eraneos

Whitepaper

Governance, Risk & Compliance

Quality by Design in een DevOps organisatie

Mei 2023

Inhoudsopgave

Inleiding: wendbaar én in control

Voor elke organisatie is het cruciaal om in control te zijn bij het naleven van wetgeving en interne processen en ook om informatiebeveiliging goed op orde te hebben. De risico's en de mogelijke gevolgen wanneer dit niet het geval is, zijn immers groot: van datalekken en aanvallen met ransomware tot nalatigheid bij illegale activiteiten (zoals fraude of hackers) en het niet compliant blijven aan snel veranderende wet- en regelgeving. Daarom is het belangrijk om gestructureerd en bedachtzaam met Governance, Risk & Compliance (GRC) om te gaan. GRC wordt geborgd door het inrichten van Quality by Design (QbD). QbD beschrijft het vastleggen van kwaliteitscontroles, onder andere in het portfolioproces en het voortbrengingsproces van de teams.

Het toepassen van QbD bij 'Governance, Risk, and Compliance (GRC) is een gestructureerde manier om ervoor te zorgen dat risico's worden beheerd en er wordt voldaan aan geldende branche- en overheidsvoorschriften.

Maar hoe functioneert dat binnen een DevOps werkomgeving, waarbij teams doorgaans voor zowel de ontwikkeling als ook het beheer van hun systeem verantwoordelijk zijn? Hoe kunnen verantwoordelijkheden zo laag mogelijk in de organisatie belegd worden om eigenaarschap en snelle besluitvorming mogelijk te maken? Wie draagt welke verantwoordelijkheden en welke rechten zijn hiervoor nodig? Dat kan een uitdaging zijn. Zeker doordat eisen vanuit wet- en regelgeving en toezichthouders vaak nog van traditioneel georganiseerde organisaties uitgaan.

Wanneer organisaties steeds meer agile gaan werken, bereiken zij op het gebied van GRC vaak een omslagpunt. De 'oude' coördinatiemechanismen blijven in stand terwijl parallel teams steeds meer zelf willen kunnen. Overlappende, conflicterende en dubbel uitgevoerde activiteiten zijn hiervan het gevolg. Het herijken van de coördinatie van GRC-taken tussen en over teams is hierdoor noodzakelijk.

In deze whitepaper gaan we dieper in op hoe organisaties hun processen, beleid, regels en voorschriften zo in kunnen richten dat het binnen een DevOps manier van werken goed functioneert. We behandelen achtereenvolgens de aanpak en uitdagingen op strategisch-, applicatie- en teamniveau. Deze whitepaper biedt zodoende een aantal handvatten waarmee organisaties wendbaar zijn én in control kunnen blijven.

GRC op strategisch niveau

De manier waarop een organisatie haar beleid rondom wetgeving, reporting en informatiebeveiliging inricht, wordt in de top van de organisatie bepaald. Hier wordt ook de visie vastgesteld op hoe verschillende lagen van de organisatie zorgdragen voor de GRC-onderwerpen. Het opgestelde beleid en de visie wordt vervolgens geborgd in bestaande processen in de organisatie.

Een van de belangrijkste taken van het hoger management is om de koers van een organisatie te vertalen in strategie en doelstellingen en dat concreet te maken in de vorm van te behalen resultaten. Onderdeel hiervan is het analyseren en prioriteren van nieuwe strategische projecten/initiatieven in het portfoliomanagement-proces. In dit proces zit het eerste moment waarop GRC-onderwerpen wordt gecontroleerd.

