Rol van de IT-auditor

Online dienstverleningsrichtlijnen AFM financiële sector

11 maart 2020

Jean-Jacques Bistervels

Dit artikel gaat in op de rol die de IT-auditor kan vervullen bij het beoordelen van de implementatie van de online dienstverleningsrichtlijn die de Autoriteit Financiële Markten (AFM) in haar handboek heeft opgenomen [AFM-a]. Veel IT-auditors worden van oudsher ingezet om de traditionele general IT-controls of andere aspecten voor de IT-organisatie te toetsen. Maar met de groei van dienstverlening die geheel of gedeeltelijk digitaal verloopt, kan de rol van de IT-auditor verschuiven naar de voorkant van de dienstverlening door een organisatie. Online dienstverlening is een voorbeeld waar de IT-auditor die rol kan oppakken mits deze zich wel adequaat verdiept in de bedrijfscontext.

De richtlijnen van de AFM zijn in 2013 beschikbaar gekomen om de destijds na de bankencrisis sterke ontwikkeling van de 'Klantbelang Centraal'-gedachtegang ook op het vlak van online dienstverlening invulling te geven.[1] Veel financiële instellingen zagen zich vanwege de (regulerings-)kosten gedwongen om hun producten ook, of zelfs uitsluitend, online aan te bieden. De achterliggende gedachte om de richtlijn te publiceren was dat financiële dienstverleners in hun dienstverlening en producten het eigen financieel gewin hoger in het vaandel hadden staan dan het handelen in het belang van hun klanten. Met de introductie van MifiD-II[2] in januari 2018 is nog een update nodig voor de uitgangspunten in de AFM-richtlijn waarop dit artikel is gebaseerd; de richtlijn is dus nog niet geheel volledig, maar vormt een eerste aanzet. Voor dit artikel is dat niet relevant omdat het niet zozeer ingaat op de inhoud en interpretatie van het handboek en de achterliggende financiële regelgeving, maar op de geprogrammeerde proceselementen waarbij de IT-auditor het management en/of de opdrachtgever toegevoegde waarde kan leveren.

Online dienstverlening: procesopbouw

De richtlijn 'Online dienstverlening' geeft de financiële organisatie handvatten om digitale diensten in te richten. Daarbij moet de dienstverlener invulling gegeven aan de proceselementen die de AFM ziet als aansluitend bij de beleving van de klant. Dit zijn:

1. online kennismaking;
2. online beeldvorming;
3. online oplossing;
4. online nazorg;
5. online randvoorwaarden (waar privacyborging van de online klant nadrukkelijk nog bij moet worden genoemd, hoewel buiten de directe scope van de AFM).

Bij veel banken is het de compliance-afdeling die de invulling van de online klantbediening (ofwel 'customer experience') beoordeelt en al dan niet goedkeurt. Veel compliance-afdelingen ontbreekt het echter totaal aan de automatiseringskennis die nodig is om de kwaliteit van de geprogrammeerde maatregelen en algoritmen te kunnen beoordelen. Juist voor een IT-auditor liggen op dit vlak kansen, omdat die daar in principe de kennis voor heeft. Automatiseringskennis alleen is natuurlijk niet genoeg. De IT-auditor moet ook de achterliggende regelgeving en kaders begrijpen om de geprogrammeerde maatregelen in de juiste context te kunnen plaatsen. Ook heeft hij of zij specifieke kennis nodig om algoritmes te kunnen beoordelen. Dat is niet anders dan bij ondersteuning van een jaarrekeningcontrole: als de IT-auditor daar met uitgebreide bevindingen en/of advies komt op het onderdeel van de continuïteitsborging van de systemen, zal dat voor de accountant maar beperkte waarde hebben omdat deze voornamelijk naar de getrouwheid van de financiële verslaggeving kijkt. De IT-auditor zal zich in meer moeten hebben verdiept dan de bekende 'general IT-controls' of de puur technische aspecten van de (IT-) bedrijfsvoering, en zich dus goed moeten hebben verdiept in de context waarbinnen de opdrachtgever opereert.

