Tom van der Ven en Hans Koster aan het woord

Normenkader auditverplichting PSD2

11 maart 2020

Wandena Birdja-Punwasi en Leon Dirks

September 2019 publiceerde NOREA, samen met de Betaalvereniging Nederland (een brancheorganisatie voor gereguleerde aanbieders van betaaldiensten in Nederland) en de Nederlandse Vereniging van Banken (NVB), een normenkader voor de audit van PSD2. Het document verscheen onder de titel 'Practical guidance for Internal Auditors on the annual audit of PSD2 related to strong customer authentication and common and secure communication'. Uit een poll van NOREA bleek een grote behoefte van RE's aan een gedeeld en breed gedragen normenkader binnen de community van betrokkenen bij het betalingsverkeer. Een goede aanleiding voor een gesprek met Hans Koster (ABN AMRO) en Tom van der Ven (Volksbank).

Roep om een aanpak

Hans: *'Uit contacten tussen diverse deelnemers van de werkgroep IT Auditing van de NvB en de Kennisgroep Betalingsverkeer van NOREA bleek behoefte aan een aanpak voor auditverplichtingen rond PSD2. De PSD2-wetgeving is in september 2019 ingegaan en riep in de voorafgaande periode veel vragen op. Het normenkader is vervolgens ontwikkeld in een samenwerkingsverband van de vier grootbanken (ABN Amro, ING, Rabobank en Volksbank), de Betaalvereniging, de NVB en de kennisgroep Betalingsverkeer van NOREA. Daarbij heeft iedereen zijn rol goed gespeeld. Zo was men bij de Betaalvereniging vooral goed op de hoogte van de concepten, en deden de grootbanken vanuit behoefte aan een normenkader of guidance proactief mee. De NVB was de initiator en NOREA vervulde de rol van facilitator tussen alle partijen.'*

Tom: *'Directe aanleiding was de invoering van PSD2 in september 2019. Het risico voor de Nederlandse banken was dat ze niet op tijd klaar zouden zijn met de implementatie van de benodigde API voor PSD2. Dan zouden ze een dure tussenoplossing moeten ontwikkelen in de vorm van screenscraping. De interne auditdiensten (IAD's) van de banken moesten daarbij wel verklaren dat hun bank op tijd klaar zou zijn met de API en dat deze oplossing aan de eisen voldeed.'*

Dit was een ingewikkeld uitgangspunt, zo geven Tom en Hans aan. Voor de IAD's was het daarbij zaak om zo snel mogelijk een normenkader voor PSD2 te ontwikkelen. Dus zijn de grootbanken aan de slag gegaan om in overleg de aanpak te bespreken en kennis te delen. Hans en Tom hebben namens deze banken de lead genomen. Tijdens dit proces kwamen ze aardig wat uitdagingen tegen. Zo was de regelgeving niet zo duidelijk, waardoor nadere interpretaties nodig waren. De werkgroep heeft dit in nauw overleg met alle betrokken partijen gedaan om tot een aanpak te komen waarmee iedereen mee uit de voeten kon: zowel auditors van grootbanken als die van kleinbanken. Verder hebben alle betrokken partijen verschillende belangen – de kunst was dan ook om deze op één lijn te krijgen. Daarnaast vragen zowel de *exemption audit* als reguliere audit om een auditaanpak. Het zou nog niet zo eenvoudig zijn om de twee te integreren. Daarom heeft de werkgroep een praktische keuze gemaakt en als doel gesteld zich in eerste instantie op de exemption audit te richten. Er moet nog worden doorgepakt om voor heel PSD2 een auditaanpak neer te zetten.

Gestart op initiatief van ABN Amro

Tom en Hans vertellen. De vier grootbanken zijn op initiatief van ABN Amro in juni 2019 bij elkaar gekomen. De gedachte was dat alle banken toen klaar waren met de aanpassingen van IT-systemen en IT-infrastructuur voor PSD2. Doel van de bijeenkomst was om niet alleen kennis over maar ook interpretaties van PSD2 te delen – de regelgeving over PSD2 was door onduidelijkheden op verschillende manieren te interpreteren. Onder leiding van Hans en Tom gebeurde deze kennisdeling in vier sessies tijdens de zomer van 2019. Resultaat was de huidige eerste versie van het normenkader (zie de link in het intro), dat vooral gericht is op *strong customer authentication*. Dit is een van de deelgebieden waarop de European Banking Authority (EBA) technische standaarden heeft vastgesteld. Om als bruikbaar startpunt voor de uitvoering van PSD2-audits bij de banken te zijn, moest het normenkader gebaseerd zijn op best practices en zich richten op alle bankprocessen. Ook zou elke bank, net als bij de AVG, op elk gewenst moment over PSD2 aan de toezichthouder moeten kunnen rapporteren.

