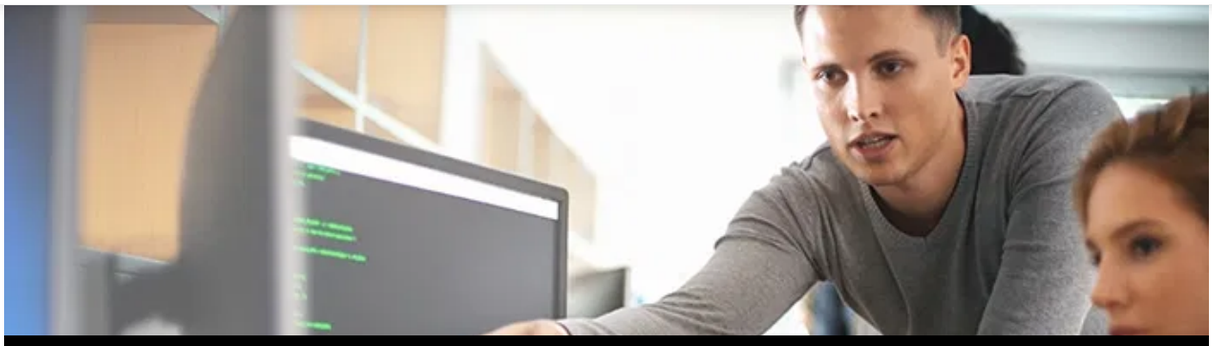
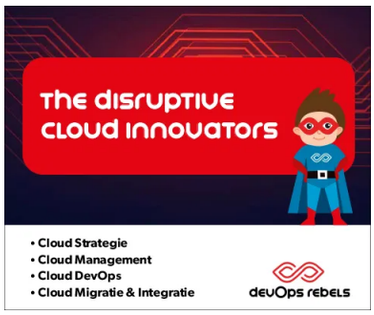


Business

Continuous delivery vraagt om continuous auditing

Door **Security by Design Guild** - 19 april 2021



Security controls vereisen een steeds kortcyclischer aandacht. Binnen het vakgebied continuous auditing is hier invulling aan gegeven voor zowel het voortbrengingsproces als de productieomgeving, in analogie met continuous integration en continuous delivery van software. De wereld van informatievoorziening verandert zo snel dat een auditperiode van een jaar wellicht onvoldoende vertrouwen geeft in de veiligheid van deze informatievoorziening. Hoe kun je grip houden op het steeds veranderende IT-landschap? Is continuous auditing een haalbare oplossing?

Hieronder gaan we in op drie methoden voor integratie van continuous auditing in de CI/CD secure-pipeline. Hoewel er bij alle drie de methoden nog uitdagingen zijn en problemen die moeten worden aangepakt, zijn de resultaten veelbelovend. Ze brengen auditing in lijn met de snelheid van ontwikkelen met DevOps en helpen daarmee ondernemingen continu in control te blijven en hun time to market te behouden. Het doel van dit artikel is om concept continuous auditing uit een te zetten.

Nieuwe, agile delivery paradigma's leiden tot een steeds sneller veranderend IT-landschap. Door deze dynamiek is het niet meer voldoende om periodiek, achteraf, audits uit te voeren op beveiligingsbeleid. Om het tempo van continuous integration en deployment bij te houden is controle op continue basis nodig voor elke wijziging in het IT-landschap. Het concept van continuous auditing zou dit probleem kunnen oplossen, maar hoe haalbaar is het?

Definitie van het probleem

Traditionele auditinstituten worden om een aantal redenen geconfronteerd met nieuwe technologie waar de audit nog onvoldoende mee rekening houdt voor de certificering van informatiebeveiliging. Ten eerste is de huidige frequentie van een auditcyclus één keer per jaar met een terugblik, wat te lang is voor de snel veranderende IT-landschappen. Verder leidt het toepassen van agile-ontwikkeling tot hoogfrequente kleine veranderingen die niet altijd worden getoetst op de effectiviteit van controls.

