Lessen uit een praktijkonderzoek

DevOps in control

3 december 2020 Steven Bauer, Hao Dinh en Jeroen Oudshoorn

Dit artikel beschrijft de observaties, aanbevelingen en conclusies uit een afgerond praktijkonderzoek naar de toepassing van het DevOps controleraamwerk van de NOREA-kennisgroep Software Development. [GANG19] Het onderzoek is uitgevoerd bij en in opdracht van Schuberg Philis, een IT-organisatie die volledig met zelfsturende teams werkt volgens de agile- en DevOps-werkwijzen.

Deze bijdrage is gebaseerd op onze thesis ter afronding van de opleiding Executive Master of IT-Auditing aan de TIAS School for Business and Society te Tilburg. In een casestudie is de (aantoonbare) beheersing getoetst van de risico's gerelateerd aan de DevOps-werkmethode van één DevOps-team.

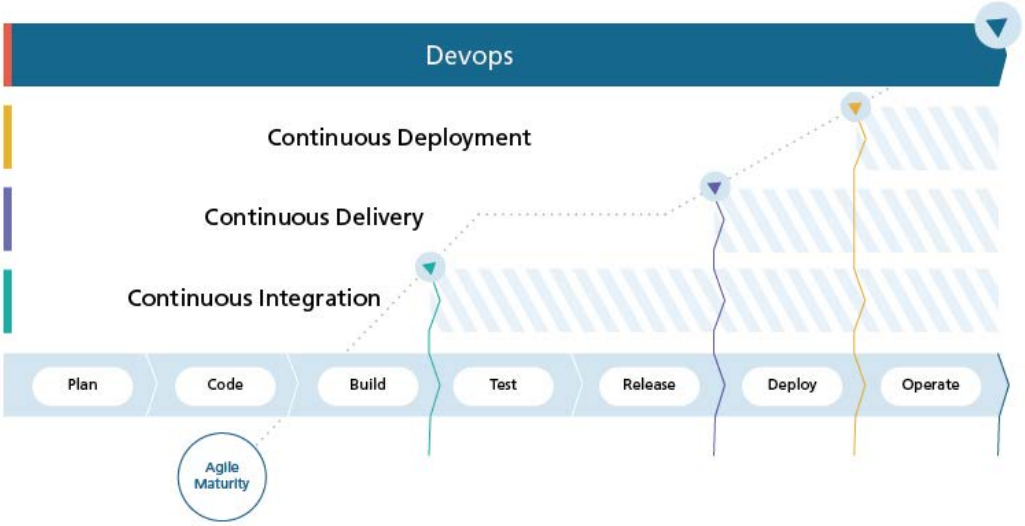
We introduceren eerst het fenomeen 'DevOps', om daarna onze positieve observaties en geobserveerde uitdagingen in risicobeheersing voor het onderzochte team te beschrijven. We sluiten af met een conclusie. Het artikel is primair gericht op IT-auditors die zich bezig (gaan) houden met het auditen van, of adviseren over, DevOps-bedrijfsomgevingen.

DevOps

De afgelopen jaren zijn de agile- en, in haar verlengde, de DevOps-werkwijze steeds vaker omarmd bij zowel grote als kleine organisaties. We hebben gemerkt dat de opkomst van achtereenvolgens agile en DevOps een nieuwe uitdaging vormt voor de conventionele werkwijze van de IT-auditor, doordat development- en operationsactiviteiten steeds verder met elkaar verweven en geautomatiseerd zijn geraakt. De IT-auditor was sindsdien zoekende naar passende handvatten.

Met de introductie van DevOps en daaraan gerelateerde nieuwe technologieën is het mogelijk in een zeer kort tijdsbestek software te ontwikkelen en in productie te brengen, met als doel de business snel waarde te kunnen leveren. Bij een volwassen implementatie is het mogelijk om per jaar honderden of zelfs duizenden veranderingen uit te rollen. Dit komt voornamelijk door de implementatie van *continuous integration / continuous delivery* (CI/CD) *pipeline(s)*.

