Continuous Auditing

Continue in control met Continuous Auditing.
Door Bart de Best

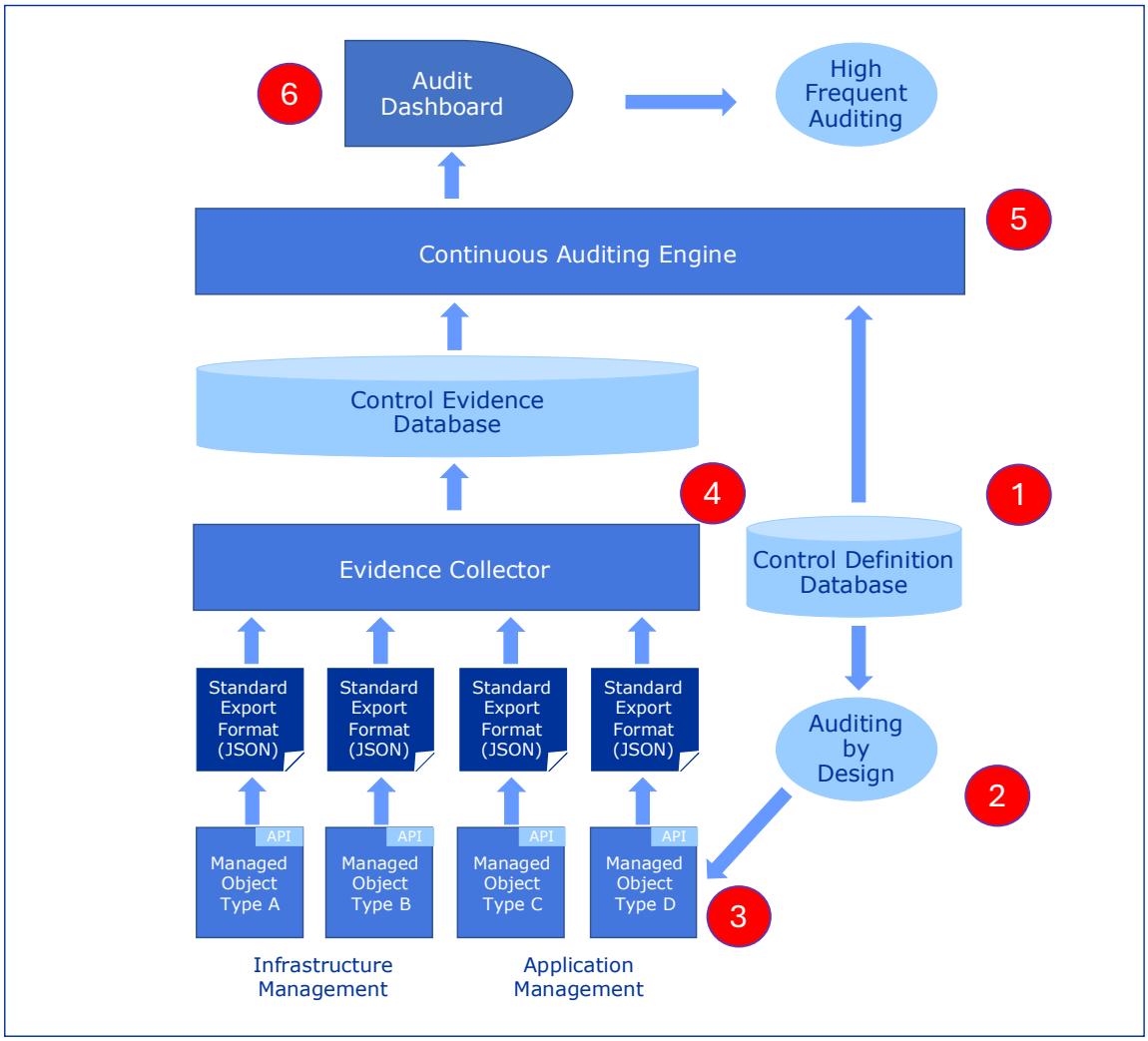
Context:
Dit verhaal is gebaseerd op een opdracht van een uitzendbureau om een hoge frequentie te bieden van control monitoring van interne en externe requirements zoals privacy, beveiliging en wet- en regelgeving.

Uitdaging:
De uitdaging van deze opdracht was dat alleen op jaarlijks niveau middels manuele evidence (bewijslast) met moeite kon worden aangetoond dat de IT serviceverlening op orde was. Vaak waren controls niet gedefinieerd en ontbrak de evidence. Er was geen groot budget om een radicale verbetering door te voeren. Alle verbeteringen moest incrementeel en iteratief worden vormgegeven na een goedkeuring.

Oplossing:
De oplossing voor deze opdracht is gevonden in het concept van Continuous Auditing. Deze blog bespreekt hoe Continuous Auditing is toegepast aan de hand van de volgende stappen:

1. Bepaal de controls
2. Bepaal de ontwerpcriteria
3. Bepaal de evidence
4. Bepaal de evidence collector
5. Bepaal de continuous auditing engine
6. Bepaal het dashboard

De totaal oplossing is weergegeven in figuur 1. De stappen 1 tot en met 6 zijn eerst manueel doorlopen. Daarna is op basis van de frequentie van de controls en de tijd die het vereist om deze te meten bepaald hoe de monitoring van de control te digitaliseren is.



