TPM verklaring

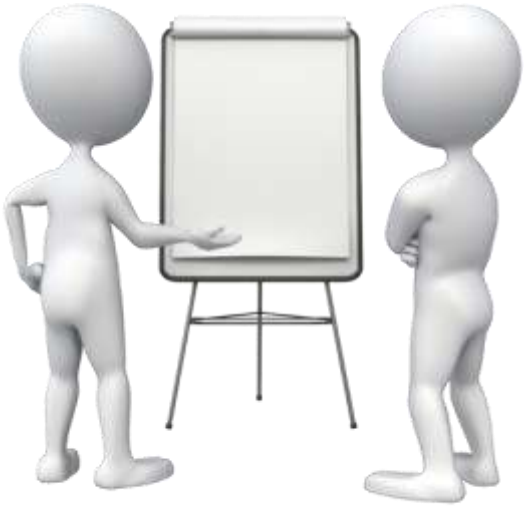
Wat is een Third Party Mededeling?

Het uitbesteden van processen is binnen hedendaagse organisaties erg gebruikelijk. Maar hoe kunt u als dienstleverlener uw (potentiële) klanten overtuigen van de kwaliteit van uw diensten? Hoe verkrijgt de klant zekerheid over de processen die uitbesteed zijn aan uw organisatie? Uw klant blijft immers zelf eindverantwoordelijk voor deze processen. Een oplossing is: de Third Party Mededeling.

Een Third Party Mededeling is een mededeling die afgegeven wordt door een onafhankelijke auditor over de kwaliteit en betrouwbaarheid van u als dienstverlener. Het maakt de kwaliteit van een organisatie en haar dienstverlening inzichtelijk. Het wordt een TPM genoemd omdat de eerste betrokken partij de leverancier als opdrachtgever is, de tweede partij de auditor als opdrachtnemer en de derde betrokken partij de uiteindelijke doelgroep, de klantengroep. De TPM toont vooraf aan dat de kwaliteit van de aangeboden dienstverlening is gewaarborgd. Het kwaliteitsniveau wordt in een rapportage aan (potentiële) klanten objectief aangetoond door een ondertekende mededeling van een externe auditor. Het verschaft de klant zekerheid van een betrouwbare werking (in de zin van volledigheid, juistheid en tijdigheid) over de uitbestede processen en geautomatiseerde systemen.

Wat zijn de voorwaarden?

Voordat sprake kan zijn van een TPM, moet aan een aantal voorwaarden worden voldaan:



- Een 1e voorwaarde is dat een TPM moet worden opgesteld en worden ondertekend door een RE auditor. RE auditors voldoen aan de eisen die NOREA, de beroepsorganisatie van IT-auditors stelt. Dit betekent dat een TPM wordt uitgevoerd overeenkomstig Nederlands recht, waaronder de NOREA richtlijn 3000: 'Richtlijn Assurance-opdrachten door IT-auditors'. Dit vereist dat een RE auditor voldoet aan de voor hun geldende ethische voorschriften en dat de werkzaamheden zodanig worden uitgevoerd dat een redelijke mate van zekerheid wordt verkregen over de vraag of de interne beheersmaatregelen, in alle van materieel belang zijnde aspecten, op afdoende wijze zijn opgezet door de opdrachtgever, bestaan en werken.
- Een 2e voorwaarde is dat het moet gaan om een *standaard* proces of een standaard applicatie of standaard infrastructuur of een standaard SAAS oplossing. Daarnaast moet uw wijzigingsbeheer volledig zijn ingericht en op orde zijn zodat wijzigingen in het object van onderzoek volledig beheerst worden doorgevoerd. Anders heeft een TPM ook geen zin en kan beter worden volstaan met een individueel assurance rapport.
- Een 3e voorwaarde is dat opdrachtgever en haar klanten het eens zijn over het gehanteerde normenkader waarover in de TPM zekerheid wordt gegeven.
- Een tenslotte is een 4e voorwaarde dat vooraf overeenstemming is bereikt over de precieze afbakening van het object van onderzoek en de diepgang (opzet, bestaan en/of werking).

TPM verklaring

Wat is uw voordeel?