Maar ook interfaces tussen informatiesystemen, clouddiensten of interfaces tussen clouddiensten zijn flexibel en veranderen zeer snel. En ten slotte kunnen bedrijven die continu in control willen komen en blijven, niet aantonen dat hun IT-landschap aan de regelgeving voldoet en/of kwetsbaarheden worden blootgelegd. Dit betekent dat de effectiviteit van de beheersing van informatiebeveiliging niet direct bekend is, deze wordt pas bij de audit bevestigd.

Oplossingen

Het antwoord op dit probleem is om de informatiebeveiliging continu te testen. Dit betekent dat de effectiviteit van de controles op elk moment bekend is. Er zijn drie (deel) oplossingen die bijdragen aan een oplossing en die elkaar versterken, te weten: verhoging van de auditfrequentie, security by design en continuous auditing.

1. Hogere frequentie van auditing

De eerste en eenvoudigste manier om het probleem op te lossen, is door de frequentie van een audit te verhogen, bijvoorbeeld maandelijks in plaats van jaarlijks. Dit kan worden gerealiseerd door vaker *evidence* te verzamelen en verspilling bij het verzamelen en verifiëren van evidence te verminderen.

Beperkingen

Deze oplossing is relatief eenvoudig toe te passen, maar is aanzienlijk duurder dan een jaarlijkse audit. Ook is een maand nog steeds een lange periode, dus op zichzelf lost de oplossing het probleem niet op.

2. Security by design

De tweede oplossing voor het probleem is de security by design-aanpak. Dit concept gaat over het voorkomen van gebreken in de informatiesystemen door de vereiste controls op te nemen in de volledige levenscyclus van het informatiesysteem. Deze controls zijn gebaseerd op een risicoanalyse van informatiebeveiliging. Dit omvat vier geïntegreerde valuesystems die de effectiviteit van de controls proactief moeten waarborgen, bekend als DVS, SVS, ISVS en BVS.

Development Value System (DVS)

DVS is een value system waarin het ontwerpen en bouwen van de software plaatsvindt. De controls voor informatiebeveiliging maken deel uit van het ontwerp, zoals Rest API's die een oauth2-authenticatiemethode gebruiken.

Service Value System (SVS)

SVS is een value system waarin het onderhoud en de inzet van de software plaatsvindt. De CI / CD Secure Pipeline bevat geautomatiseerde controles voor informatiebeveiliging, bijvoorbeeld het scannen van de code op het opnemen van kwaadaardige software.

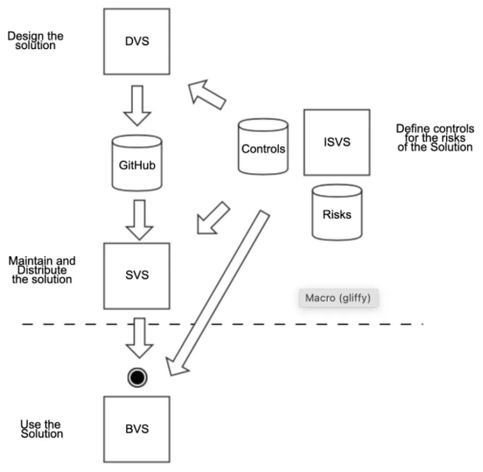
Information Security Value System (ISVS)

ISVS is een value system waarin de definitie van de informatiebeveiligingscontrols plaatsvindt, evenals de verificatie van de effectiviteit van deze controls in de DVS-, SVS- en BVS-waardesystemen zoals de 114 controls van ISO 27001: 2013.

Business Value System (BVS)

BVS is een value system waarin het informatiesysteem op een veilige manier wordt gebruikt zoals geëxporteerde spreadsheets en rapporten.

Alle value systems worden gedefinieerd in termen van value streams die zijn ontworpen door het gebruik van use case-diagrams en use cases. Ze zijn bijvoorbeeld geschreven in de Gherkin-taal om het gedrag van de use case uit te drukken. Hierdoor blijven de value streams agile, worden knelpunten opgelost en wordt verspilling verminderd om de waarde voor de business (BVS) te vergroten.



