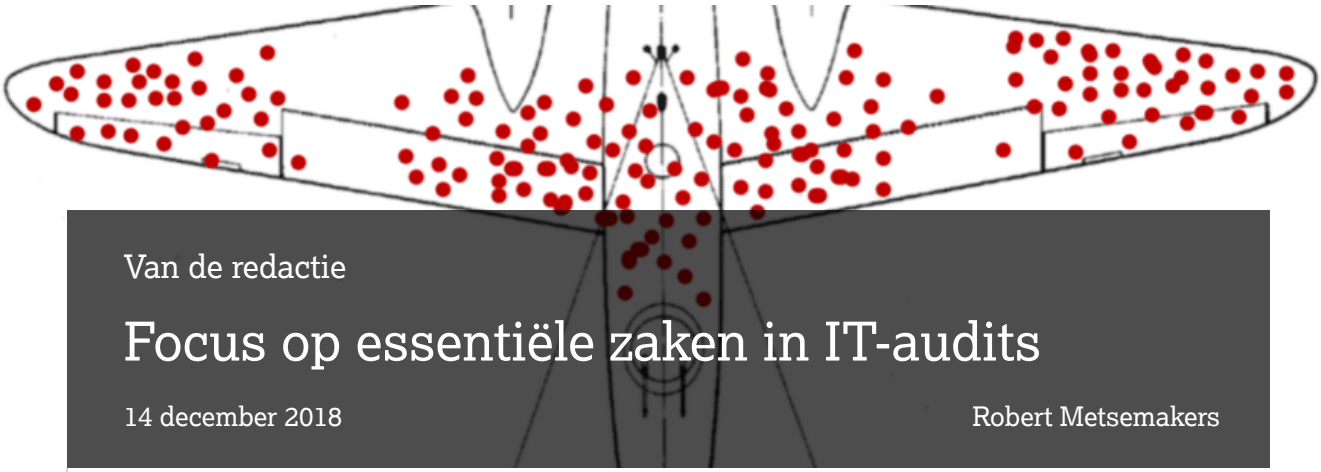


Van de redactie

Focus op essentiële zaken in IT-audits

14 december 2018

Robert Metsemakers

Waar let je op als je de kwaliteit van informatiebeveiliging wilt verbeteren of op het reeds hoge niveau wilt houden? Let je op het ontbrekende deel in de mitigerende maatregelen of juist op wat wél aanwezig is? Focus, als keuze om bepaalde dingen wel en andere juist niet te doen, is meestal goed. Maar richt daarbij de aandacht dan wel op het juiste onderwerp.

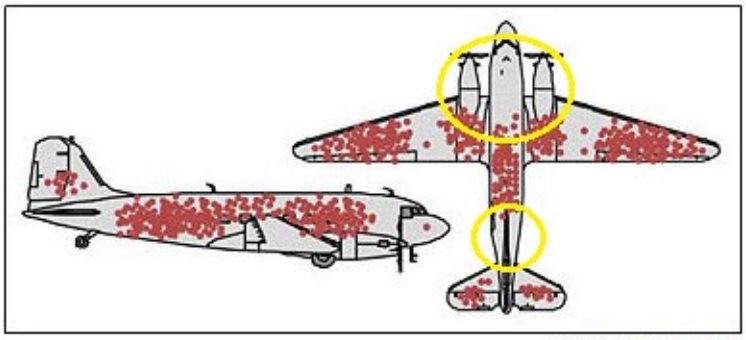
Britse vliegtuigen bombardeerden en beschoten in de Tweede Wereldoorlog steden in Nazi-Duitsland. Ze werden zelf ook geraakt, door vliegtuigen en luchtafweergeschut – de Nazi's verdedigden immers hun burgers, militairen, handel en industrie tegen deze aanvallen. Alle Britse vliegtuigen werden daarom bij terugkeer op de vliegvelden in het Verenigd Koninkrijk nauwkeurig onderzocht en de bepantsering werd verstevigd. Maar de geallieerden hadden er enige tijd plus het inzicht van wiskundige, statisticus en econoom Abraham Wald – die van het begrip *survivorship bias* – voor nodig om in te zien dat het verstevigen juist moest gebeuren op de plaatsen waar de vliegtuigen niet geraakt waren. Want de geraakte plaatsen, zichtbaar aan de kogelgaten of geheel weggeschoten delen, waren duidelijk niet essentieel om terug te kunnen keren naar de vliegbasis. Juist de niet-geraakte delen hadden het teruggekeerde vliegtuig immers gedragen.