Bij hoog geprioriteerde nieuwe strategische initiatieven, is het zaak om in kaart te brengen welke impact deze initiatieven op de staande organisatie (kunnen) hebben. Onderdeel hiervan is het inhoudelijk verkennen van de gevolgen op het gebied van GRC. Wanneer er wordt besloten om over te stappen naar een nieuw systeem, is het bijvoorbeeld belangrijk dat data correct wordt overgezet en het traceerbaar is wie toegang tot welke informatie heeft en wie er veranderingen aan toe mag brengen. Net zoals het bij het introduceren of wijzigen van een applicatie belangrijk is om te voorkomen dat er persoonsgegevens worden opgeslagen terwijl dat volgens de Algemene verordening gegevensbescherming (AVG) niet is toegestaan. Om dit te bereiken wordt een lijst met de belangrijkste impactgebieden doorlopen. Hierbij is het de kunst om de juiste experts deel te laten nemen aan de analyse. Zij schatten vanuit hun expertise de effecten in die de mogelijke invoering van het strategische initiatief met zich meebrengt.

Het is daarom raadzaam om bij elk strategisch initiatief een impactonderzoek uit te voeren aan de hand van een vaste checklist. Onderstaande vraagstukken kunnen als onderdeel van deze checklist helpen om een gedegen impactanalyse van de beoogde verandering te maken:

- Wat zijn de gevolgen voor de wet- en regelgeving waaraan de organisatie moet voldoen?
- Wat is de mogelijke impact op onze organisatie, ook op reputatiegebied?
- Is het voor dit initiatief nodig om de IT-infrastructuur aan te passen?
- Wat zijn de specifieke aandachtspunten per branche en organisatie?
- Wat is de impact volgens het Privacy & Security assessment?

GRC op applicatieniveau

Zodra op strategisch niveau besloten is welke veranderingen worden doorgevoerd én wat de impact hiervan op de organisatie gaat zijn, is het tijd om dieper in de functionaliteit van het systeem of product te duiken. Het doel hiervan is om ervoor te zorgen dat de beoogde wijziging goed en integer werkt, waarbij er rekening is gehouden met alle relevante GRC-vraagstukken.

Het is hierbij de bedoeling om vanuit het strategische initiatief een vertaalslag te maken naar de werkpakketten voor de (ontwikkel) teams van de betreffende applicaties. Er wordt hiervoor een eigenaar van het initiatief aangewezen die dit verder oppakt. Dit kan bijvoorbeeld een Product Manager (PM) zijn. Om de werking en vereisten van de te wijzigen applicatie zo goed mogelijk te kunnen definiëren, is het zaak om tijdens dit analyseproces interne en externe stakeholders te betrekken en te informeren.

Waar nodig kunnen dan gespecialiseerde collega's zoals architecten, juristen dan wel risicomangers aanhaken. Deze collega's zijn vaak georganiseerd in competence centres, waar de specialistische kennis geborgd wordt. Competence centres hebben vaak een directe lijn met de teams om snel en adequaat te kunnen helpen.

Binnen een organisatie die agile werkt, ligt de verantwoordelijkheid voor het betrekken van andere afdelingen en stakeholders bij de eigenaar van het initiatief. Dit komt de snelheid ten goede en zorgt ervoor dat organisaties wendbaar blijven en adequaat kunnen reageren op veranderingen in de markt of verzoeken van klanten.

Rol van de Change Advisory Board (CAB)

Zeker in traditioneel ingerichte organisaties wordt er vaak gebruik gemaakt van een CAB. Hierin zitten mensen uit de organisatie die het applicatielandschap goed kennen en akkoord geven op voorgestelde wijzigingen. Wanneer een team een wijziging wil doorvoeren, is het binnen deze constructie gebruikelijk om eerst de plannen en de verwachte impact aan de CAB toe te lichten en hen om goedkeuring te vragen. De CAB beoordeelt dan welke implicaties de wijziging op de organisatie en het applicatielandschap heeft en of dit binnen de huidige visie en architectuur past.

Bij DevOps organisaties ligt de verantwoordelijkheid zo veel mogelijk bij de teams, en kan de behoefte ontstaan om helemaal geen gebruik meer te maken van een CAB of dit op een andere manier te doen. Dit kan bijvoorbeeld worden vormgegeven door het aanstellen van adviseurs voor de (ontwikkel)teams. Om te voorkomen dat dit aan de ene kant de DevOps werkwijze belemmert en vertraagt, terwijl het aan de andere kant zorgt voor de benodigde controles en akkoorden is het vooral belangrijk om goede afspraken te maken.

