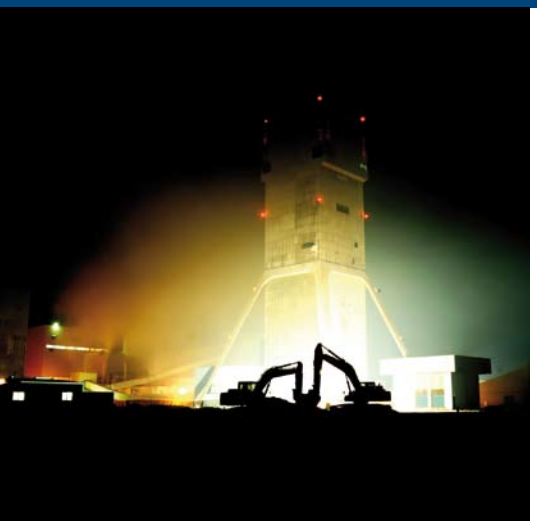


Facts to Value, beyond application security

Drs. M.A. Francken RE RA CISA
is als director werkzaam binnen diverse interne beheersingstrajecten, vanuit audit en advisory. Hierbij lag de nadruk op de IT controls in relatie tot de financiële verantwoording. Daarnaast is hij actief betrokken bij IT Attestation (SAS70) en External Audit support services binnen KPMG IT Advisory.

francken.marco@kpmg.nl

Ing. J.A.M. Hermans RE
is associate partner bij KPMG IT Advisory. Binnen KPMG is hij verantwoordelijk voor de dienstverlening op het gebied van informatiebeveiling. Hij heeft vele projecten op het gebied van Identity & Access Management uitgevoerd bij diverse grote organisaties in en buiten Nederland. Daarnaast leidt hij de internationale productontwikkeling van KPMG op dit terrein, wat heeft geleid tot de overkoepelende KPMG Identity & Access Management-methodologie.

hermans.john@kpmg.nl

G.H. Schreurs
is senior manager en geeft leiding aan het Forensic Technology team binnen KPMG Forensic. Hij heeft een uitgebreid track record opgebouwd op het vlak van computer forensics, data-analyse en e-discovery. Daarnaast heeft hij een gedeelde verantwoordelijkheid voor de Special Interest Group Data Analytics binnen de EMA-regio van KPMG.

schreurs.gerben@kpmg.nl

Drs. Marco Francken RE RA CISA, ing. John Hermans RE en Gerben Schreurs

Datamining, data-analyse, Facts to Value en 'fact based audits' zijn veelgehoorde kreten in deze tijd. De ontwikkelingen in IT maken een andere wijze van IT-audit in het kader van de jaarrekeningcontrole mogelijk. In dit artikel wordt stilgestaan bij het beoordelen van de IT-beheersing in de gehele keten, naast applicaties ook de technische infrastructuur. Met behulp van moderne tooling en verfijnde auditingtechnieken kan de daadwerkelijke inrichting van autorisaties en security settings efficiënter en effectiever worden beoordeeld. De auteurs stellen hierbij een integrale aanpak en visie voor.