Een CI/CD-pipeline is een geautomatiseerde ontwikkelstraat met daarin geïntegreerd onder andere (geautomatiseerd) versiebeheer, *build tooling, user acceptance tests* en *software delivery*. Zie figuur1 voor automatiseringsmogelijkheden in de verschillende ontwikkelstappen in een CI/CD-pipeline.



Figuur 1: Ontwikkelstappen in een CI/CD-pipeline (bron: [GANG19])

Omdat een DevOps CI/CD-pipeline een keten van verschillende tools vormt, kan het softwareontwikkelproces veelal via deze tools worden beheerst. Daarnaast kunnen de tools ook worden gebruikt om kwaliteitscontroles te doen op de software die wordt ontwikkeld. Denk aan het uitvoeren van geautomatiseerde tests, zoals de statische code review op bekende kwetsbaarheden in de broncode. Voldoet de software, dan kan de software automatisch naar de volgende processtap. Zo niet, dan kan er worden besloten het proces te stoppen en de ontwikkelaars van de software op de hoogte te stellen, zodat ze een correctie kunnen aanbrengen.

Toetsingskader voor DevOps

Het IT-auditvakgebied heeft (nog) niet met dezelfde snelheid meebewogen als de organisaties en teams die de DevOps-werkwijze hebben omarmd. Zo bestonden er tot voor kort geen richtlijnen of referentiekaders voor IT-auditors, om DevOps-softwareontwikkelingsprocessen te auditen. NOREA heeft eind 2019 het IT-audit controleraamwerk voor DevOps gepubliceerd. [GANG19] Dit raamwerk biedt IT-auditors handvatten om IT-risico's van een DevOps-bedrijfsomgeving te toetsen en beheersen.

Observatie 1: Onderzocht DevOps-team is goed in staat om de technische controls zelf in te richten

Uit ons onderzoek is naar voren gekomen dat het onderzochte DevOps-team goed in staat is om de technische controls binnen het ontwikkelproces zelf in te richten en aantoonbaar te maken zonder tussenkomst van de IT-auditor. Inrichting van het proces, borgen van juiste logging en documentatie van inrichting en gebruik van tools waren allemaal aanwezig. Zo waren de verschillende systemen en omgevingen geautomatiseerd gekoppeld via scripts. Deze scripts zorgen ervoor dat altijd hetzelfde proces wordt gevolgd, inclusief de vereiste testen en controles. Deze testen en controles worden specifiek ingericht voor inspecties naar softwarekwaliteit, juiste configuraties en beveiliging. Bij afwijkingen van de vooraf bepaalde standaarden ontvangen teams daar direct feedback op, zodat het verantwoordelijke team problemen zo snel mogelijk kan oplossen. Mocht een belangrijke kwaliteitseis niet worden behaald, dan wordt het proces gestopt. Bij het succesvol doorstaan van alle testen en controles wordt de ontwikkelde software automatisch naar productie gebracht.

Bovenstaande observatie is gebaseerd op onze casestudie van één DevOps- team. Om te bepalen of DevOps-teams ook in algemene zin in staat zijn om technische controls juist uit te voeren, is aanvullend onderzoek nodig. We vinden het toch belangrijk om de observatie te benoemen, omdat deze de mogelijkheden laat zien die DevOps met zich meebrengt voor het aantoonbaar kunnen voldoen aan technische controls. Een aandachtspunt voor de IT-auditor is om te beoordelen welke controls kunnen worden geautomatiseerd en onder welke voorwaarden de IT-auditor deze kan gebruiken als bewijs. Op hun beurt kunnen DevOps-teams meedenken over hoe deze controls kunnen worden geïmplementeerd in hun omgevingen. Op deze manier kunnen de twee werelden dichter bij elkaar komen.

