Toezichthouder: De Nederlandsche Bank (DNB)				
Vitaal proces:		**Sector:**		**Grondslag:**
• Betalings- en effectenverkeer		Financiële sector		NIB / eIDAS
Risicogebaseerde aanpak	**Organisatie van netwerk- en informatiebeveiligings-beheer**	**Incidenten voorkomen**	**Detectie & response**	**Art. 1:24 Wet Financieel Toezicht (Wft) NIB / Wbni**
Operationele en IT risico's	Operationele en IT risico's	Operationele en IT risico's	Operationele en IT risico's	Operationele en IT risico's
Aanleiding:	Cyberrisico's staan hoog op de agenda van de belangrijkste instellingen voor de vitale processen betalings- en effectenverkeer (samen de financiële kerninfrastructuur FKI), en DNB. Vanuit DNB wordt toezicht gehouden op de manier waarop deze risico's door de FKI beheerst worden. Dit toezicht wordt onder meer uitgevoerd door middel van gestructureerde vragenlijsten, onderzoeken, inspecties, en gesprekken om voortgang van bevindingen uit onderzoeken te monitoren en om nieuwe risico's te identificeren. Tevens worden door DNB Threat Intelligence Based Ethical Red Teaming (TIBER) testen gecoördineerd. Daarnaast bestaat er een beeld van de cyber beheersing bij instellingen via gestructureerde vragenlijsten over IT risico's die jaarlijks door instellingen worden ingevuld. DNB voert tevens zelfstandig, alsmede ten behoeve van het Single Supervisory Mechanism (SSM) van de ECB, inspecties uit bij onder toezicht staande instellingen. Voor de periode 2022-2024 heeft de ECB een werkprogramma vastgesteld voor het toezicht op IT risico's waarin DNB sterk betrokken is. Cyber security krijgt hierin een hoge prioriteit. Tevens coördineert DNB cyber resilience surveys die door de ECB uitgezet zijn bij Europese Financial Market Infrastructures voor wat betreft de Nederlandse instellingen.			
Status onderzoek:	Surveys en questionnaires worden elk jaar opgevraagd bij instellingen. De informatie hieruit wordt ingezet voor risico gebaseerd toezicht en kan tevens een aanleiding vormen voor gerichte onderzoeken of inspecties die doorlopend van aard zijn.			
Algemeen beeld:	Uit de uitgevoerde onderzoeken zijn een drietal hoofdthema's naar voren gekomen. **1. Risicomanagement gericht op informatiebeveiliging behoeft verbetering.** De risicomanagementcyclus gericht op informatiebeveiliging kan doorgaans verbeterd worden omdat: I) zij geen onderdeel uitmaakt van het overkoepelende risicomanagement raamwerk van de instelling, II) de gebruikte scenario analyses niet langer aansluiten op het snel veranderende dreigingsbeeld, en III) de effectiviteit van de mitigerende maatregelen moeilijk meetbaar is. Een positieve connotatie hierbij is dat cyberrisico's steeds vaker als belangrijk risico worden onderkend op bestuursniveau van financiële instellingen. **2. Beheersen van informatiebeveiliging in ketens vereist meer aandacht.** Instellingen moeten aantoonbaar controleren, monitoren en meten in hoeverre dienstverleners en onderaannemers hun afspraken nakomen op het gebied van informatiebeveiliging, cybersecurity en business continuïteit. Gebleken is dat niet alle instellingen de juiste risicomanagementprocessen hebben ingeregeld rondom hun dienstverleners. Daarnaast is vastgesteld dat het bij de onderzochte instellingen soms ontbreekt aan een volledig inzicht in de beheersmaatregelen bij dienstverleners en eventuele onderaannemers die zijn betrokken in de uitbestedingsketen. Deze waarnemingen kunnen cyberrisico's opleveren voor instellingen, immers door uitbesteding worden instellingen blootgesteld aan het aanvalsoppervlak van de dienstverlener. Steeds vaker blijkt dat gerichte cyberaanvallen op organisaties en bedrijven starten bij een dienstverlener van de financiële instelling. **3. De weerbaarheid tegen cyberaanvallen moet worden versterkt.** Enerzijds zien we verbeteringen onder andere door goede processen en procedures maar anderzijds zijn er nog veel risico's op het gebied van cyber hygiëne zoals I) volwassenheid van vulnerability & patch management, II) beheersing van End-Of-Life systemen, en cyber resilience: III) testen op basis van een risico analyse om zwakheden op te sporen. Ten aanzien van vulnerability & patch management is inzicht in mogelijke kwetsbaarheden in IT-systemen, en de risico inschatting van deze kwetsbaarheden, een proces dat meer aandacht verdient. In veel gevallen is hierbij sprake van het niet hebben van een goed overzicht van de belangrijkste IT-middelen (IT-assets) of een goed inzicht in de mogelijke (cyber)kwetsbaarheden daarvan. Een connotatie hierbij is dat wanneer er kwetsbaarheden naar buiten komen met een zeer hoog risicoprofiel, zoals bij de Log4J kwetsbaarheid, instellingen weliswaar zeer snel reageerden maar het tegelijkertijd complex was om vast te stellen hoe kwetsbaar zij waren als gevolg van onduidelijkheid rondom de aanwezigheid van Log4J in actieve IT-assets.			

Toezichthouder: De Nederlandsche Bank (DNB)	
	Ten aanzien van het testen is het voor instellingen van belang om periodiek de cyberweerbaarheid te testen op basis van een risicoanalyse en actuele cyberdreigingen met als doel zwakheden op te sporen en de mogelijke impact inzichtelijk te maken. Het TIBER-NL programma van DNB dat al enkele jaren in samenwerking met de financiële sector deze testen faciliteert is hier een voorbeeld van. Tenslotte blijft response en recovery een blijvend aandachtsgebied voor de financiële sector in het kader van weerbaarheid tegen cyberaanvallen. Reguliere business continuity en recovery plannen die zijn opgezet om zeer snel te kunnen herstellen van scenario's zoals stroomuitval of brand zullen door instellingen wellicht uitgebreid moet worden om effectief te kunnen zijn bij grootscheepse cyberaanvallen zoals een ransomware aanval.
Interventie:	De uitkomsten van surveys en questionaires worden o.a. gebruikt om aanvullende toezichtinstrumenten zoals gerichte inspecties en onderzoeken in te zetten. Bevindingen van een onderzoek of inspectie worden in een rapport aan het bestuur van een instelling gecommuniceerd. Voor de opvolging van bevindingen wordt van instellingen verwacht een plan met acties en daaraan gekoppelde tijdslijnen te overleggen. De opvolging van een dergelijk actieplan wordt gemonitord middels voortgangsgesprekken via regulier toezicht.
Relatie met andere toezichthouder:	DNB werkt in de uitvoering van haar toezicht actief samen met de Europese Centrale Bank (ECB), nationale toezichthouders in Europa inzake het toezicht op financiële instellingen, alsmede met de Autoriteit Financiële Markten (AFM).