Value systems

Deze integratie van waardesystemen is vergelijkbaar met de Automobiel industrie. Zo is DVS de fabriek van de auto's waarbij de beveiliging is geïntegreerd in het ontwerp van de auto zoals de aerodynamica, het frame, de aanrijdingsdetectie, et cetera. Het SVS is de garage waarin de auto wordt gecontroleerd op effectiviteit van bedieningselementen zoals de wielen, de remmen en waar kwetsbaarheden worden weggenomen. Het ISVS staat voor de controls die wettelijk verplicht zijn en periodiek worden gecontroleerd door een garage en gerapporteerd aan de overheid. En ten slotte wordt het BVS vertegenwoordigd door de beveiligingsmaatregelen die de bestuurder naleeft om alleen te rijden als hij nuchter is en niet te moe is om te rijden.

De integraties van de value systems garanderen de effectiviteit van de controls. Bijvoorbeeld de value stream van de IT-servicecontinuïteit van de SVS in relatie tot de ISVS waarin noodherstel vereist is. De controls zijn gebaseerd op geïdentificeerde informatiebeveiligingsrisico's. Dit resulteert in een proactieve manier van informatiebeveiligingsbeheer.

Deze proactieve security by design-aanpak kan worden gebruikt in zowel agile-omgevingen als niet-Agile-omgevingen. Deze aanpak is ontwikkeld bij Plint AB (Göteborg) en wordt gepromoot in Plint-webinars samen met een publicatie in de nabije toekomst.

Beperkingen

Organisaties maken steeds vaker gebruik van informatieservices die in de cloud worden aangeboden. Dit brengt ook (veiligheids) risico's met zich mee. Deze informatiesystemen zijn black boxes die tot op zekere hoogte kunnen worden gecontroleerd, maar uiteindelijk black boxes blijven. Dit betekent dat de effectiviteit van de controls die worden verkregen door software en hardware van leveranciers te kopen, getest moet worden.

In deze cloud omgevingen wordt dit testen echter nog moeilijker als blackboxes in de cloud gestapeld worden (bijvoorbeeld IaaS, PaaS en SaaS). Uiteraard zijn er SLA-clausules die transparantie vereisen van de blackboxes en wijzigingsrapportage zijn tot op zekere hoogte mogelijk. Ook kunnen er in de SLA eisen worden opgenomen zoals de ISO 27001:2013, de ISAE 3402, en certificeringen op het gebied van cyber security, zoals NOREA CSA & ICR.

3. Continuous Auditing

De derde optie is om het volledige auditproces te automatiseren door alle informatie te extraheren uit de managed objects die worden gebruikt om het informatiesysteem als een service aan klanten aan te bieden. De ontvangen informatie is in real-time, indien een afwijking wordt geconstateerd wordt direct een signaal afgegeven en mogelijk een correctieve actie. De mogelijkheid tot informatie-extractie moet echter worden gerealiseerd in alle relevante oude en nieuw te realiseren componenten.

Beperkingen

Alle componenten van een service moeten hun informatie exporteren in een standaard informatiestructuur (JSON-formaat). De vraag is wat de kosten zijn om deze export per product mogelijk te maken en wat uiteindelijk de daadwerkelijke dekking van deze objecten is. Ook het begrijpen van de componenten van een service is niet eenvoudig. Voor services in de cloud is dit zelfs niet mogelijk tenzij ondersteund door de leverancier van de internetdienst.

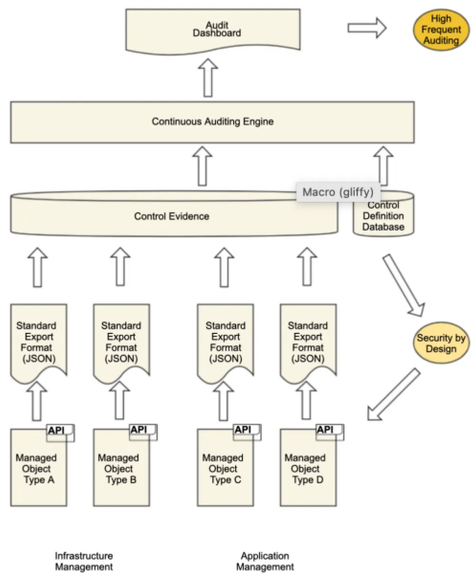
"DE EFFECTIVITEIT VAN DE BEHEERSING VAN INFORMATIEBEVEILIGING IS NIET DIRECT BEKEND, DEZE WORDT PAS BIJ DE AUDIT BEVESTIGD"

Continuous auditing, de oplossing

Alle drie gedefinieerde alternatieve oplossingen hebben hun waarde en kunnen ook worden gecombineerd. Maar het laatste alternatief wordt door veel organisaties erkend als de *silver bullet*. We vervolgen hier met uitleg van het concept van continuous auditing en sluiten af met een conclusie.