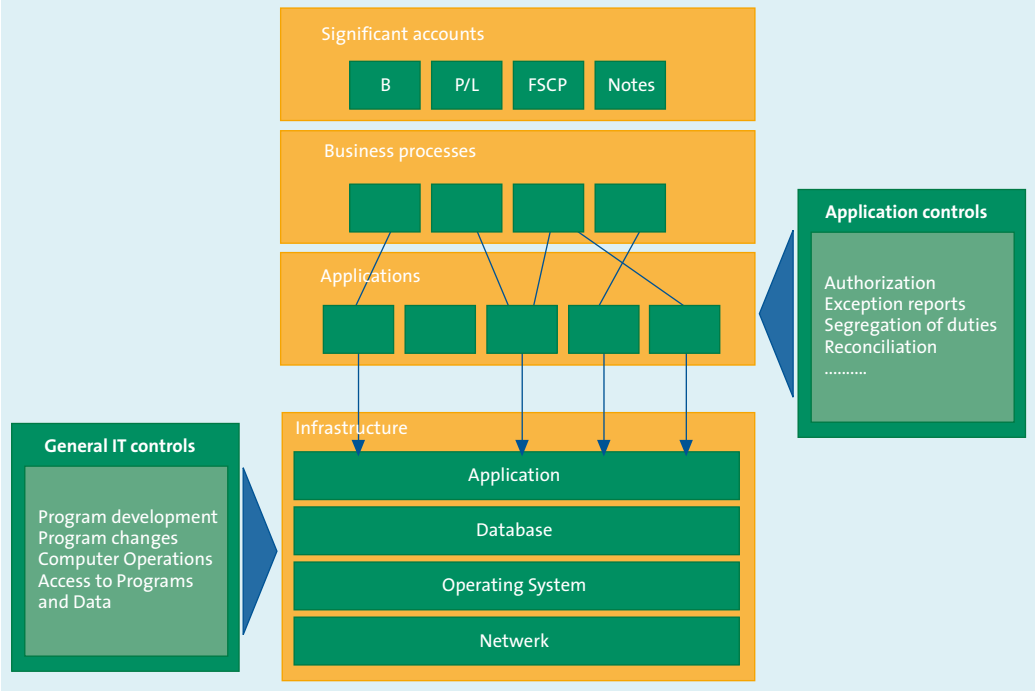
Inleiding

In de praktijk zien we dat de IT-audits verschillende accenten hebben over de jaren heen. Na de invoering van SOx zagen we een verhoogde aandacht voor IT in het kader van de jaarrekeningcontrole, waarbij het accent in eerste instantie lag op de IT general controls (hierna: ITGC). Na een sterkere focus op de application controls zien we nu een sterke nadruk op de zogenaamde Facts to Value-aanpak (Tole10). In deze aanpak wordt datamining onder andere toegepast om de goede werking van de application controls aan te tonen en gegevensgericht te controleren. De auteurs onderschrijven het belang van de focus op de primaire bedrijfsprocessen en willen in dit artikel stilstaan bij het belang om de IT-security in de gehele keten te blijven beoordelen en hierbij eveneens de efficiency en effectiviteit te verbeteren door het gebruik van datamining.

In de eerste paragraaf zal kort worden ingegaan op het belang van de IT-controls in het kader van de jaarrekeningcontrole, waarbij de keten kort wordt toegelicht. Vervolgens wordt verder ingegaan op de samenhang tussen de Facts to Value-aanpak en Access Governance en Automated Security Review. Het artikel wordt afgesloten met een conclusie.

Application en IT general controls

In het kader van de jaarrekeningcontrole staat de beheersing van de bedrijfsprocessen ten behoeve van de financiële verantwoording centraal. Hierbij is betrouwbaarheid een belangrijk aspect, maar ook continuïteit (BW9) en Fraude (ISA-240). De IT ondersteunt



Figuur 1. **Application controls en IT general controls en hun relatie met de bedrijfsprocessen.**

de betreffende processen en zal daarmee ook voldoende moeten worden beheerst in het licht van deze drie aspecten. In de huidige aanpak wordt een onderscheid gemaakt tussen:

1. de application controls (input – output controls, validation rules, toleranties, autorisaties, interfacecontrols, IT dependent controls…), en
2. de IT general controls (Change Management, Security Management, …).

Deze twee soorten controls hebben een (in)directe relatie met de bedrijfsprocessen en worden vanuit de geïdentificeerde risico's in de processen geselecteerd. Hierbij worden de application controls direct in de processen geïdentificeerd en zijn de ITGC gericht op de IT-componenten die de werking van deze application controls waarborgen. Deze relaties zijn in figuur 1 weergegeven.