Bedrijven maar ook de overheid besteden steeds vaker activiteiten uit aan gespecialiseerde serviceorganisaties. Dit vereist wederzijds vertrouwen en transparantie. Een eigenaar van de uitbestede dienst blijft eindverantwoordelijk en moet bijvoorbeeld aan een toezichthouder over de uitbestede dienst zich verantwoorden. Dat kan door een Assurance mededeling afgegeven door een RE. Dit betekent dat de klant of zijn vertegenwoordiger (de accountant) de serviceorganisatie zou moeten bezoeken om vast te stellen of de risico's voldoende zijn afgedekt. Door een TPM-mededeling is dit niet meer nodig. De mededeling verschaft namelijk de klant aantoonbare zekerheid omtrent een betrouwbare werking van de uitbesteden processen en geautomatiseerde systemen die de dienstverlener aan de klant aanbiedt. Tot slot is een TPM-mededeling bruikbaar voor alle afnemers.

Wij kunnen voor u een TPM afgeven. Dit betekent dat we vaststellen dat uw software of hosting voldoet aan de richtlijnen. De RE auditor van uw klant kan op dit bewijs "steunen" en hoeft dan geen afzonderlijk onderzoek te doen naar de beveiliging bij u als dienstverlener. In de praktijk betekent dat bijvoorbeeld de pentesten voor dat onderdeel kunnen vervallen bij de klant. Dat scheelt u tijd en uw klant geld.

Wat is de aanpak?

De onafhankelijke auditor doorloopt drie stappen. Tijdens de eerste stap (de voorbereiding), vraagt de auditor inzicht in het object van onderzoek, bakent dit af met bijvoorbeeld een netwerktekening en wenst inzicht in de beveiligingsmaatregelen die u als dienstverlener heeft genomen om de risico's in de huidige processen te kunnen beheersen.[1]

Tijdens de uitvoering (stap 2) van het TPM onderzoek, toetst de auditor de opzet en het bestaan. Afhankelijk van de gecontracteerde diepgang wordt ook de werking van de beschreven werkwijze getoetst door interviews af te nemen, documenten te bestuderen en door waarnemingen ter plaatse en eventuele penetratietesten uit te (laten) voeren, logs op te vragen etc.

Tijdens de rapportagefase (stap 3) verklaart de onafhankelijke auditor aan de hand van de vooraf opgestelde criteria of de interne beheersingsmaatregelen voldoen. Zijn bevindingen over de organisatie geeft hij weer in een (Assurance)rapport. Indien de controles goed verlopen zal de auditor een TPM-mededeling afgeven.