Observatie 2: Uitdagingen van het onderzochte DevOps-team bij het beheersen van de DevOps-risico's

Tegenstrijdige belangen. Inherent aan de DevOps-werkwijze is dat het werk wordt gedaan door zelfsturende teams met een hoge mate van eigen beslissingsbevoegdheid en verantwoordelijkheid. Een dergelijk team is zelf verantwoordelijk voor het totale proces waarin producten of diensten voor de interne of externe klant tot stand komen. Resultaatgerichtheid is daarbij vaak een sleutelwoord: een team wordt afgerekend op de producten of diensten die ze leveren. Het onderzochte DevOps-team had echter tegelijkertijd ook de verantwoordelijk de risico's in hun proces te beheersen in overeenstemming met het risicobeleid van de organisatie. Het team had dus twee tegengestelde belangen: het moest in staat zijn om snelle oplossingen te leveren, terwijl het tegelijkertijd verantwoordelijk was

voor een beheerste bedrijfsvoering. Uit ons onderzoek bleek dat bij het onderzochte team, bestaande uit engineers met een technische achtergrond, de nadruk lag op resultaatgerichtheid. Dit had verminderde aandacht voor beheersing van risico's tot gevolg.

Onduidelijke verantwoordelijkheden. Het onderzochte DevOps-team kende een complexe verdeling van verantwoordelijkheden in de ontwikkel pipeline, omdat er sprake was van een ander bedrijf als opdrachtgever en een externe partij die door de opdrachtgever was ingehuurd om de software te ontwikkelen. Bij het ontwikkelen maakte de externe partij gebruik van de ontwikkel-pipeline die werd beheerd door het onderzochte DevOps-team. Bij het ontwikkelproces waren dus drie partijen betrokken – de opdrachtgever, het ontwikkelteam en een externe partij – die ieder verantwoordelijk waren voor een gedeelte van het proces en de bijbehorende risico's. Voor deze partijen was voor een gedeelte van het proces geen expliciet eigenaarschap gedefinieerd, waardoor vaak onduidelijk was wie verantwoordelijk was voor het identificeren van de risico's en inrichten van adequate beheersmaatregelen. Hierdoor bleek het een uitdaging voor de opdrachtgever om scherp zicht te houden op de risicobeheersing.

Inrichting general IT controls. Naast de reeds genoemde uitdagingen bleek ook het vertalen van de randvoorwaardelijke *general IT controls* naar de DevOps-manier van werken lastig. Deze controls moeten zo worden ingericht dat ze het juiste proces en de kwaliteitseisen voor software afdwingen, zodat we het technische proces kunnen vertrouwen. Denk hierbij aan toegangsbeheer tot beheer- en pipeline-tools, het kunnen wijzigen van deze tools gedurende het jaar, beveiliging van deze tools en scheiding van functies.

Aanbevelingen voor de IT-auditor

In deze paragraaf doen we aanbevelingen voor IT-auditors die een toets (gaan) uitvoeren op een DevOps-bedrijfsomgeving.

Heldere verdeling van verantwoordelijkheden

Uit de resultaten van onze casestudie blijkt dat het opzetten van de juiste rollen en verantwoordelijkheden in een complexe organisatie met meerdere (externe) stakeholders een uitdaging voor het DevOps-team is. Door geen helder eigenaarschap van deze partijen te definiëren, was onduidelijk wie verantwoordelijk was voor het identificeren en mitigeren van risico's. De IT-auditor kan met zijn of haar kennis het team helpen bij een heldere afbakening van de verantwoordelijkheden van diverse stakeholders voor het uitvoeren van controls. Denk aan het opstellen van een RACI-matrix en risico-inschattingen van externe partijen die zijn betrokken in de CI/CD-pipeline. Heldere afspraken over de taken en verantwoordelijkheden op het gebied van controls binnen het ontwikkelproces zorgen ervoor dat de ontwikkeling van nieuwe releases beheersbaar blijft.

Eventueel kan de opdrachtgever de gemaakte afspraken vastleggen in een SLA tussen opdrachtgever en het team zodat niet uitsluitend gestuurd wordt op de kernwaarden van DevOps, zoals snelheid, waarde en innovatie. We hebben gezien dat het DevOps-team en een IT-auditor risico's anders benaderen. Door een intensievere samenwerking van het DevOps-team met de IT-auditor kan een team leren zijn verantwoordelijkheid voor risicobeheersing beter in lijn te brengen met de vereisten die de IT-auditor stelt.