De ITGC in scope hebben betrekking op de betreffende applicaties en de onderliggende IT-infrastructuur, zoals de database, het operatingsysteem en het netwerk. Deze IT-componenten ondersteunen de goede werking van de applicatiecontroles, die vanuit de bedrijfsprocessen zijn geselecteerd. Voor een goede beoordeling van de betrouwbaarheid van de applicaties en beveiliging van gegevens, is het van belang om de gehele keten en alle IT-componenten te overzien. Concreet voorbeeld: Binnen een ERP-applicatie kan de functiescheiding voldoende geborgd zijn. Indien de toegangsbeveiliging van de onderliggende database, bijvoorbeeld Oracle, niet op databaseniveau voldoende is geregeld maar men vertrouwt op de application controls, dan is het mogelijk dat gebruikers door middel van generieke applicaties zoals Microsoft Access of Excel toegang krijgen tot de database en deze zelfs kunnen muteren zonder de beperkingen van de ERP-applicatie.

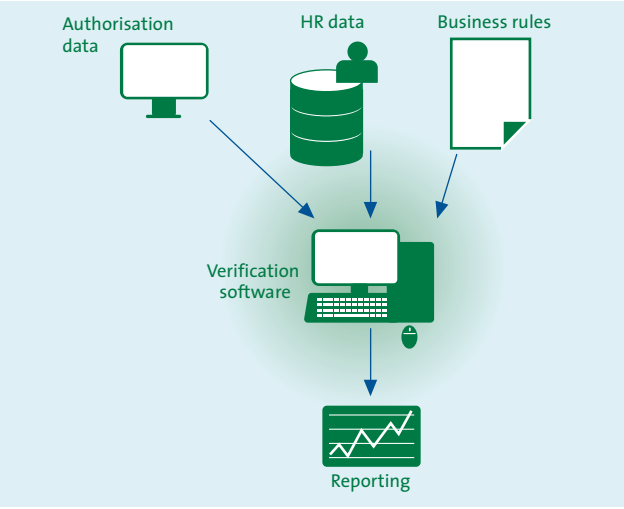
Deze aanpak is niet nieuw, maar de samenhang tussen de componenten zou ons inziens meer integraal moeten worden opgepakt. Dit geldt ook indien er niet (of gedeeltelijk) wordt gesteund op de aanwezige controls en er meer gegevensgericht wordt gecontroleerd. Indien gebruik wordt gemaakt van datamining voor het beoordelen van verbanden in de bedrijfsprocessen, is het van groot belang dat deze analyses worden uitgevoerd op alle data (volledigheid) en dat deze data integer zijn. Dit betekent dat de toegangsbeveiliging op de diverse IT-componenten adequaat moet zijn, zodat data leakage en datamanipulatie kunnen worden beperkt. In het kader van de jaarrekeningcontrole is het daarnaast van belang dat voldoende aandacht wordt gegeven aan continuïteit, waar wij nu niet verder op in zullen gaan.

Access Governance

Zoals aangegeven dienen data-analyses te worden uitgevoerd op alle data en dienen deze data integer te zijn. Hierbij ligt de nadruk op een goede toegangsbeveiliging op de diverse IT-componenten. Dit kan worden vastgesteld door alle relevante beheersingsmaatregelen te beoordelen, zoals de application controls en de ITGC, maar dit kan ook door een meer geautomatiseerde aanpak. Hierbij maken wij onderscheid tussen Access Governance en Automated Security Review.

Wij definiëren Access Governance als een proces waarbij met behulp van analytische tooling toegang tot applicaties en IT-platformen periodiek wordt beoordeeld. Enkele kenmerken van Access Governance zijn:

- correlatie en analyse van toegangsrechten op zowel netwerk-, database- als applicatielaag, alsmede tussen de verschillende lagen;



Figuur 2. **Het proces van Access Governance.**

- toegangsrechten kunnen worden verrijkt met HR en/of organisatiedata;
- analyse op basis van voorgedefinieerde bedrijfsregels:
  - generieke bedrijfsregels: regels van toepassing op toegangsrechten van alle componenten die onderzocht worden,
  - applicatiespecifieke regels: regels van toepassing op toegangsrechten binnen de applicatie (vaak de vertaling van functiescheidingsregels);
- off-lineanalyse, geen geautomatiseerde koppeling met de infrastructuur.