Kritische procesonderdelen

Als het goed is, begint de audit met een risicoanalyse. Daaruit volgt waar de kritische online elementen zitten die de IT-auditor zou moeten onderzoeken. De AFM geeft hiervoor in het handboek al de nodige algemene aandachtspunten per dienstverleningsfase en bijbehorende procesactiviteiten. Aanvullend moet ook

de opdrachtgever of het management nadrukkelijk input leveren vanuit de specifieke implementatie en lokale omstandigheden.

De activiteiten en procesfasen die de AFM in haar richtlijn onderkent, zijn in tabel 1 weergegeven. In de eerste kolom staan daarbij de door de AFM onderkende activiteiten benoemd, en in de tweede kolom de procesfasen. Voor het begin van de daadwerkelijke audit moet de auditor inschatten welk risico de klant loopt bij fouten in de geprogrammeerde maatregelen of wanneer de bank de verkeerde uitgangspunten hanteert. De auditor moet deze inschatting vanzelfsprekend voorafgaand aan de audit valideren bij de opdrachtgever. De weergegeven weging vormt hierbij een voorbeelduitwerking.

Aspect dienstverlening (activiteit)	Risico-categorie per proces-fase				Toelichting op het te controleren aspect
	Kennis-making	Beeld-vorming	Oplos-sing		
1.1. Bepaal uw doelgroep	-				Voornamelijk beleid- / procesgerelateerd
1.2. Denk na over de producten die deel uitmaken van uw dienstverlening	L				Voornamelijk beleid- / procesgerelateerd: juistheid online productaanbod.
1.3. Omschrijf uw doelgroep duidelijk	M				Voornamelijk procesgerelateerd: functioneren van het algoritme dat de doelgroep-controle toetst.
1.4. Leg uw dienstverlening uit	M				Juiste versies bij wijzigingen, en functioneren van het algoritme dat productbegrip toetst.
2.1. Ondersteun de klant bij het aanleveren van de gevraagde informatie		L			Voornamelijk procesgerelateerd: adequaat functioneren communicatiekanalen.
2.2. Stuur uw klant niet		H			Aantoonbaar geen klantkeuze-sturing via applicatiealgoritmen.
2.3. Pas 'nudging' zorgvuldig toe [2]		H			Algoritmen volgen de regels voor toegestane nudging via de applicatiesoftware.
2.4. Zorg dat de verkregen informatie juist is		M			Controls gericht op juiste verwerking invoer klantgegevens. Doelbinding conform de AVG.
2.5. Filter inconsistente antwoorden en maak spanningen in het klantbeeld zichtbaar		H			Betrouwbaarheid geprogrammeerde signaleringsalgoritme
2.6. Geef uw klant tijd om te antwoorden		L			Voornamelijk procesgerelateerd: er kan worden geverifieerd of time-outs niet leiden tot verlies of verminking van gegevens indien de klant wens door te gaan.
2.7 Zorg voor een printversie van de geïnventariseerde gegevens		M			Integriteit reproductie van klantgegevens op print
3.1. Biedt een persoonlijke oplossing			M		(Historisch) Blijvende aansluiting met 1.2.
3.2. Maak afwijkingen van het advies inzichtelijk			M		Betrouwbaarheid geprogrammeerde signaleringsalgoritme
3.3. Leg vast en bewaar het oorspronkelijke advies			H		Advies aantoonbaar authentiek & integer
4.1. Maak afspraken over nazorg				-	Voornamelijk procesgerelateerd
4.2. Goede nazorg begint met vastlegging				M	Aanvullingen klantdossier aantoonbaar authentiek & integer
4.3. Monitor het klantbeeld en de dienstverlening regelmatig				H	Betrouwbaarheid geprogrammeerde monitoringsalgoritmen

Tabel 1: Overzicht van activiteiten in het online dienstverleningsproces het bijbehorend afbreukrisico door foutieve software

Het afbreukrisico van de geprogrammeerde beheersmaatregelen en gehanteerde softwarealgoritmen zit vooral in de activiteiten uit de risicocategorie 'Hoog (H)'. Hoewel de richtlijn van de AFM nog niet expliciet rekening houdt met geprogrammeerde algoritmen, is heden ten dage de aandacht voor de goede werking van algoritmen sterk toegenomen. Het is dan ook relevant bij het beoordelen van de (implementatie van) de online dienstverlening door de financiële organisatie dat de juiste werking van geprogrammeerde functies en algoritmen wordt getoetst.