Opstellen van key controls

Tijdens onze casestudie werd duidelijk dat niet voor iedere DevOps-implementatie alle vijftien controls en alle daaronder vallende subcontrols uit het Norea DevOps Framework even noodzakelijk zijn. Deze relatief grote set aan (sub)controls zorgde ervoor dat niet altijd voldoende prioriteit werd gegeven aan de meest urgente controls. Een IT-auditor kan een DevOps-team helpen om de set 'key' controls te bepalen die minimaal noodzakelijk is bij het inrichten van het DevOps-proces, om de risico's binnen de reikwijdte van het team beheersbaar te houden. Ook kan de IT-auditor het team advies geven hoe die key controls zo ingericht kunnen worden dat deze aantoonbaar zijn voor de (externe) auditor en eventuele toezichthouders.

Voor het bepalen van een heldere set aan key controls is volgens ons vervolgonderzoek nodig. Bovendien zal iedere DevOps-implementatie een ander risicoprofiel hebben, wat het onmogelijk maakt om één generieke set aan key controls op te stellen. Wel denken we dat sommige controls altijd deel moeten uitmaken van de set key controls. Zie voor een voorbeeld het tekstkader 'Voorbeeld universele key control'.

Voorbeeld universele key control

Goedkeuringen voor releases naar productie dienen aantoonbaar vastgelegd te zijn, zodat deze naar een individu en releaseversie te herleiden zijn. Ongeautoriseerde wijzigingen uitrollen naar productie kan direct gevolgen hebben voor de bedrijfsvoering of zelfs leiden tot fraude. Ook (externe) auditors en toezichthouders zien dit als een groot risico, waarbij het van belang is om een deployment gecontroleerd en aantoonbaar uit te voeren. Dit kan technisch worden ingericht in de deployment-tool, waarbij een goedkeuring voor release altijd wordt afgedwongen of geautomatiseerd wordt gegeven en vastgelegd na uitvoering van de controle. Dit kan zowel preventief als achteraf.

Aantoonbaarheid door technische mogelijkheden

Ondanks dat het DevOps-team in staat is de technische controls in te richten, worden processtappen zoals code review en het bespreken van ontdekte afwijkingen vaak onjuist of niet vastgelegd. De IT-auditor kan het DevOps- team heldere criteria geven, waardoor het team in staat is goed aantoonbaar risicomanagement uit te voeren. De verantwoordelijkheid van risicobeheersing wordt dan bij het DevOps-team gelegd. De IT-auditor kan de DevOps-engineers een helder beeld geven hoe risicomanagement zou

moeten verlopen en welke controls er moeten worden ingericht, bijvoorbeeld rond de ondersteunende applicaties. Een DevOps-team kan dan een optimale balans zoeken tussen aantoonbaar risicomanagement en de voordelen van DevOps realiseren.

Conclusie

Ons artikel beschrijft de ervaringen uit een afgerond praktijkonderzoek naar de toepassing van het DevOps controleraamwerk. Wij observeerden bij het onderzochte DevOps team een aantal uitdagingen waaronder: tegenstrijdige belangen, onduidelijke verantwoordelijkheden en een gebrek aan de inrichting van de randvoorwaardelijke IT-controls voor de DevOps-omgeving.

Echter, de agile- en DevOps-werkwijze bieden niet alleen uitdagingen, maar ook kansen voor de IT-auditor. Het wordt bijvoorbeeld mogelijk om de aantoonbaarheid van controls te verhogen door gebruik te maken van de automatisering en logging die DevOps-tools met zich meebrengen. Om deze kansen te benutten, zien wij de noodzaak voor IT-auditors om helder de verwachte standaarden te formuleren en deze gezamenlijk met de DevOps- teams te verscherpen.

In veel gevallen betreft dit dan het instrueren van de DevOps-teams bij het op efficiënte wijze generen van afdoende bewijs voor de werking van de controls. Dit verhoogt de *risk awareness* en kennis omtrent risicomanagement van DevOps-engineers.

Door een betere samenwerking tussen de IT-auditor en het DevOps-teams kunnen de twee werelden dichter bij elkaar komen. Continue leren en communiceren zullen daarbij helpen. De IT-Auditor kan met de volgende activiteiten een startpunt maken om dit te bereiken:

- Schetsen van de IT-randvoorwaarden voor de engineers, waarbinnen zij de vrijheden en verantwoordelijkheden krijgen die specifiek passen binnen de klantcontext waarin ze opereren.
- Regelmatig evalueren van de risico's en controls in een ritme dat past bij de hoge frequentie van zowel de deployments als de veranderingen in processen en toegepaste techniek.