Zo is het bijvoorbeeld mogelijk om vast te leggen bij welke soort wijzigingen het wél of juist niet nodig is om samen te werken met een adviseur (of de CAB). Ook is het handig om een aanvraag al zo vroeg mogelijk samen met de CAB te bespreken, nog voordat het team ermee aan de slag gaat. Dit versnelt het proces, waardoor het team zo autonoom mogelijk kan opereren en er voldoende controles zijn om te voldoen aan wet- en regelgeving.

Ten behoeve van de snelheid worden verantwoordelijkheden dus vaak lager in de organisatie neergelegd, echter mag dit natuurlijk niet ten koste gaan van het naleven van wet -en regelgeving. Het is daarom raadzaam de werking van een nieuw systeem of product via een impactchecklist ook op productniveau te borgen. Wijzigingen op productniveau zijn concreter dan voorgenomen strategische wijzigingen en het detailniveau van deze checklist is daarom uitgebreider. Denk hierbij vooral aan de volgende onderdelen, wanneer er gekeken wordt naar de nieuwe oplossing of applicatie functionaliteit:

- **Volledigheid:** Werkt de applicatie volledig en worden alle benodigde gegevens daadwerkelijk verwerkt?
- **Nauwkeurigheid:** Werkt de applicatie zoals die hoort te werken en worden de gegevens op de juiste manier verwerkt?
- **Autorisatie:** Wie mogen er bij de applicatie en de gegevens en is dit op de juiste manier ingericht?
- **Reporting:** Is het – bijvoorbeeld door logs bij te houden – mogelijk om achteraf te traceren welke acties de applicatie heeft uitgevoerd?

Zodra deze punten zijn onderzocht, kan het verantwoordelijke IT-team met de beoogde wijziging aan de slag.

Gezien het de bedoeling is om verantwoordelijkheden zo laag mogelijk in de organisatie te beleggen komen de meeste verantwoordelijkheden en controls bij de teams te liggen. Hoewel het productniveau vrijwel altijd noodzakelijk is, is het daarom aan te raden om de functionele controls op dit niveau tot een minimum te beperken en deze zo veel mogelijk binnen de teams in te richten.

GRC op teamniveau

In een DevOps werkomgeving heeft het team dat het nieuwe systeem of functionaliteit gaat bouwen, zoveel mogelijk vrijheid en verantwoordelijkheid. Uiteraard moet dat wel binnen bepaalde kaders en richtlijnen gebeuren. Om hiervoor te zorgen, is het mogelijk om op verschillende momenten van het ontwikkelproces controles in te bouwen.

Geautomatiseerde wijzigingscontroles, versiebeheer en in overleg met de CAB vooraf goedgekeurde standaardwijzigingen zijn veilige manieren om de snelheid in het ontwikkelproces te houden. Zo is het bijvoorbeeld mogelijk om met de CAB in een vroeg stadium af te spreken welke soort wijzigingen het verantwoordelijke team zelf kan doorvoeren. Denk hierbij onder meer aan zaken die geen directe impact hebben op andere applicaties of teams.

Definition of Done (DoD)

Hoe kunnen organisatie borgen dat aan GRC-kaders wordt voldaan? Voor DevOps organisaties biedt het 'Definition of Done'-principe uitkomst. Hierin worden op basis van de input van relevante stakeholders de afspraken beschreven waaraan werk, activiteiten en mensen moeten voldoen. Door dit in een systeem af te vinken bij al het werk dat wordt gedaan, ontstaat een audit trail die laat zien dat aan de gestelde kaders is voldaan. Vaak werkt het goed om de Definition of Done op verschillende niveaus vast te stellen. De hele organisatie heeft immers te maken met wet- en regelgeving, zoals er ook per team specifieke wensen en eisen zijn waaraan moet worden voldaan.