Randvoorwaarden

In tabel 1 is nog geen rekening gehouden met de ook in de richtlijn opgenomen randvoorwaarden voor een zorgvuldige online dienstverlening. In tabel 2 zijn deze randvoorwaarden weergegeven en voorzien van een toelichting.

Randvoorwaarden dienstverlening	Belang voor de IT-auditor	Toelichting op het te controleren aspect
R.1 De vakbekwaamheidseisen gelden ook online	L	Niet direct relevant voor de IT-auditor.
R.2 Uw klant heeft bedenktijd	-	Niet direct relevant voor de IT-auditor.
R.3 Wees zorgvuldig bij informatieverstrekking	H	Veiligheid van de verwerking en opslag (technisch & organisatorisch). Naleving wettelijk retentietijden indien geprogrammeerd. Backup & recovery aspecten.
R.5 Verstrek een dienstverleningsdocument (DVD)	M	Juiste versies bij wijzigingen, en de onweerlegbaarheid van verstrekking van de DVD aan de klant.
R.6 Bescherm gegevens van uw klanten	H	Veiligheid van de verwerking (technisch). De AFM verwijst hier naar de kaders van de Autoriteit Persoonsgegevens [AUTO], en de naleving van artikel 32 (Beveiliging) uit de AVG.
R.7 Controleer de identiteit van uw klant	H	Veiligheid van de verwerking (technisch). Betrouwbaarheid controle-algoritme om de identiteit vast te stellen (i.v.m. onder meer de compliance met de Wwft en AVG).
R.8 Ook bij uitbesteding blijft u verantwoordelijk	M	Verdeling beveiligingsafspraken als onderdeel van het contract, rol verwerkingsverantwoordelijke en verwerker en formele verwerkersovereenkomst. Compliance met artikel 4 en 28 uit de AVG.
R.9 Test uw dienstverlening regelmatig	H	Periodieke controle beveiligingsniveaus. Correct blijven functioneren van procesmatige beheersmaatregelen en algoritmen (zie activiteiten 1.x t/m 4.x).

Tabel 2: Overzicht van randvoorwaarden en hun belang in het auditprogramma voor de IT-auditor.

In de randvoordwaarden gaat de AFM niet in detail in op alle aanvullende eisen vanuit de AVG, want die liggen op het terrein van een andere toezichthouder, de Autoriteit Persoonsgegevens. Wel zijn de AVG-eisen globaal terug te vinden in de randvoorwaarden R.4 en R.6 en, meer indirect, R.7, R.8 en R.9. In december 2019 heeft de AFM de 'Principes voor Informatiebeveiliging' vastgesteld. Dat aanpalende toezichtkader kan de

IT-auditor prima richting geven in wat de AFM verwacht bij deze randvoorwaarden [AFM19]. Zoals in tabel 2 als voorbeeld voor een belangenafweging (middelste kolom) is uitgewerkt, zal de IT-auditor per situatie een eigen inschatting moeten maken van de risicofactoren en hun gewichten.

Selectie van de te beoordelen maatregelen

Nadat de individuele weging en globale aanpak voor de beoordeling zijn vastgesteld en uitgewerkt, zoals weergegeven in de tabellen 1 en 2, kan de auditor in overleg met de opdrachtgever vaststellen welke set van beheersmaatregelen daadwerkelijk wordt getoetst en dus onderdeel van de scope wordt. De keuze kan zijn om de hele set integraal te toetsen, of om zich te richten op de belangrijkste beheersmaatregelen in het online dienstverleningsproces voor een financieel product.