Continuous auditing concept

Het concept van continuous auditing wordt weergegeven in de figuur hieronder.



Het concept van continuous auditing

Managed objects

Infrastructuurbeheer bestaat uit de hardware (netwerkcomponenten, server blades, et cetera) en systeemsoftware (besturingssystemen, databasebeheersystemen, et cetera). Applicatiebeheer bestaat uit de componenten die bedrijfslogica bevatten zoals applicaties, databases, rapporten, et cetera. Al deze objecten moeten worden beheerd en er moeten controls worden toegepast zoals authenticatie en autorisatie.

Ook de services die worden geleverd op basis van het *managed object* kunnen als managed object worden beschouwd.

Control evidence export

De doeltreffendheid van de control van alle managed objects die deel uitmaken van het informatiesysteem moet worden geverifieerd en er moet dus informatie worden geëxtraheerd uit de managed objects.

Zowel de controls als de informatie die nodig is om de effectiviteit van de control te verifiëren, verschilt echter per managed object. Zo is bijvoorbeeld de geëxporteerde informatie van een firewall niet hetzelfde als voor een database. Voor een firewall moeten er controls zijn die de effectiviteit van de configuratie van de poorten en routes verifiëren. Deze controls zijn niet van toepassing op een database. In een database worden echter bedrijfsgegevens opgeslagen die controls vereisen om de effectiviteit van toegangsrechten te verifiëren.

Control database

De business rules voor het testen van de effectiviteit van de controls worden vastgelegd in de control database. Per type managed object wordt de informatie voor de bedrijfsregel gedefinieerd en geprotocolleerd. Ook zijn niet alle managed objecten even gevoelig voor een risico en hoeven ze dus niet door een control te worden getest.

Control evidence

Alle verzamelde informatie wordt centraal opgeslagen. De informatie is gestandaardiseerd en eenvoudig te toetsen aan de controls die zijn opgeslagen in de control database.

Continuous auditing engine

De informatie in de controle evidence database moet worden geanalyseerd, gefilterd en geaggregeerd om de informatie te vergelijken met de relevante controles in de control database. Dit wordt gedefinieerd in de engine voor continuous auditing.

Auditing dashboard

De effectiviteit van de controls wordt gevisualiseerd op het control dashboard. Er zijn meerdere weergaven mogelijk om de gegevens te bekijken, zoals de effectiviteit per value system, value stream, informatieservice en managed service en ten slotte de effectiviteit volgens ISO 27001: 2013 control.

Wat zijn de uitdagingen?

Het concept van continuous auditing kent een aantal valkuilen:

Vereiste vaardigheden

De decompositie van de service naar componenten moet worden uitgevoerd om de managed objecten voor een service te bewaken. De kennis om deze services te analyseren vereist vaardigheden die niet altijd beschikbaar zijn (full stack engineer / E-shaped people).

Gebrek aan evidence

Het is niet altijd mogelijk om de benodigde evidence uit de managed objects te exporteren.

Handmatige controls

De toewijzing van de controls aan de managed objects moet worden gedefinieerd. Voor standaardproducten op de markt kan dit één keer worden gedaan, maar voor maatwerkoplossingen moet dit handmatig gebeuren.

Kwetsbaarheid

Net als bij alle monitoring tools concentreert deze benadering alle niet-conforme informatie op één plaats, wat een nieuwe kwetsbaarheid is die moet worden beschermd.

Het concept van security by design kan deze valkuilen compenseren. Ook het selecteren van managed objects voor een informatieservice op basis van de gedefinieerde controles is een goede proactieve maatregel.