Vierogenprincipe

Door bij veranderingen in de code het ‘vierogenprincipe’ toe te passen, verklein je de kans op fouten of misbruik. Er kijkt immers altijd iemand anders mee. Dit kan onder meer worden geborgd door het aanmaken van merge requests. Een developer kan zo’n verzoek aanmaken wanneer hij of zij code wil inchecken en live wil brengen. Een ander teamlid dient de code vervolgens eerst goed te keuren voordat die volgende stap mogelijk is.

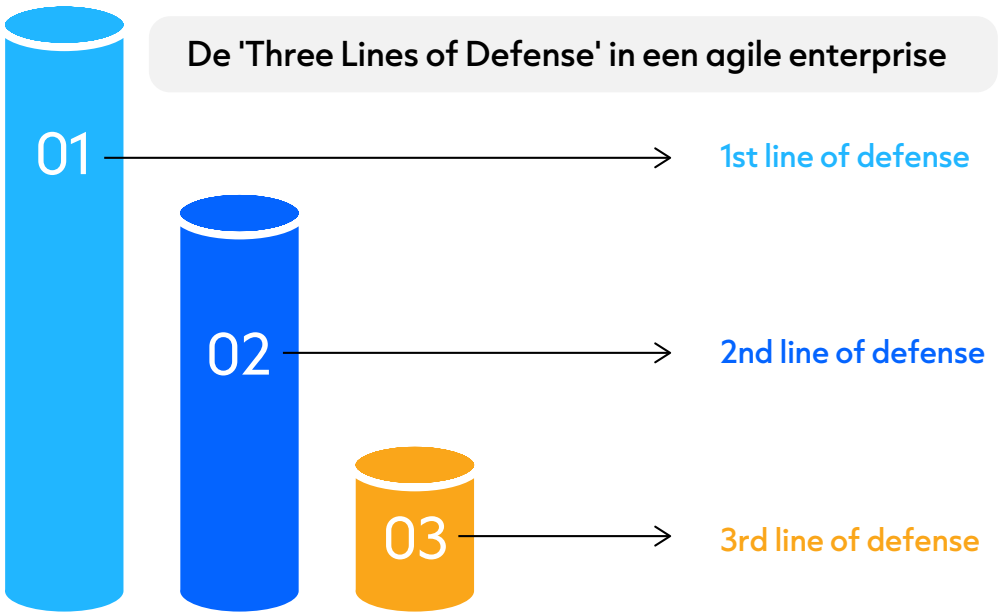
Toegang tot programma’s en data

Zeker wanneer organisaties werken met privacygevoelige informatie, is het belangrijk om goed te bepalen wie op welk moment toegang tot specifieke programma’s en data heeft. Medewerkers moeten hier een goede reden voor hebben, die het liefst ergens duidelijk omschreven staat. Daarbij is het echter belangrijk om te voorkomen dat er te weinig mensen zijn die toegang hebben. Het is belangrijk om continuïteit te borgen en snel te kunnen schakelen wanneer dat nodig is.

Zo wordt voorkomen dat een ontwikkelproces vertraging oploopt omdat één programmeur uitvalt. Per organisatie moet gekeken worden wat de beste oplossing is om hiermee om te gaan. Sommige organisaties kiezen er bijvoorbeeld voor om developers standaard geen toegang tot de productieomgeving te geven, in dit geval wordt de geschreven code vaak automatisch getest en in productie gezet. Echter kan het ook een mogelijkheid zijn om developers wel toegang te geven door tijdelijke wachtwoorden te verstrekken en activiteiten op de productieomgeving structureel te monitoren en loggen.

Monitoring en logging

Zodra het nieuwe systeem of product live is, zijn er veel mogelijkheden om de omgeving te monitoren en automatisch te loggen wat er binnen de productomgeving gebeurt. Zo is het bijvoorbeeld mogelijk om te zien of er iemand in het systeem ingelogd is geweest, of automatisch een alarm af laten gaan wanneer er veel servercapaciteit wordt gebruikt.



Three lines of defense

Een klassieke manier om GRC-activiteiten in organisaties te integreren, is het three lines of defense-model. Maar ook binnen een agile of DevOps werkomgeving kan dit model van waarde zijn, zoals hieronder is weergegeven.