Maatregelen met een hoog afbreukrisico

Op basis van de risicoanalyses uit de twee vorige paragrafen kan de IT-auditor een concreet, gedetailleerd toetsingsprogramma gaan afstemmen met de opdrachtgever. Dit werkprogramma omvat de geprogrammeerde beheersmaatregelen (binnen het geautomatiseerde dienstverleningsproces) met de risicoclassificatie 'hoog'. Dat wil dus zeggen dat de juiste werking van die geprogrammeerde beheersmaatregel zwaar weegt in de selectie van het uiteindelijke product dat de klant krijgt aangeboden (of juist uiteindelijk niet krijgt aangeboden, want ook dat is een mogelijke consequentie). De AFM heeft in haar richtlijn niet uitgewerkt hoe de exacte invulling dient te zijn van de norm voor het adequaat functioneren, slechts wat zij per activiteit verwacht. Hier ligt een taak voor de IT-auditor. Een toetsing van deze geautomatiseerde beheersmaatregel(en) op basis van die normen kan dan bijvoorbeeld weer door de interne auditor of compliance officer worden gebruikt als onderdeel van de beoordeling van het integrale online dienstverleningsproces.

Een voorbeeld ter illustratie: activiteit 2.5 vereist dat spanningen in het klantbeeld zichtbaar worden gemaakt. Het gebruikte algoritme moet de antwoorden van klanten dus betrouwbaar analyseren op inconsistenties. Achterliggend klantbelang-principe is dat de klant alleen een passend product aangeboden krijgt en er dus geen sprake is van 'mis-selling.[3] Dit vergt dat het algoritme (in principe gewoon softwarecode) zo is geprogrammeerd dat (bijvoorbeeld):

- inconsistenties in antwoorden adequaat worden gedetecteerd (norm 1);
- inconsistenties juist en eenduidig aan de klant worden getoond (norm 2);
- de hieruit volgende consequenties duidelijk aan de klant worden getoond én de klant de optie krijgt deze bij te stellen dan wel te negeren (norm 3). Hiermee wordt voldaan aan artikel 22 van de AVG betreffende geautomatiseerde, individuele besluitvorming waarin wordt bepaald dat een individu niet mag worden onderworpen aan een uitsluitend op geautomatiseerde verwerking gebaseerd besluit.

De IT-auditor moet op basis van deze drie normen verifiëren of de software juist functioneert. Dit kan aan de hand van de ontwerpdocumentatie en onder meer op basis van de testresultaten. Zoals norm 3 laat zien, moet de IT-auditor ook rekening houden met andere regelgeving dan de online dienstverleningsrichtlijnen zelf.

In dit voorbeeld worden overigens basale softwarealgoritmen beoordeeld door de IT-auditor. Algoritmen als onderdeel van een zelflerend system, een Artificiële Intelligentie of AI, is momenteel actueel onderdeel van een verkennend onderzoek door AFM en DNB [AFMDNB]. Dit onderwerp ligt echter buiten de scope van dit artikel, en vergt een hoge mate van deskundigheid – zelfs specialisatie – van een IT-auditor om te kunnen beoordelen.

Maatregelen met een middel of laag afbreukrisico

De toetsing van geautomatiseerde beheersmaatregelen met de risicoclassificatie 'middel (M)' of 'laag (L)' (afbreuk-)risico bij disfunctioneren is vooral nuttig om de opdrachtgever meer zekerheid geven of zijn online procesontwerp goed uitgebalanceerd is, en het online platform voldoende aansluit bij de richtlijnen uit het handboek. Dat is laatste is dan vooral een kosten-batenafweging.

Toegevoerde waarde IT-auditor: waarop beoordelen?