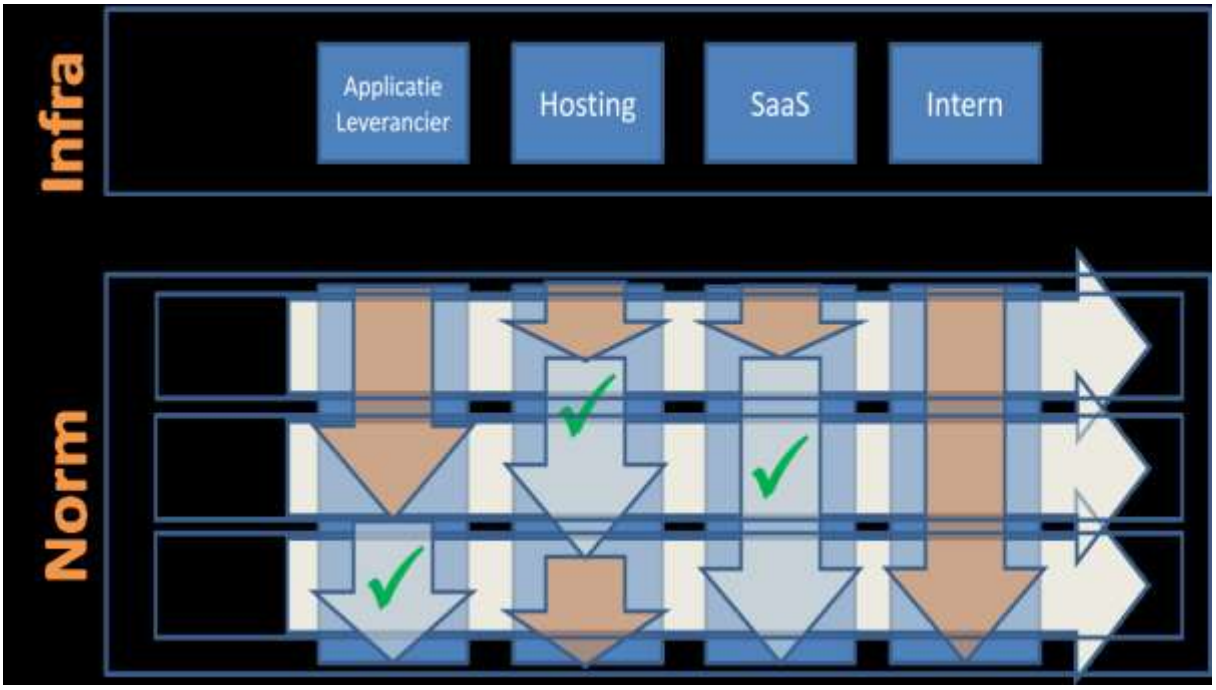
Een voorbeeld: een DigiD TPM

Het ICT-beveiligingsassessment is gericht op het stelsel van maatregelen en procedures met als doel de beveiliging van een webomgeving te optimaliseren. Het stelsel omvat zowel geautomatiseerde als niet geautomatiseerde maatregelen en procedures. Het Digid beveiligingsassessment is een controle op de betrouwbaarheid van de Digid-koppeling van overheidswebsites. Via deze koppeling kunnen burgers een persoonlijke toegang tot de website verkrijgen. Alle DigiD-gebruikende organisaties moeten jaarlijks een ICT-beveiligingsassessment laten uitvoeren.

[1] *Een preventieve maatregel heeft als doel de risico's vooraf te verkleinen onder het motto: voorkomen is beter dan genezen; een repressieve maatregel heeft als doel om de risico's achteraf te verkleinen.*

TPM verklaring

Dit assessment vindt plaats conform een door het Nationaal Cyber Security Center opgestelde beveiligingsrichtlijn en de daarop door Logius gebaseerde Norm op straffe van afsluiting van DigiD. Meer informatie over het assessment is terug te vinden op het YouTube kanaal van BKBO. Volg hiervoor de link https://www.youtube.com/watch?v=XuT8PPnxj_g



In de linker kolom is een organisatie opgenomen die een webapplicatie heeft 'gekocht' bij een externe leverancier. De richtlijnen die gelden voor de software kunnen worden getoetst op een gelijkwaardige omgeving bij de leverancier.
De tweede kolom geeft de situatie aan waarbij de organisatie gebruikmaakt van een externe partij voor het hosten van de webapplicatie. De richtlijnen die gelden voor de infrastructuur, maar ook een aantal procesmatige richtlijnen kunnen worden vastgesteld bij de hostingpartij.
De derde kolom is een combinatie van de eerste twee situaties, namelijk een organisatie die een webapplicatie afneemt bij een leverancier die dit aanbiedt in een SaaS-oplossing. Hierbij zal een groot gedeelte van de richtlijnen voor zowel de software, de infrastructuur als een aantal processen bij deze SaaS-leverancier getoetst kunnen worden. De laatste kolom geeft de situatie weer waarbij de organisatie die DigiD gebruikt alles zelf geregeld heeft.
Op basis van de richtlijnen van Logius is een TPM maximaal één jaar geldig en mag door een klant slechts eenmaal worden gebruikt voor het DigiD assessment. Ergo, het TPM onderzoek moet jaarlijks worden herhaald. Dat geldt voor de meeste TPM's.

Zie voor een gedetailleerde uitleg de animatie op ons YouTube kanaal https://www.youtube.com/channel/UCkr-OEs61ynZhqR69XNbyQw

Hoe doen wij dat?