Deze aanpak (zie figuur 2) start met een voorbereidingsfase, waarin onder andere de relevante HR-data worden opgevraagd, alsmede de bedrijfsregels op het gebied van taken en verantwoordelijkheden. Op basis hiervan wordt inzicht verkregen wie wat zou mogen in de systemen. Vervolgens vindt er een validatie plaats van de ingerichte autorisaties op basis van specifieke verificatiesoftware, waarbij tevens wordt gekeken naar de mogelijkheden van de zogenaamde superusers. Ten slotte wordt hierover gerapporteerd aan het management.

Deze aanpak is in opzet niet anders dan voorheen, maar met behulp van de meest recente verificatiesoftware kan de daadwerkelijk ingerichte toegangsbeveiliging sneller en efficiënter worden verkregen, zonder de, normaal gesproken, handmatige verificatieslagen. Daarnaast helpt deze aanpak bij het verkrijgen van een volledig inzicht in alle ingerichte autorisaties over alle systemen, dus niet uitsluitend in één applicatie. Deze aanpak is dus op feiten gebaseerd (fact based) en heeft voor de auditor als voordeel dat:

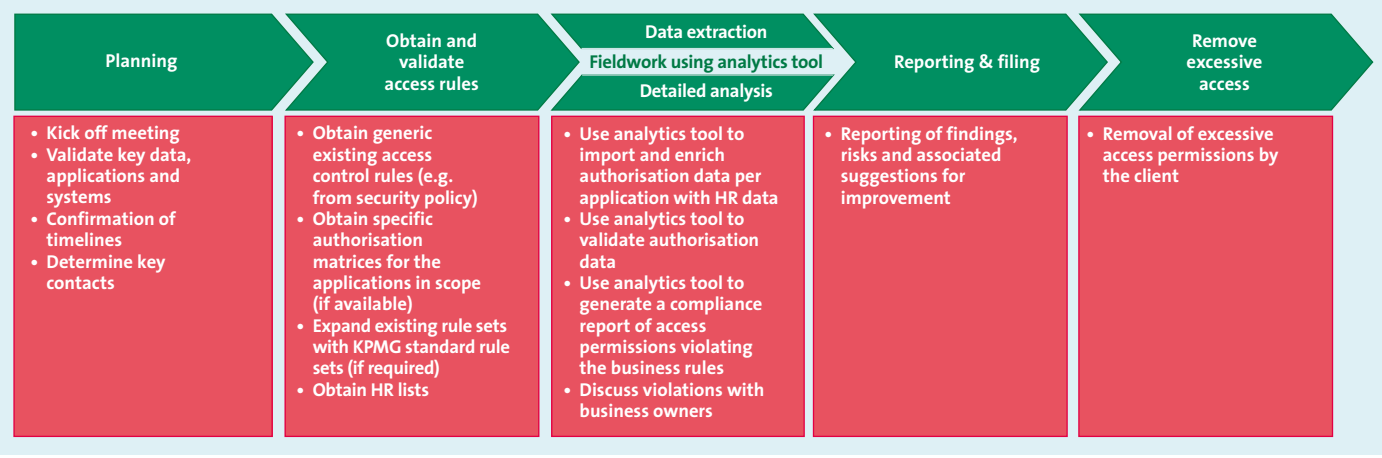
- er een beter overzicht aanwezig is van de daadwerkelijk ingerichte autorisaties, over alle systemen heen;
- de belangrijkste functiescheiding sneller kan worden getest;
- het uiteindelijke audit risk wordt gemitigeerd;
- de rapportage concreter is dan voorheen, gebaseerd op feiten;
- eventuele afwijkingen, ontstaan buiten de applicaties, eerder gesignaleerd kunnen worden.

De organisatie heeft er ook voordeel bij:

- Ze krijgt gedetailleerd inzicht in de inrichting en werking van haar functiescheiding in de systemen.
- Deze rapportages helpen om de interne beheersing verder te versterken en het bedrijfsrisico te verlagen.
- De rapportage is specifiek en toegesneden.

De aanpak en planning ziet er op hoofdlijnen uit als weergegeven in figuur 3.