Voor de IT-auditor zit bij de online dienstverlening het leveren van toegevoegde waarde in het kunnen beoordelen van ten eerste de gebruikte geprogrammeerde controles en algoritmen en ten tweede de randvoorwaarden voor veilige online gegevensuitwisseling. Bij een ondeugdelijke implementatie volgt een onbetrouwbare dienstverlening met alle gevolgen van dien voor de financiële dienstverlener of instelling. Maar ook en vooral voor de klant, die dacht te maken te hebben met een betrouwbare zakenpartner die het beste voor had met zijn of haar belangen.

Formeel heeft de AFM het verstrekken van 'assurance' voor de uitvoering van deze richtlijnen niet verplicht gesteld. Kwaliteitsgebreken en een gebrekkige bediening van het klantbelang kunnen echter wel onderdeel van een periodiek gesprek zijn van een financiële dienstverlener met de toezichthouder. Een objectief onderzoek door een IT-auditor, al dan niet in combinatie met een andere 'assurance'-verschaffer, kan het vertrouwen van de toezichthouder in de financiële dienstverlener aanzienlijk vergroten. Dat is dringend nodig. Online dienstverlening is immers nog altijd, en door de stijgende kosten van fysiek financieel advies, in steeds grotere mate een groeiende markt waarmee financiële dienstverleners hun winstmarges op peil kunnen houden.

Literatuur

[AUTO] Financiële ondernemingen, Autoriteit Persoonsgegevens. https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/financien/financiele-instellingen, geraadpleegd op 27 januari 2020.

[AFM] Handboek Online Dienstverlening, AFM. https://www.afm.nl/~/profmedia/files/onderwerpen/online-dienstverlening/handboek-online-dienstverlening.ashx, geraadpleegd op 27 januari 2020.

[AFM19] Principes voor informatiebeveiliging, AFM, 19 december 2019. https://www.afm.nl/nl-nl/nieuws/2019/dec/principes-informatiebeveiliging, geraadpleegd op 27 januari 2020.

[INVES20] Misselling, Investopedia, 19 januari , 2020. https://www.investopedia.com/terms/m/misselling.asp, geraadpleegd op 27 januari 2020. Zie https://www.afm.nl/nl-nl/professionals/onderwerpen/mifid-2

[MiFID II] MiFID II, AFM, https://www.afm.nl/nl-nl/professionals/onderwerpen/mifid-2, geraadpleegd op 27 januari 2020.

[WIKI] Nudging, Wikipedia, https://nl.wikipedia.org/wiki/Nudging, , geraadpleegd op 27 januari 2020.

[AFMDNB] Artificiële Intelligentie in de Verzekeringssector – Een Verkenning, https://www.afm.nl/~/profmedia/files/rapporten/2019/afm-dnb-verkenning-ai-verzekeringssector.pdf, geraadpleegd op 28 januari 2020.

Noten

1. Hiernaar heeft onder meer de Vrije Universiteit heeft bij het begin van de crisis in 2008 onderzoek gedaan.
2. Mifid 2 is de 'Markets in Financial Instruments Directive' update van de oorspronkelijke regelgeving uit 2007, en onderdeel van de Wet op het Financieel Toezicht (Wft). [MiFID II]
3. Misselling is een verkooppraktijk waarbij een product of dienst opzettelijk onjuist wordt voorgesteld of waarbij een klant wordt misleid over de geschiktheid ervan. [INVES20]

Ir. J.E. (Jean-Jacques) Bistervels | informatiebeveiligingsmanager en privacyspecialist bij *Sanoma*

Jean-Jacques Bistervels is werkzaam als Informatiebeveiligingsmanager bij Sanoma. Daarnaast houdt hij zich bij Sanoma ook bezig met fraudebeheersings- en privacyvraagstukken. Na zijn studie Technische Bedrijfskunde aan de TUE is hij zijn carrière bij Ernst & Young gestart als IT-auditor. Hij heeft daarna ruim zeven jaar gewerkt binnen de farmaceutische sector en daarna tien jaar in de financiële sector. Sinds oktober 2018 is hij werkzaam in het bedrijfsonderdeel Learning & Media.