Wij hebben een standaard uitvoeringswijze ontwikkeld voor alle type TPM's die we leveren. Op basis van een door ons ontwikkelde documentatieverzoek kunnen we uw lokale situatie overzichtelijk in kaart brengen en weet u meteen welke bewijsstukken we precies nodig hebben. Vervolgens zal onze auditor bij u ter plaatse een quick scan uitvoeren om samen met u vast te stellen of uw beeld volledig is en klopt. Daarbij wordt een auditplan met u besproken waarbij duidelijk wordt welke bewijsstukken precies worden verlangd, welke testen dienen te worden uitgevoerd en op welke termijn dat mogelijk is. We maken hierbij verschil tussen de verschillende types TPM's. We

TPM verklaring

kunnen een TPM verklaring afgeven voor elk normenkader dat te auditen is. We doen dit normaliter volgens de ISAE3000/A of ISAE3000/D richtlijn van onze beroepsvereniging NOREA. Zie voor een gedetailleerde uitleg ons YouTube kanaal

Ingeval dit nodig is, worden vervolgens de penetratietesten uitgevoerd door de gecertificeerde pentesters van onze partner Defenced BV. Eerst wordt een zogenaamde blackbox test (grotendeels via geautomatiseerde scans) uitgevoerd om na te gaan of het mogelijk is om ongeautoriseerd toegang te krijgen. Als dat mogelijk blijkt, wordt in fase 2 vastgesteld of het mogelijk is via de website - met de daarop aangetroffen kwetsbaarheden – ongeautoriseerd toegang te verkrijgen tot de achterliggende systemen. Dat is dan een grey-box pentest, waarbij u desgevraagd de benodigde privileges en configuratie-instellingen van relevante netwerkcomponenten via ons aan de penetratietester verstrekt. Volledige medewerking van uw IT personeel en dat van uw eventuele leveranciers is hierbij een vereiste.

Tegelijk vindt door de Register EDP auditor van BKBO een audit plaats op uw contracten, procedures en de beveiligingsorganisatie.

In een overzichtelijke conceptrapportage worden vervolgens de bevindingen gerapporteerd en doen we aanbevelingen om de tekortkomingen op te heffen. Het assessment wordt afgesloten met een gesprek waarin de bevindingen worden toegelicht, waarna de rapportage definitief wordt gemaakt. De uitvoering van het onderzoek en de rapportage vinden plaats op basis van de Richtlijn 3000 van NOREA die betrekking heeft op het verrichten van assurance werkzaamheden. De rapportage bevat een overzicht van de feitelijke bevindingen per maatregel, waarbij per maatregel wordt aangegeven of deze voldoet. De definitieve rapportage dient u als opdrachtgever naar Logius te versturen.

Omdat de opdracht ook een penetratie- en of vulnerabilitytest omvat, wordt u gevraagd om een vrijwarings-verklaring overeen te komen. Uiteraard zullen we proberen zoveel mogelijk ongelukken te voorkomen, worden de tests nauwkeurig met u afgestemd en is het onderuit halen van uw webportals niet aan de orde. Ingeval u als organisatie over een Third Party Mededeling (= TPM) van uw leverancier(s) beschikt is een dergelijke test doorgaans niet nodig.

Verschillende TPM's

We hebben tot dusver ervaring met de volgende specifieke TPM onderzoeken:

- BIO TPM
- DigiD TPM (zowel SAAS, als applicatie en/of hosting diensten)
- DigiD LMA (leverancier Meervoudige Aansluiting)
- Suwinet (zowel DKD als Inkijk)
- Vecozo TPM
- Wpg TPM

TPM verklaring

Wat is uw investering?

De kosten voor de levering van een TPM variëren afhankelijk van het normenkader en wat er onderzocht moet worden tussen de € 3.600,- en € 12.000,- afhankelijk van wat er door ons moet gebeuren. Genoemde prijzen zijn exclusief btw, maar inclusief reis- en verblijfskosten. Meer informatie over het assessment is terug te vinden op het YouTube kanaal van BKBO.

Geen gekibbel garantie

Anders dan andere auditorganisaties geven wij u "geen gekibbel garantie". Onze prijs is vast en dus inclusief een eventuele her pentest, heraudit of aanvullend assessment.

Meer weten?

Dit product wordt voor uw situatie geheel op maat gemaakt. Daarom kunnen wij ons voorstellen dat u nog vragen heeft. Wij staan voor u klaar en gaan graag met u in gesprek om tot een definitieve offerte te komen.

U kunt direct bellen met BKBO op telefoonnummer: 073 – 211 03 37.

Is het voor u duidelijk? Dan kunt u ook direct een offerte aanvragen. Ga naar de site: https://bkbo.nl/offerte-aanvragen-tpm-verklaring/