**Vraagstelling:**

Er is aangegeven dat er een continu of periodiek geautomatiseerd proces moet komen om pieken in de opvraging van ruwe data te voorkomen. Hoe moeten we deze functionele eis implementeren?

**Huidige praktijk**

Op dit moment wordt bij de jaarlijkse accountantscontrole[[1]](#footnote-1) een grote hoeveelheid data opgevraagd om de organisatorische status te kunnen bepalen van de procedures omtrent authenticatie, rollen en rechten.

Deze controle omvat onder andere de volgende punten:

1. Vanuit het oogpunt van mogelijke fraude is het niet de bedoeling dat een werknemer meer rechten heeft dan voor zijn werk noodzakelijk is;
2. Bij het uitdienst treden dient de toegang tot de systemen te worden ingetrokken;
3. Rollen en rechten mogen niet conflicterend zijn;
4. Er mag geen vermoeden van belangenverstrengeling bestaan;
5. Het aantal Administrators op een systeem mag niet meer zijn dan functioneel nodig

***Praktische bezwaren***

Aan de huidige praktijk kleven een aantal praktische, maar ook wettelijke bezwaren. Praktische bewaren zijn:

1. Het opvragen van de bulk aan data gebeurt altijd op ad hoc basis en er wordt vaak meerdere malen in een korte periode een gelijksoortige vraag gesteld, waarbij er telkens meerdere medewerkers en externe serviceproviders in korte tijd veel werk moeten verzetten.
2. Vervolgens wordt gedeeltelijk met de hand door de berg informatie gezocht op afwijkingen. Ook dit is een zeer grote klus met een zeer grote impact.
3. Omdat de controle een jaarlijks fenomeen is, is ook dit alles een jaarlijks terugkomende belasting, die met de groei van de organisatie steeds groter wordt.

***Wet- en regelgeving***

De wet geeft aan dat er een deugdelijke administratie[[2]](#footnote-2) moet worden gevoerd, en de AVG[[3]](#footnote-3) specificeert dat verder in het geval van de gegevensverwerkingen. De AVG heeft het over een “passende technische en organisatorische maatregelen om te waarborgen en te kunnen aantonen dat de verwerking in overeenstemming met deze verordening wordt uitgevoerd.” De overweging noemt ook de effectiviteit van de maatregelen en dat die effectiviteit moet kunnen worden aangetoond. Dat impliceert dat op elk moment een de status van de maatregelen moet kunnen worden weergegeven.

Zonder jullie direct mee te nemen in de theorie van de Bestuurlijke Informatievoorziening (BIV) kan uit bovenstaande al wel worden afgeleid dat op de een of andere manier een systeem moet worden bedacht om in de eis te voorzien. Op basis van de classificatie die grondlegger van de BIV[[4]](#footnote-4) heeft geïntroduceerd, kan voor de digitale administratie ook een classificatiesysteem worden opgezet. Wat hierin helder moet worden is het proces dat wordt doorlopen. Dus niet de black box met een invoer die een uitvoer betekent, maar wat is de relatie tussen de invoer en de uitvoer die ervoor zorgt dat de uitvoer voldoet aan de gestelde eisen.

Wettelijk gaat het er dan dus om de processen van de systemen te doorgronden en op die wijze te kunnen aantonen dat de maatregelen die zijn of worden genomen effectief zijn voor de informatiebeveiliging en de bescherming van de persoonsgegevens in het bijzonder. Van deze processen kunnen bevindingen worden opgetekend en die documenten behoren dan weer tot de “boeken en bescheiden” die elke organisatie en elk bedrijf verplicht is te administreren en te bewaren. Op basis van deze boeken en bescheiden doet een accountant dan ook verslag in het bestuursverslag dat jaarlijks dient te worden opgesteld.

***Functionele eis***

Met deze wettelijke en praktische overwegingen kunnen we de functionele bepalen:

Vanuit de wettelijke noodzaak moet de effectiviteit worden aangetoond van de maatregelen. Dat kan op een continue basis worden gedaan, maar dat kan te veel impact hebben op beschikbaarheid van verschillende systemen, vandaar dat een periodieke controle, bijvoorbeeld dagelijks in de nachtelijke uren als er minder activiteit op de servers plaatsvindt, ook een optie is. Het gaat er uiteindelijk om dat een regelmatige controle op afwijkingen de trend van de effectiviteit kan aangeven. Met deze periodieke controle zal ook de noodzaak van de ad hoc vraag om data te leveren tot het verleden gaan behoren.

Functionele eis:

Het systeem om de afwijkingen (de signalen) vast te stellen moet via een continu of periodiek geautomatiseerd proces verlopen.

1. Management letter PWC 2014, 2015 en 2016 [↑](#footnote-ref-1)
2. Burgerlijk Wetboek 2, artikel 391 lid 1, artikel 391 lid 5, artikel 393, lid 1, artikel 10, Burgerlijk Wetboek 3, artikel 15i [↑](#footnote-ref-2)
3. AVG, artikel 24 lid 1 en overweging 74 [↑](#footnote-ref-3)
4. Algemene Grondslagen Starreveld (2014), Bestuurlijke informatieverzorging, O.C. van Leeuwen, J.B.T. Bergsma [↑](#footnote-ref-4)