“CONTINUOUS AUDITING IS GEEN HYPE, HET IS EEN BEWEGING VAN DE MARKT

DIE DE OUDE MANIER VAN WERKEN ZAL VERANDEREN”

Conclusie

Het concept van continuous auditing is geen hype, het is een beweging van de markt die de oude manier van werken zal veranderen. Het bevindt zich echter nog in de beginfase; het concept is vrij onvolwassen. De toepassing van continuous auditing moet op de roadmap worden geplaatst van alle organisaties die hun time-to-market van oplossingen op de markt willen behouden of verbeteren.

De oplossing van continuous auditing heeft potentie, maar vereist een aantal randvoorwaarden:

- De behoefte of visie om in control te zijn (informatiebeveiligingsrisico’s die moeten worden beheerd)
- Het vermogen om control vanuit standaarden te vertalen naar de context van de organisatie (ISO 27001: 2013 of andere kaders)
- Het vermogen om de informatiebehoefte te definiëren om de effectiviteit van een control te valideren
- De mogelijkheid om services te vertalen naar de onderliggende managed objects (te beheren objecten zoals applicaties en infrastructure) en de juiste controls te selecteren voor de risico’s van deze managed objects.
- De mogelijkheid om evidence van de effectiviteit van de controls van de managed objects te exporteren. Het verzamelen van evidence om de effectiviteit te valideren en te visualiseren.

In het volgende artikel in deze serie gaan we dieper in op dit concept door voorbeelden te laten zien van implementaties van onderdelen van de ISO 27001: 2013 controls. We geven ook een vooruitblik welke tools kunnen helpen om het concept van continuous auditing te ondersteunen.

Dit artikel is mogelijk gemaakt door Bart de Best, Dennis Boersen (Argis IT), Freek de Cloet (smartdocuments), Jan-Willem Hordijk, Willem Kok (Argis IT) en Niels Talens – www.nielstalens.nl

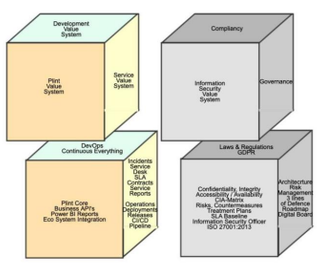
Waarom One Agile Way of Working?

Plint AB verleent lokalisatieservices in de mediawereld: het bedrijf maakt media toegankelijk door vertalingen te verrichten voor bedrijven zoals Netflix. In deze wereld is het belangrijk om snel in te springen op behoeften van contentaanbieders. Hierbij kijkt Plint steeds naar hoe het beste waarde kan worden toegevoegd aan de business value streams van de klant. Mediabestanden moeten niet alleen snel en goed vertaald worden, ook de beveiliging is een belangrijk aspect voor mediabedrijven. Daarom heeft Plint AB de One Agile Way of Working opgezet.

Plint is een informele organisatie die vooral business doet op basis van relaties en samenwerkingsverbanden. Bij het groeien van het bedrijf bleek het steeds lastiger om de vragen van verschillende klanten goed te definiëren en te realiseren. Zo kostte het inwerken van een nieuwe IT medewerker in een half jaar.

Maar ook de snelheid van het realiseren van nieuwe functionaliteit daalde steeds verder terwijl de fragiliteit van informatiesystemen toenam door de snelle ad hoc wijzigingen die werden doorgevoerd. Dat de technische debt torenhoog was valt te raden. Er was behoefte aan een business DevOps aanpak om het tij te keren. Daarbij is gekozen voor de value system aanpak waarbij het werk van de hele organisatie is vertaald naar value stream die uitgewerkt zijn in use case diagrams en use cases.

Het eenvoudigste laat dit zich visualiseren aan de hand van een kubus, zoals linksboven is weergegeven in de figuur hieronder. Deze kubus representeert de Plint organisatie. Van een kubus zijn alleen de drie zijden te zien en dat is ook zo voor de klant van Plint. Voor Plint zijn dit het Plint Value Systems (PVS) die de business value streams vormen (oranje). Service management is invulling gegeven aan de hand van het Service Value System (SVS) op basis van ITIL 4. En de derde is het Development Value System (DVS) dat invulling is gegeven aan de hand van DevOps en agile scrum.



