Control by Design: risicovrije processen als heilige graal

Een belangrijk concept voor kostenbesparing en het vergroten van je risicobeheersing. Mooie theorie, maar ook praktisch toepasbaar?

Ing. Thomas Schoonhoven
is Risk Control Partner binnen Rabobank.

Drs. Robin Polder
is Lead Data & Technology voor Coöperatief Klantbelang bij Rabobank.

Risicomanagement krijgt een steeds prominentere rol binnen organisaties. Met de snel veranderende omgeving, toenemende digitalisering en regelgeving ten aanzien van de dienstverlening is een goede risicobeheersing een uitdaging. Voor een meer geautomatiseerde risicobeheersing zie je de term Control by Design voorbijkomen, niet alleen binnen de financiële instellingen maar ook als belangrijke beweging voor de toekomst bij andere organisaties. Maar wat betekent deze term eigenlijk? En wat maakt het noodzakelijk om dit gedachtegoed te omarmen en daadwerkelijk toe te passen? In dit artikel worden de achtergrond en de kansen van Control by Design toegelicht. Ook wordt stilgestaan bij de toepassing, de mogelijke obstakels en hoe hiermee om te gaan om het concept zo meer handen en voeten te geven.

Bart Olieman
is Productmanager Bedrijven binnen Rabobank.

Mourad Fakirou MSc RE
is manager bij KPMG Digital Transformation.

Dit artikel is ook een roep naar andere organisaties om met elkaar van gedachten te wisselen.
Stuur een e-mail naar info@compact.nl als u uw ideeën met ons wilt delen.

INTRODUCTIE

Bedrijfsprocessen veranderen continu. Er vinden optimalisaties plaats, (deel)processen of systemen worden uitbesteed, nieuwe producten of diensten worden ontwikkeld en oude producten of diensten worden stopgezet maar moeten nog wel worden beheerd. Wet- en regelgeving of (intern) beleid wordt geïntroduceerd of aangepast, nieuwe risico's duiken op of bestaande risico's worden anders gewogen. Daarnaast vinden reorganisaties plaats, verantwoordelijkheden en prioriteiten schuiven op. Dat vertaalt zich naar complexer wordende processen, het inrichten van work-arounds of het toevoegen van handmatige stappen om toch aan nieuwe eisen te kunnen voldoen. Dit alles gaat vaak sneller dan veel IT-afdelingen aankunnen. Dit zie je ook terug in de beheersingsmaatregelen (controls), waar handmatige controles op de work-arounds en uitzonderingen de beheerskosten steeds opdrijven, met het risico dat deze handmatige controles onvoldoende worden uitgevoerd.

De complexe en continu veranderende en zwaarder wordende regelgeving zorgt ervoor dat belangrijke risico's niet meer zijn op te lossen door alleen maar handmatige beheersingsmaatregelen. En naast de toenemende beheerskosten van het proces zelf, ontstaat hogere druk op de monitoring. Zekerheid op de werking van de beheersingsmaatregelen wordt gezocht door toenemende eerste-, tweede- en derdelijns controles, gedreven vanuit het Three Lines Model (3LM). De kosten die het handmatige werk met zich meebrengt voor het uitvoeren van de beheersingsmaatregelen plus de kosten die gepaard gaan met het handmatig monitoren van de werking van de beheersingsmaatregelen leiden tot een steeds groter wordende 'cost of control'.

Three Lines Model

Het Three Lines Model (3LM) bestaat uit drie lijnen die samen toezien op het beheersen van risico's. De eerste lijn bestaat uit managers en medewerkers die verantwoordelijk zijn voor het identificeren en het beheersen van risico's als onderdeel van hun dagelijkse werkzaamheden. De tweede lijn ondersteunt en begeleidt hierbij door het bieden van richtlijnen, beleid en beheersingsraamwerken. Daarbij draagt de tweede lijn ook zorg voor de monitoring om vast te stellen dat de risico's juist worden beheerst. Tot slot richt de derde lijn zich op een onafhankelijke review dan wel audit op de naleving van de verantwoordelijkheden door de eerste en tweede lijn. Vaak betreft dit een internal-auditafdeling ([CIIA21]).

Los van bovengenoemde complexiteit en de toenemende 'cost of control' zien we ook een digitaliseringsbeweging. Financiële instellingen bedienen de klant steeds meer online, waarbij de processen en systemen worden aangepast. Customer journeys worden uitgewerkt en nieuwe systemen ingekocht en/of ontwikkeld. Het opnieuw uittekenen van processen en het inrichten en primair gebruikmaken van systemen (Design) biedt gelijk de kans om ook je risico's anders te beheersen (Control) of, beter nog, te voorkomen. Door de (proces)risico's zo vroeg mogelijk mee te nemen in je ontwerp (Design), kun je de beheersing (Control) hiervan veel efficiënter inrichten. Lees 'Control by Design'! Een baanbrekend en nieuw idee? Nou nee, maar wel eentje dat vraagt om praktiseren om zo daadwerkelijk de 'cost of control' te kunnen verlagen. Om hiertoe te komen staan we allereerst stil bij de definitie en hoe Control by Design in de praktijk gebracht kan worden. Vervolgens lichten wij scenario's toe indien Control by Design niet haalbaar is, waarna we afsluiten met waar men tegenaan kan lopen bij de implementatie van Control by Design.