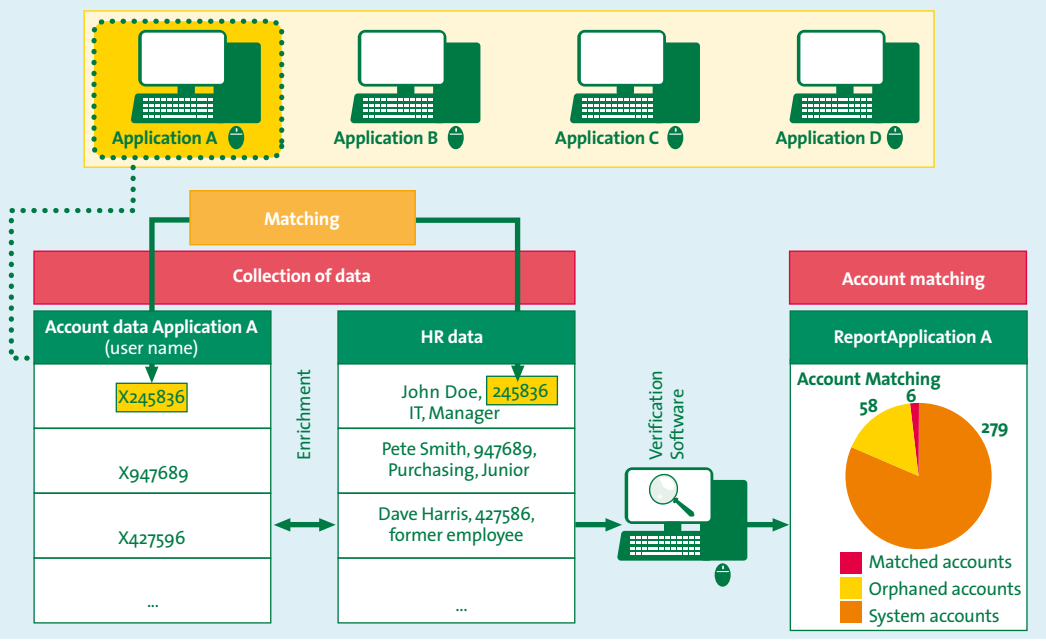
Access Governance is volgens ons noodzakelijk als randvoorwaarde om vervolgens met behulp van datamining verbanden te leggen en de bedrijfsprocessen te beoordelen. Met behulp



Figuur 3. **Access Governance: aanpak en planning.**

van de huidige verificatiesoftware, zoals Aveksa, Bhold, Oracle en Sailpoint, kan dit efficiënter dan voorheen.

Enkele voorbeelden van concrete Access Governance reviews



Figuur 4. **Voorbeeld 1: het analyseren van alle accounts van een applicatie.**

Het eerste voorbeeld (zie figuur 4) betreft het analyseren van alle accounts van een applicatie met als doel te verifiëren of alleen personen die werkzaam zijn binnen de organisatie toegang hebben tot de applicatie.

Deze review wordt uitgevoerd door het importeren van de accountdata van de applicatie alsook de HR-data met daarin alle medewerkers werkzaam voor deze organisatie. De verificatiesoftware zal op basis van de matching van de accountdata met de HR-data bepalen welke accounts niets voldoen aan dit policy-statement (bedrijfsregel). De accounts die niet voldoen aan deze regel zijn enerzijds 'orphaned accounts' (accounts van personen die niet meer werkzaam zijn) of anderzijds system accounts (niet-persoonlijke accounts).