De Value system view, klik/tap om te vergroten

Rechtsboven is de achterkant van de kubus weergegeven. Deze drie zijden worden gevormd door de aspecten Information Security Value System (ISVS), compliancy en governance. De termen die bij deze zes zijden van de kubus horen zijn in de tweede rij kubussen weergegeven.

Door invulling te geven aan deze value systems is het Plint gelukt om een Plint Factory vorm te geven die inzicht heeft in de werkwijze van de business (PVS) en de behoefte vanuit deze value stream te realiseren door een integratie van DVS, SVS en ISVS value systems.

Het resultaat van deze ordening van werk maakte het mogelijk om grip te krijgen op het veranderproces zodat ruimte ontstond om de fragiliteit en technical debt te bestrijden. Deze journey heeft twee jaar gekost en zal nog wel een tweetal jaren nodig hebben. Het resultaat is echter verbluffend, met als bewijs de certificering van Plint voor ISO 27001:2013 in 2020.

Wat is ISO 27001?

ISO is het instituut voor interne standaardisatieorganisatie dat de ISO 27001-norm heeft gepubliceerd om te definiëren waar informatiebeveiliging over gaat en om een set van 114 controls te bieden om informatiebeveiligingsrisico's te beheren.

Wat is auditing?

Auditing is de activiteit van een onafhankelijke auditor om het bestaan van een informatiesysteem (ontwerp), het beheer van het informatiesysteem (verantwoording) en de correcte werking (prestatie) van het informatiesysteem te beoordelen aan de hand van een gedefinieerde set normen (bijvoorbeeld ISO 27001: 2013 of Sarbanes Oxley).

Wat betekent 'continuous'?

Deze term wordt heel vaak gebruikt in de DevOps-wereld en verwijst naar het feit dat veranderingen in het IT landschap hoogfrequent worden uitgevoerd en in de basis vaak kleiner zijn. Het centrale idee is om snel feedback te geven om verbeteringen door te voeren.

Wat is agile?

Agile is een beweging in de markt van softwareontwikkeling die beschrijft hoe meerwaarde voor het bedrijf kan worden gecreëerd door vast te houden aan Lean-principes, zoals bv. het verminderen van verspilling in het ontwikkelingsproces en het verlengen van de time-to-market om het resultaat van de zakelijke waardestromen te vergroten.

Wat is een value system?

Een value system is een set van samenhangende value streams (stromen, bedrijfsprocessen) die samen de bedrijfsresultaten direct of indirect vergroten.

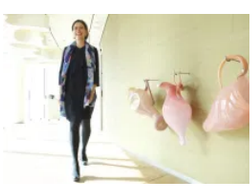
Wat is Security by design?

Het vermogen van een dienst (of product) om continue informatie te exporteren op een geprotocolleerde manier die aantoont dat de service voldoet aan de gegeven informatiebeveiligingsstandaard (ISO 27001: 2013) in termen van beschikbaarheid, integriteit en vertrouwelijkheid om vast te stellen dat de ontworpen controles voor de gedefinieerde risico's van die dienst effectief zijn.

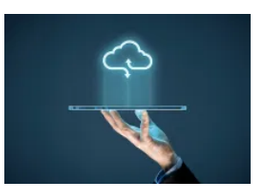
TAGS CA CD CI CONTINUOUS AUDITING DEVOPS SECURITY BY DESIGN SECURITY BY DESIGN GUILD

Security by Design Guild

GERELATEERD MEER VAN DEZE AUTEUR



Rabobank: 100% digitaal gemak



'Haal blijvend waarde uit technologie'

Marcel Krom (PostNL): 'We hebben de digitale transformatie tot leven gebracht'

REAGEREN

Reactie:

Naam:*

E-mail:*

Website:

Mijn naam, e-mail en website opslaan in deze browser voor volgende reacties.

Reactie plaatsen

OVER ONS

IT Executive.nl is een platform voor beslissers op C-niveau bij de grootste bedrijven en instellingen in Nederland met affiniteit voor informatietechnologie, digitalisering, sourcing en leiderschap.

VOLG ONS

© IT-Executive is onderdeel van ICT Media

Privacy - Terms