Op Agile-wijze gewerkt

De werkwijze van de werkgroep is gebaseerd op Agile. De eerste versie van het normenkader is te zien als het eerste *minimum viable product* (MVP1). Net als bij Agile zitten er ook nog op te pakken activiteiten in de backlog. Zo komen er naast het normenkader voor strong customer authentication ook nog normenkaders voor de overige EBA-richtlijnen voor PSD2. Ook wordt het normenkader aangepast aan de tweede versie technische standaarden voor customer authentication. En, na de ervaringen met het normenkader in 2020, wordt de feedback daarover verwerkt. Eind 2020 volgt

een evaluatie van het proces en de inhoud van deze versie van het kader. Spannend voor de werkgroep is nog welke vragen de ECB daadwerkelijk zal stellen. Het normenkader helpt bij het beantwoorden van de vragen van de toezichthouder. Elke bank moet de auditresultaten beschikbaar kunnen stellen aan de ECB, als die erom vraagt. Daarbij geeft het normenkader de banken een stramien om de ECB te laten wat je aan PSD2 op het gebied van betalingsverkeer hebt gedaan.

Status van het normenkader

Tom en Hans lichten toe dat de conceptversie ter consultatie is aangeboden aan een aantal partijen. Van verschillende partijen hebben ze nuttig commentaar ontvangen. Bijvoorbeeld van de Vaktechnische commissie van Norea, van de Betaalvereniging en van NVB, en ook van een individuele auditors.

DNB heeft alleen kennisgenomen en staat er positief in: 'fijn, dat het er is'. Begrijpelijk, want natuurlijk heeft DNB er zelf ook baat bij dat er enige consistentie in aanpak binnen de sector is. Formeel hebben ze niet inhoudelijk gereageerd, maar enkele medewerkers hebben dit op persoonlijke titel wel gedaan.

Afdronk tot dusver

De bank-community gaf positieve feedback, vooral in de zin van: 'goed dat jullie hiermee bezig zijn!' Ook ontving de werkgroep tal van inhoudelijke opmerkingen en aanvullingen. Hans en Tom denken dat het normenkader generiek genoeg is om voor alle partijen toepasbaar te zijn. Nu moet het nog wel echt gebruikt worden in het audit-kalenderjaar 2020. Pas daarna kan de werkgroep het geheel weer verder finetunen. Voor de verplichte jaarlijkse auditverklaring is dit normenkader te gebruiken als handvat: het dekt je hele betalingsverkeer af, niet alleen een specifiek onderdeel. Wel moet elke IAD keuzes maken wat wanneer te doen.

De wetgeving van PSD2 is een hele puzzel geweest: de EBA guidance en alle richtlijnen, dat is alles bij elkaar 'nogal een brei!'. Het heeft het tweetal behoorlijk wat inspanning gekost voordat ze de wetgeving in alle finesses begrepen. Het zijn uiteindelijk toch wel sterk juridische richtlijnen, en ze hebben zich dan ook flink moeten verdiepen in de wetteksten.

Impact van het PSD2-normenkader en PSD2 zelf

PSD2 heeft consequenties voor het gehele betaalproces. Daarom heeft de implementatie van het PSD2-normenkader in 2020 gevolgen voor het auditplan en de werkzaamheden bij beide banken. Het normenkader richt zich namelijk onder meer op de set van key controls om op te kunnen steunen. Naar verwachting worden de eerste PSD2-audits in het derde kwartaal van 2020 al afgerond. Daarna is het zaak de PSD2-audits mee te nemen in het auditjaarplan van 2020. De EBA geeft daar harde normen voor.

Verdere ambities

De werkgroep gaat de commentaren verwerken, en voor het beheer van het normenkader wordt een structurele oplossing gezocht. Nog belangrijker voor Tom en Hans is dat ze de samenwerking als zeer inspirerend hebben ervaren – alle betrokkenen hebben out of the box moeten denken, en dat is ze goed bevallen. Deze inspiratie willen ze vasthouden en op de een of andere manier een vervolg geven. Hans en Tom vinden dat binnen de Audit Community het gezamenlijk ontwikkeling vaker zou moeten gebeuren. Kortom, ze zijn dus nog lang niet klaar. To be continued….

W. (Wandena) Birdja-Punwasi RE RC CISA | zelfstandig gevestigd IT-auditor bij *Acsis Consultancy*

Wandena is reeds vijfentwinig jaar werkzaam in het Internal (IT) Audit vakgebied. Zij voert haar werkzaamheden met veel passie uit bij organisaties in de financial- en healthcare-sector.

Drs. L. G. (Leon) Dirks RE | Coördinerend IT-auditmanager bij Auditdienst Rijk

Als coördinerend IT-auditmanager bij de ADR (Auditdienst Rijk, onderdeel van het ministerie van Financiën) is Leon verantwoordelijk voor het organiseren dan wel leiden van de IT-audits die de ADR doet voor de jaarrekeningcontrole van het ministerie van Justitie en Veiligheid. Daarnaast is hij lid van de Norea-kennisgroep Betalingsverkeer. Eerder was hij werkzaam in diverse functies bij de Europeesche Verzekeringen en de Westland Utrecht Hypotheekbank.