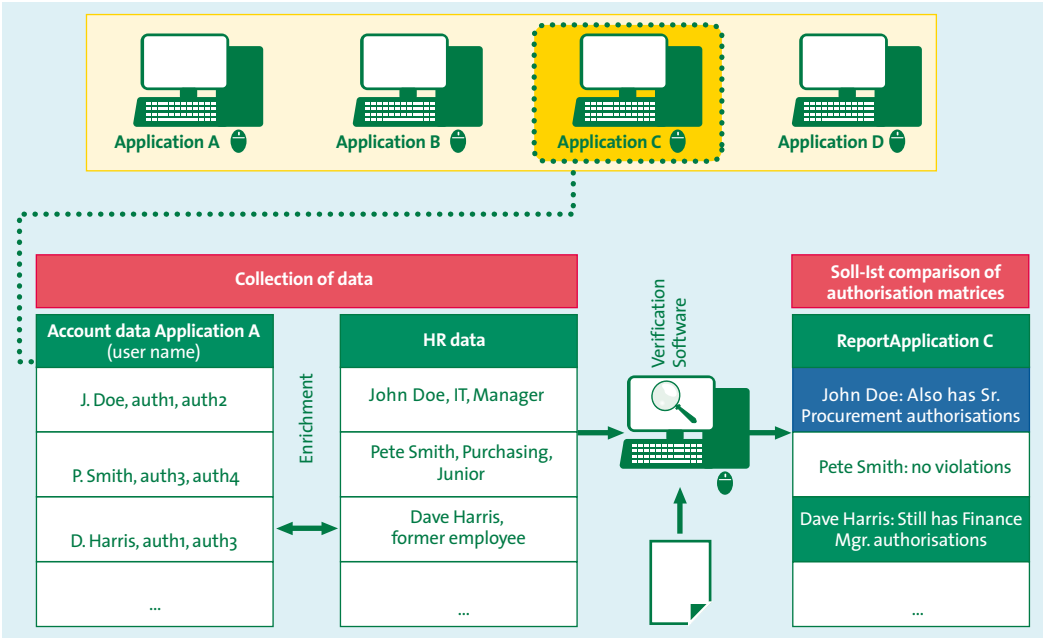
Het tweede voorbeeld (zie figuur 5) betreft het analyseren van de fijnmazige toegangsrechten (authorisation data) van een bepaalde applicatie op basis van vooraf gedefinieerde bedrijfsregels, zoals die zijn vastgesteld in een autorisatiematrix. Op basis van de analyse zal een rapportage worden gegenereerd van alle personen (die gematcht worden op basis van accounts), waarvan de toegangsrechten niet in overeenstemming zijn met de gewenste rechten ('Soll-Ist' vergelijking).

Het toepassen van Access Governance betekent ons inziens dat de ITGC, dat wil zeggen de procedures zoals wijzigingsprocedures en het toekennen van rechten in de systemen, niet langer afzonderlijk hoeven te worden beoordeeld door uitsluitend de beheersingsmaatregelen in de processen te beoordelen. Volgens ons kan de integriteit worden aangetoond door tevens datamining toe te passen op de ingerichte autorisatie op de diverse systemen en IT-platformen. Aangevuld met het geautomatiseerd beoordelen van de security baselines, kan zo voldoende audit evidence worden verkregen. Kortom, een efficiënte beoordeling door een mix van preventieve beheersingsmaatregelen en (detectieve) datamining.

Automated Security Review

Naast het beoordelen van de ingerichte toegangsbeveiliging over de applicaties heen, zal moeten worden vastgesteld dat de onderliggende IT-componenten, zoals de netwerk- en databasecomponenten, geen grote gaten bevatten. Indien er mogelijkheden zijn dat ongeautoriseerde personen van (buiten) de organisatie zelf toegang verkrijgen en/of gevoelige data kunnen zien/muteren, dan loopt de organisatie een risico op data leakage, fraude, privacyovertredingen, etc.

