Security (www.iso.org)

3. SELECTIE CONTROLS VOOR MINIMUM LEVEL "4"

3.1 **Inleiding**

De toegenomen cybercrime dreigingen zoals "Advanced Persistent Threats" (APT's) onderstrepen het belang van een effectieve informatiebeveiliging en continue monitoring van deze dreigingen. Dit wordt breed binnen de financiële sector onderkend. Vanuit (IT) risicomanagement wordt dit geadresseerd. Een belangrijk onderdeel hiervan zijn de (IT) risk assessments die de basis vormen voor het treffen van de controls (beheersmaatregelen) en het minimum niveau van deze controls.

DNB benadrukt dat de instelling zelf verantwoordelijk zijn om een adequaat (IT) risicomanagement in te richten. In perspectief van het Toetsingskader Informatiebeveiliging heeft DNB dit vertaald naar het verhogen van het verwachte volwassenheidsniveau van de drie controls in de categorie "Assess and manage (IT) risks" naar het volwassenheidsniveau "4". Dit betreft de controls:

4.1 IT Risk Management Framework;
4.2 Risk Assessment;
4.4 Maintenance and monitoring of a risk action plan.

DNB beoogt hiermee de risicobeheersing voor actuele dreigingen ondermeer op gebied van cybercrime door de instellingen zelf te versterken.