Figuur 1, Continuous Auditing concept.

1. Bepaal de controls

De control definitie database is de kern van deze auditaanpak. Controls zijn de tegenmaatregelen van de risico's die beheerst dienen te worden. De risico's zijn verkregen uit diverse bronnen zoals:

- Risico's vanuit business doelen
- Risico's van business value stream doelen
- Risico's vanuit audits
- Risico's vanuit wet & regelgeving
- Risico's vanuit normkaders zoals ISO 27001
- Risico's vanuit change management en service level management

De tegenmaatregelen zijn toegekend op basis van de classificatie van de risico's te weten:

- Modify: bedenk een tegenmaatregel (eliminatie of mitigatie risico)
- Avoid: bedenk hoe het risico te vermijden is (b.v. notebook alleen op kantoor)
- Share: deel de risico's (b.v. het afsluiten van een verzekering)
- Retain: neem het risico (geen actie nodig)

Alleen de risico's de moeten worden beheerst (modify) zijn voorzien van een tegenmaatregel. Tevens is voor de controls de informatievoetprint bepaald die het mogelijk maakt om vast te stellen of de tegenmaatregel effectief is. Tenslotte is de frequentie van de meting in de control vastgelegd. ISO 27001 is de belangrijkste bron van controls gebleken.

2. Bepaal de ontwerpcriteria

De ontwerpcriteria betreffen zowel het ontwerp als de ontwerp-requirements die borgen dat de tegenmaatregel effectief en meetbaar is. Deze ontwerpcriteria worden meegenomen in de acceptatiecriteria van de product backlog items. Een voorbeeld is schaalbaarheid van een infrastructurele voorziening zodat piekbelastingen de toegankelijkheid van informatie niet verstoord. Een ander voorbeeld is de vertrouwelijkheid van data te borgen door de invoering van een two-factor-authenticatie.

3. Bepaal de evidence

Op basis van de control definitie is bepaald welke te beheren objecten (managed objects) in scope zijn voor de risicobeheersing. Dit is gedaan door het opstellen van een portfolio van applicatie services en infrastructuur services en vervolgens per item vast te stellen welke controls van belang zijn. Het aantal controls per item bleek te overzien te zijn.

Daarna is bepaald op welke wijze de informatievoetprint, zoals gedefinieerd in de control, uit het managed object te extraheren is en in welk formaat dat kan. Lang niet altijd blijkt dit met een REST API te kunnen, maar is het wel mogelijk gebleken de informatie aan het object te onttrekken. Middels een microservice is deze interface wel te bouwen. Een voorbeeld is het uitlezen van een firewall om vast te stellen of er onterecht poorten openstaan. Of het uitlezen van een applicatie om vast te stellen of deze verdachte transacties bevat.

4. Bepaal de evidence collector

De evidence collector haalt periodiek de evidence op van de managed objecten. In plaats van een pull mechanisme is uiteraard ook een push mechanisme mogelijk. Zolang de frequentie van de collectie van de evidence maar overeenkomstig is met de controls. Op de korte termijn is gekozen voor een manuele collector op basis van verschillende frequenties van collectie die in de controls is gedefinieerd.

5. Bepaal de continuous auditing engine

De audit engine is een eenvoudige stap. Er hoeft alleen een verificatie te worden verricht tussen de control definitie en de verzamelde evidence. Ook deze is stap is eerst manueel uitgevoerd om vast te stellen dat de logica correct werkt.

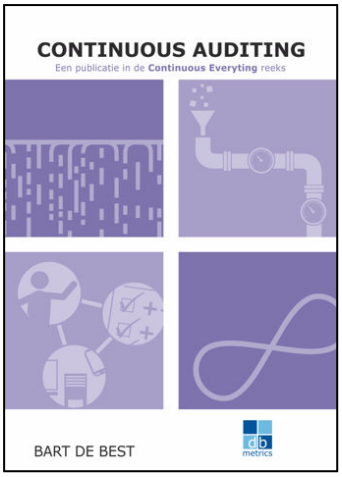
6. Bepaal het dashboard

Het dashboard vormt de rapportage over de resultaten. De periodiciteit is bepaald door de controls. Omdat de eerste aanzet manueel is uitgevoerd moest ook de frequentie van de publicatie op het dashboard laag worden gehouden. Met elke stap van digitalisering is de frequentie per control verhoogd.

Deze eenvoudige aanpak van het continu meten van het in control zijn is erg aantrekkelijk omdat de mate van control continue wordt bepaald. Deze vorm van auditing is daarmee een mooi voorbeeld van Continuous Auditing.

Door Bart de Best
DutchNordic.Group

By Bart de Best
DutchNordic.Group



https://www.dbmetrics.nl/ce-nl/continuous-auditing-nl/