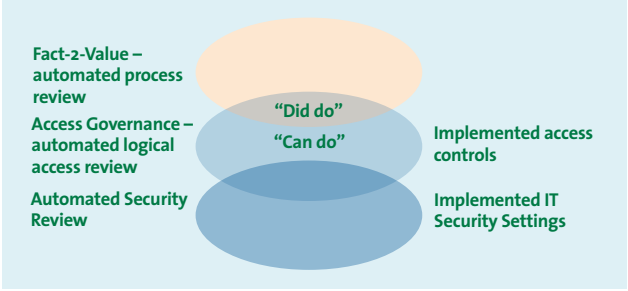
In navolging van het toepassen van dataminingtechnieken bij het beoordelen van de toegangsbeveiliging (Access Governance) zien we een dergelijke aanpak ook bij het beoordelen van de belangrijkste IT-beveiligingsrisico's binnen de technische infrastructuur. Op basis van de relevante bedrijfsapplicaties en data in scope, wordt vastgesteld welke IT-componenten in scope zijn waar specifiek wordt gekeken naar configuratie-instellingen, zoals password settings, patch management, en monitoringparameters. Dit gebeurt door middel van audit scripts, fact based, waarbij de uitkomsten worden vergeleken met de geldende policies, waardoor een indruk wordt verkregen van de feitelijk geïmplementeerde ITGC. Door middel van 'automated security testing' wordt vastgesteld dat de gehele securityarchitectuur voldoende is, over de diverse IT-infrastructuurlagen heen, zoals



Figuur 5. **Voorbeeld 2: het analyseren van fijnmazige toegangsrechten van een applicatie.**

de applicatie, database, netwerk, storage en middleware. Zeker in de huidige wereld met SOA-achtige oplossingen, virtualisatie, off site storage en bussen, is het van groot belang dat het gehele IT-landschap wordt beoordeeld. Alleen kijken naar de bedrijfsprocessen en -stromen, op basis van datamining, is ons inziens te beperkt. De risico's daarbuiten zullen ook onderdeel van de totale scope moeten zijn van de auditor. Dit betekent niet dat alle IT-componenten dezelfde aandacht moeten krijgen, ook hier is een risicoaanpak van belang. Het gebruik van datamining om de daadwerkelijke inrichting van autorisaties, over de applicaties heen, en de beveiligingsinstellingen te beoordelen, maakt het mogelijk op een efficiënte wijze toch de vereiste zekerheid en toegevoegde waarde te realiseren.

Samenvattend zien we hier een duidelijke afhankelijkheid om naast de data-analyse op de processen, eveneens vast te stellen wat men binnen de gehele (relevante) IT-infrastructuur kan en heeft gedaan, op het gebied van toegangsbeveiliging. De samenhang tussen de processen (Facts to Value) en de beveiliging van de relevante infrastructuur (Access Governance en Automated Security Review) zal ons inziens moeten worden beoordeeld, waarbij zowel 'did do' (wat heeft men daadwerkelijk gedaan in de systemen, data-analyse) en 'can do' (wat kan men, instellingen) relevant zijn.



Figuur 6. **Het proces in samenhang weergegeven.**

Conclusie

In de huidige aanpak van de jaarrekeningcontrole kan men niet om de IT-systemen heen, dat is inmiddels wel duidelijk. Dat de aanpak efficiënter en effectiever kan, is ook duidelijk. Zo zien we een tendens richting 'fact finding'-achtige oplossingen met behulp van diverse tooling. Deze aanpak lijkt zich voornamelijk te richten op het aantonen van verbanden in de bedrijfsprocessen en onderliggende datastromen en minder op de risico's in het gehele IT-landschap en onderliggende IT-platformen. Dat is ons inziens niet terecht. De integriteit van de data is een belangrijke randvoorwaarde, voordat überhaupt een conclusie kan worden getrokken over deze data. Met behulp van dataminingtechnieken kan de daadwerkelijke inrichting van de toegangsbeveiliging worden beoordeeld over de diverse applicaties en IT-platformen heen (Access Governance) en kan worden aangetoond dat de onderliggende IT-infrastructuur geen relevante zwakheden kent waardoor derden alsnog ongeautoriseerd data kunnen zien en/of wijzigen. Naast Facts to Value is er ook een duidelijke behoefte en noodzaak om de geïmplementeerde toegangsbeveiliging en security settings te beoordelen. Alleen zo kan daadwerkelijk worden aangetoond wie welke transactie heeft uitgevoerd in de betreffende geautomatiseerde bedrijfsprocessen.

Literatuur

[Tole10] Drs. Peter van Toledo RE RA, drs. Gideon Lamberiks RE en Quintra Rijnders MSc RA, *Facts to Value, data omzetten in toegevoegde waarde*, Compact 2010/1.