1st line of defense

Klassiek: Managers en medewerkers in de business en in de IT-processen vormen de eerste lijn. Deze is verantwoordelijk voor het leveren van klantwaarde.
Agile: De Product Owner (PO) is verantwoordelijk. Teamleden ondersteunen de PO met risico-analyses, het ontwerpen en implementeren van securitymaatregelen en beheersmaatregelen en het opleveren van evidence.

2nd line of defense

Klassiek: Stafafdelingen produceren beleid en frameworks en controleren de eerste lijn.
Agile: Vakmensen die de business ondersteunen geven richting aan de teams. Dit is een kleine kern die kennis en informatie verspreid via Professional Groups, Competence Centers of Communities of Practices. Ook vertalen zij regels naar acceptatiecriteria en DoD's die door de teams zelfstandig of met een controle door de derde lijn toegepast kunnen worden.

3rd line of defense

Klassiek: De interne Audit-afdeling
Agile: Nog steeds de interne Audit-afdeling, maar met auditers die de kernwaarden van agile of DevOps organisaties begrijpen en kunnen overbrengen.

Organisatievereisten

In deze whitepaper beschreven we de manier waarop organisaties met een DevOps werkomgeving op verschillende niveaus controlemechanismen in kunnen voeren zonder dat dit al te grote gevolgen heeft op de wendbaarheid.

Maar wanneer een organisatie aan het begin van een DevOps transformatie staat is het vaak nog niet mogelijk en verstandig om alle traditionele controlemechanismen meteen los te laten. Ook de mate waarin processen geautomatiseerd zijn, spelen hierbij een rol. Veel van de DevOps controlemechanismen zijn tenslotte pas mogelijk bij een hogere automatiseringsgraad.

Wil een organisatie op een agile manier met GRC omgaan, maar kunnen bepaalde verantwoordelijkheden nog niet op teamniveau worden belegd? Dan is het aan te raden om een aantal verantwoordelijkheden vooralsnog op een hoger niveau in de organisatie te beleggen en teams langzamerhand op hun nieuwe verantwoordelijkheden voor te bereiden door de juiste trainingen en ontwikkelingen te verzorgen.

Wil je advies over de mate waarin jouw onderneming op een DevOps wijze met GRC-taken om kan gaan en hoe je dit in je organisatie kan implementeren? Eraneos adviseert je graag over de mogelijkheden. Neem contact op met Gwendolyne Brink, Sander Hoogland of Olivia Plant.

Gwendolyne Brink
Manager

Olivia Plant
Senior Consultant

Sander Hoogland
Senior Consultant

eraneos

Ervaren in een breed scala van industrieën

OVER ERANEOS

Eraneos is een internationaal adviesbureau op het gebied van management en technologie die de digitale toekomst van organisaties helpt vormgeven. Eraneos adviseert organisaties niet alleen bij het vormgeven, maar ook bij het succesvol implementeren van de digitale transformaties en oplossingen. Samen met onze adviseurs en engineers helpen we organisaties veranderen en verbeteren met als doel een duurzame groei en blijvende impact te realiseren.

Dit doen we door goed te luisteren naar wat bedrijven willen en nodig hebben. Deze behoefte vertalen wij naar een aanpak waarin we de mensen verbinden met technologie, processen en leiderschap, waardoor transformaties snel en efficiënt gerealiseerd kunnen worden.

Dankzij onze brede branchekennis, ervaring met technologie en serviceverlenende instelling hebben we alles in huis om het verschil te maken.

Zo zijn we in staat om elke uitdaging aan te gaan en écht bij te dragen aan het succes van organisaties. Onze klanten vertrouwen ons van de ontwerp- tot uitvoeringsfase wat voelbaar is in onze samenwerking. Van complexe strategische uitdagingen in finance tot ethische AI-toepassingen in de zorg.

Wij luisteren niet alleen naar jouw wensen en behoeften, wij zorgen ervoor dat we ze begrijpen én waarmaken. Samen met jou halen we alles uit de digitale wereld wat erin zit.

Contact >

Onze kantoren >

Bezoek onze website >