'Hel en verdoemenis' … niet dus

Laten we nu eens een te auditen afdeling of proces vergelijken met het vliegtuig en de auditor oneerbiedig met het luchtafweergeschut. De auditor raakt in zijn audit of onderzoek het vliegtuig en zet een flink aantal bevindingen als kogelgaten op papier. Die bevindingen of 'issues' verschillen onderling in omvang, plaats, invloed op het 'vliegtuig' en daarmee in hun belang. Elke auditor, ook ik, weet dat bij gerapporteerde bevindingen die niet urgent, dringend, of belangrijk worden genoemd, de aandacht van de lezer al snel verslapt. Zeker als die auditee als manager toch al te weinig tijd heeft of neemt om het hele rapport te lezen en zich daarom beperkt tot de aanbevelingen in de managementsamenvatting vooraan in het rapport. De (zeer) belangrijke issues komen in de managementsamenvatting. De nogal belangrijke bevindingen komen nog wel in het rapport zelf, en de niet belangrijke bevindingen komen niet eens in het rapport terecht.

De auditor bespreekt de bevindingen met de auditee, er worden per oplosactie realisatiedata en verantwoordelijke personen bepaald en alles wordt vastgelegd op een actielijst. Sommige issues zijn urgent en moeten snel, binnen drie maanden, opgelost worden. Andere issues zijn dringend en moeten over zes maanden klaar zijn. Anders gaat het licht uit, vergaat de wereld, komen er grote problemen enzovoort. Belangrijke issues moeten bijvoorbeeld binnen een jaar worden opgelost en issues met de urgentie 'behoeft management aandacht' binnen twee jaar.

Vaak duurt het echter langer, veel langer dan de vooraf afgesproken periode om issues op te lossen. En toch blijft het licht ondertussen branden, gaat de tent niet failliet en komen er geen enorme boetes van de toezichthouder. Werkend aan de auditee-kant dronk ik ooit champagne omdat een urgent genoemd issue – dat dus binnen drie maanden opgelost moest worden – reeds zes volledige jaren 'open' op de actielijst stond, terwijl de onderzochte afdeling nog steeds succesvol draaide. Met andere woorden, het vliegtuig vloog nog steeds! Het door de auditor gevonden 'gat' was weliswaar een tekortkoming, maar niet essentieel. Het 'urgent' van de auditor was destijds overgekomen op de auditee als louter tijdgedreven. De auditor achtte de kans dat het op dat punt fout zou gaan zo hoog, dat het gat geen drie maanden meer open kon blijven. Als de auditee er na het plaatsen op de actielijst in slaagt om toch jarenlang in de lucht te blijven, zonder dat urgente issue ooit aan te pakken, gaat het tijdsdrukgevoel echter verloren. 'The thrill is gone', zou bluesgitarist B.B. King zingen, want *the sense of urgency* for the auditee heeft te veel lettergrepen. Het mooiste is wanneer auditor en auditee gezamenlijk de prioriteit van oplossen bepalen en daarbij rekening houden met de impact én de kans op een bedreigende gebeurtenis.



Credit: Cameron Moll

Gentlemen, you need to put more armour-plate where the holes aren't because that's where the holes were on the airplanes that didn't return - Abraham Wald 1942.

Urgentie van issues in soorten en maten

Er kunnen goede en minder goede redenen zijn waarom een auditor vindt dat bepaalde issues urgent zijn en dus als eerste opgelost moeten worden, namelijk omdat ze:

a. zeer riskant zijn door een hoge *impact* als het fout gaat;
b. zeer riskant zijn door een hoge *kans van optreden*;
c. noodzakelijk zijn om daarna andere issues goed, goedkoop of snel – let op, kies er slechts twee uit deze 'duivelsdriehoek' – op te kunnen pakken;
d. niet veel tijd hoeven te kosten en de auditee het gevoel kunnen geven 'dat zijn medewerkers meters maken' met de noodzakelijke verbeteringen.

Reden (a) is de beste motivatie en deze is ook goed te onderbouwen met een inschatting van de mogelijke schade bij optreden. Maar dit onderbouwen moet de auditor dan wel expliciet doen in zijn managementsamenvatting, want anders denkt de auditee dat het issue urgent is om reden (b).

Reden (b) is ook een goede, maar de auditor moet daarvoor wel beschikken over een kristallen bol van uitzonderlijke kwaliteit of gewoon uit de losse pols zelf de toekomst kunnen voorspellen. De ingeschatte kans van optreden kun je met statistisch goochelen omrekenen naar een periode waarin de vervelende impact naar verwachting zal gaan optreden. Maar wanneer die periode inmiddels meerdere jaren verstreken is – zie het champagne-voorbeeld – worden voortgangsgesprekken over de actielijst tussen auditor en auditee wel een beetje ongemakkelijk. Zeker wanneer de prioriteit-inschatting puur van de kant van de auditor komt en de auditee, achteraf, 'de kans altijd al te hoog had gevonden'.