Literatuur
[GANG19] S. Gangaram Panday. *DevOps and Agile in control; A study report by NOREA*. NOREA, 2019. https://www.norea.nl/download/?id=6047, geraadpleegd op 10 november 2020.

S. (Steven) Bauer MSc EMITA | Senior Consultant bij *KPMG*

Steven is werkzaam binnen IT Assurance & Advisory van KPMG, waar hij organisaties helpt bij het verbeteren van hun IT-beheersing en IT-systemen, en opstellen van diverse IT-raamwerken. Steven heeft ervaring met diverse IT-audits en assuranceopdrachten met een focus op financiële instellingen.

Ir. H. (Hao) Dinh EMITA CISSP | Senior Cybersecurity Advisor bij *EY*

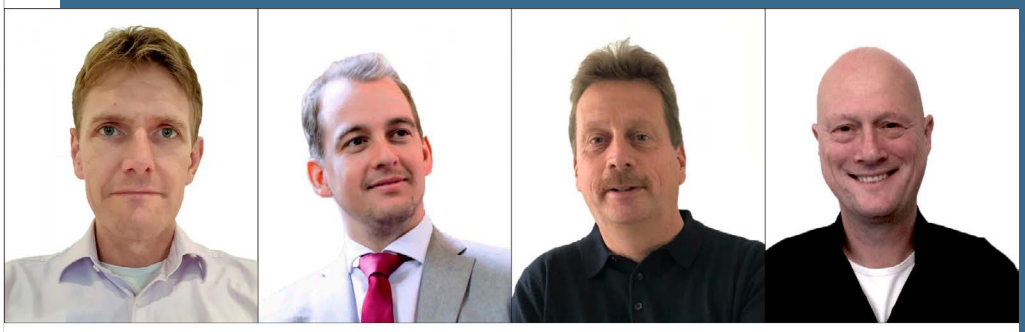
Met een brede kennis van informatiebeveiliging ondersteunt Hao bedrijven bij het ontwerp, de inrichting en de implementatie van systemen die functioneel en tegelijkertijd veilig dienen te zijn. Hij specialiseert zich hierin voornamelijk in organisaties en afdelingen op het raakvlak tussen de IT-innovatie en de financiële sector.

J.V. (Jeroen) Oudshoorn MSc EMITA | IT Risk Specialist bij *DNB*

Jeroen is werkzaam als toezichthouder op de financiële sector, met een specifieke focus op IT-risico's in het (inter)nationale betalingsverkeer. Eerder deed hij ervaring op als (senior) technology consultant bij diverse banken en verzekeraars.

De kennisgroep Betalingsverkeer

Dit artikel is een product van de kennisgroep Betalingsverkeer van NOREA. De kennisgroep produceert guidance en achtergronddocumenten en organiseert en seminars op het gebied van betalingsverkeer. Leden van de kennisgroep zijn:



Lodewijk Benjaminse | Willian Crielaars | Léon Dirks | Hans Koster

Wandena Punwasi | Erus Schuurman | Frank Waatjes

De kennisgroep is te bereiken via norea@norea.nl of via ons twitteraccount @PaymentFriends

Recente activiteiten zijn:

- Webinar 'Risico's van betalingsverkeer en PSD2';
- Handreiking auditaanpak PSD2;
- Factsheet overview PSD2

Literatuur

Banken.nl. *Bankensector.*

Ellen Klijnstra. *Anti Money Laundering in a Digital World; NOREA & ISACA Young Prof Event.*

European Banking Authority. *EBA publishes revised Guidelines on outsourcing arrangements.*

Hans Koster and Tom van de Ven. *Practical guidance for Internal Auditors on the annual audit of PSD2 related to strong customer authentication and common and secure communication.* NOREA.

Kennisgroep Betalingsverkeer. NOREA.

NOREA. *Payment Services Directive (PSD2).*

NOREA. *PSD2 Practical guidance Worksheet MVP 1-1.*