Reden (c) is misschien wel de beste, maar per slot van rekening ook gebaseerd op een niet al te harde inschatting.

Reden (d) is de politieke of verkoopmotivatie. Wat verkocht wordt is het 'laaghangend fruit' – dat is misschien niet zo voedzaam of lekker of gezond als de hoger hangende vruchten, maar je kunt er wel gemakkelijker bij. Het motiveert de plukker dat hij zijn eerste mandje al snel gevuld heeft en volgende issues zullen hopelijk ook voortvarend aangepakt worden. Bijkomend nadeel is dat deze issues meestal inderdaad snel worden opgelost en dus van de actielijst verdwijnen. De moeilijke en tijdrovende issues blijven dan over, wat vervolgens de via deze truc opgebouwde motivatie bij de auditee weer teniet kan doen. Niet de allerbeste reden dus.

Hoe dan wel ?

Begrijp me goed: auditors moeten blijven auditen (lees: schieten op vliegtuigen) en daarbij letten op zaken die niet voldoen aan een voorafgaand aan de opdracht met de

opdrachtgever vastgestelde set normen. En ze moeten die 'foute' zaken melden en ook de urgentie van de oplossing: urgent of 'slechts' dringend.

Maar ik zou er graag een lans voor breken onze audits te verrijken door nadrukkelijk ook aandacht te geven aan de niet-geraakte delen van het onderzochte vliegtuig (de wel onderzochte aspecten, waar echter geen bevindingen waren). Dat betekent analyseren wat er juist wél goed gaat in de uitvoering van precies die vitale, dus onmisbare delen en daar *lessons learned* en *best practices* uit te halen. Want andere auditees met hetzelfde proces kunnen dat proces daarmee vaak verbeteren en/of tijd en geld besparen. Hierbij ga ik uit van de situatie dat een (interne) auditor een proces een aantal keren onderzoekt zoals in een thema-onderzoek waarbij hetzelfde proces bij meerdere afdelingen wordt beoordeeld. Er zijn natuurlijk ook audits of onderzoeken gericht op de oorzaak van een groot incident, of met een forensisch karakter waar een dader van een eerdere (moedwillige) foutieve actie moet worden opgespoord. Daar zijn de gevonden issues anders van aard. En is het lastiger, ook door de noodzakelijke vertrouwelijkheid, om tot elders toepasbare lessons learned te komen.

'Voorspellen is moeilijk, vooral als het om de toekomst gaat', zoals natuurkundige Niels Bohr ons al waarschuwde. Als onafhankelijke buitenstaander kan een auditor soms beter het belang of de prioriteit van een aanbeveling inschatten dan de auditee die verantwoordelijk is voor uitvoering of implementatie ervan. Maar als tegenhanger hiervan moeten we als auditor wel conclusies trekken uit het gegeven dat het 'vliegtuig', ondanks alle in de audit ontdekte wérkelijke gaten en tekortkomingen, nog steeds vliegt en terugkeert op de basis.

Natuurlijk moeten we als auditors de auditee blijven helpen door voor en liefst samen met hem, de audit-issues te prioriteren naar hun belang en ernst. Maar laten we daarbij ook de durf hebben om na enige tijd die inschatting te heroverwegen. En dan een nieuwe inschatting en dus nieuwe selectie voor de issuelijst te maken: hoe zit het zes jaar later eigenlijk met die destijds tot urgent bestempelde issues, waren die echt allemaal zó urgent? Dat er al die tijd niets vervelends is gebeurd, betekent niet per definitie dat de urgentie aanvankelijk was overschat. Maar het stemt wel tot nadenken of het in de audit aangetroffen gat inderdaad een vitaal of essentieel punt in het proces of de onderzochte organisatie is. En dat is waar ik de focus zou willen leggen.

R. (Robert) Metsemakers | IT-auditor en informatiebeveiligingsexpert

Robert is een ervaren IT-auditor en informatiebeveiligingsexpert. Hij heeft ruime ervaring met het uitvoeren van audit- en adviesopdrachten. Hij gaat graag uitdagingen aan op gebieden als de inrichting van informatiebeveiliging, security advies en schrijfopdrachten op verschillende terreinen.

Robert is te bereiken via:

Robert.metsemakers@gmail.com

https://www.linkedin.com/in/robert-metsemakers