CONTROL BY DESIGN: RISICOBEHEERSING ALS VAST ONDERDEEL VAN HET (IT-)ONTWIKKELPROCES

De term Control by Design is niet nieuw. Ook de zogenoemde Application Controls worden al geruime tijd gebruikt en geïmplementeerd. De voordelen zijn helder. Een goed geprogrammeerd systeem doet iedere keer dezelfde juiste handeling, ook op de maandagmorgen of vrijdagmiddag. Daarnaast hoef je qua monitoring geen intensieve dossiercontroles te doen maar test je de Application Control tijdens de implementatie of systeemverandering zelf. Daarvoor leun je op goed ingerichte IT-processen (General IT Controls) om te waarborgen dat het systeem blijft doen wat het moet doen. Dit houdt in dat de General IT Controls effectief werken zonder significante bevindingen die de dagelijkse operatie van het systeem kunnen beïnvloeden. General IT Controls zien toe op een beheerst applicatieveranderproces, een effectief autorisatiebeheer en een geborgde systeemcontinuïteit ([ISAC11]). Deze elementen zijn een randvoorwaarde om vast te stellen dat een geautomatiseerde control (Application Control) blijft doen wat hij moet doen.

Toch zien we binnen organisaties dat er nog niet altijd optimaal gebruik wordt gemaakt van dergelijke geautomatiseerde beheersingsmaatregelen om de risico's te beperken. Verschillende zaken kunnen brede automatisering in de weg staan. De redenen hiervoor zijn divers. Een voorbeeld is dat de implementatie van geautomatiseerde beheersingsmaatregelen complex, duur en kwetsbaar voor verandering kan zijn. Ook kan het zijn dat deze maatregelen onvoldoende prioriteit krijgen in veranderprocessen, omdat ze zich richten op het realiseren van business value. Zo worden keuzes gemaakt om alleen key risico's (half) te automatiseren.

Het verschil met de reeds bekende Application Controls is dat het bij Control by Design draait om het inrichten van een proces op dusdanige wijze dat bepaalde risico's direct vanuit de procesinrichting worden beheerst (worden voorkomen dan wel gemitigeerd). Dit betekent dat het proces en de bijbehorende risico's het vertrekpunt zijn, en niet het automatiseren van reeds bestaande beheersingsmaatregelen. Daarbij is het van belang te zorgen voor een goed samenspel tussen de proceseigenaar (die weet hoe zijn proces in elkaar zit), de risk manager (die weet waar in het proces de risico's en controls zich manifesteren) en de IT'er (die weet welke systemen en data gebruikt worden in het proces). Door het aansluiten van het risicomanagementproces op het ontwikkelingsproces van een product en/of systeem(aanpassing) zorg je ervoor dat het identificeren van de grondoorzaak van de belangrijkste risico's, en het automatiseren van de bijbehorende controls, standaard onderdeel wordt van het verandermechanisme van de organisatie. Bij het bepalen van de prioriteiten van je veranderkalender zorg je ervoor dat duidelijk is welke risicogerelateerde veranderingen (bijvoorbeeld het implementeren van een harde invoercontrole) kunnen worden meegenomen bij geplande aanpassingen (bijvoorbeeld het aanpassen van invoerschermen). Het is immers goedkoper om de rioleringsbuis te vervangen als de straat toch opengaat om het glasvezelnetwerk aan te leggen.

Het idee daarbij is zoals bijvoorbeeld Elon Musk dat benoemt in zijn First Principles-aanpak: ga terug naar de basis. Wanneer je vanuit het niets het proces opzet in plaats van dat je een bestaand proces aanpast, kom je waarschijnlijk met een ander ontwerp. Dit werkt het beste in een greenfieldsituatie, waar alle ontwerpkeuzes nog gemaakt kunnen worden en je weinig rekening hoeft te houden met een bestaand systeemlandschap waarbinnen je processen worden uitgevoerd. De realiteit is dat die situaties weinig voorkomen. Je moet dus streven naar een situatie waarin de *verander*processen standaard rekening houden met de doelstellingen van Control by Design. In dit artikel ligt de nadruk op die uitdaging.

Voorbeeld

Een voorbeeld is het geven van een korting op een tarief. Uiteraard kan daarbij worden gekeken naar de systeemondersteuning door bevoegdheden in te regelen in het systeem. Een efficiëntere stap is het systeem te laten bepalen wie de korting zou mogen hebben en hoe hoog die dan moet zijn. En als de bediening ook prima vanuit vaste tarieven kan werken, dan zou het proces al zo ingericht moeten zijn dat korting überhaupt niet mogelijk is. Zo wordt het risico op onjuiste of onterechte kortingen vanuit het proces afgedwongen. Je gaat hierin terug naar de basis: het (her)ontwerp van je proces en systeem.

Control by Design richt zich in essentie op het zo veel mogelijk voorkomen van risico's in de systeeminrichting van je proces

CONTROL BY DESIGN TOEPASSEN IN DE PRAKTIJK

Voor het toepassen van Control by Design blijven traditionele risicomanagement- of procesmodellen gewoon overeind. Sterker nog, voor een brede acceptatie en goede werking is het van belang om Control by Design te borgen in de modellen die de organisatie hanteert.

Zoals eerder aangegeven is het daarbij belangrijk om verschillende disciplines zo veel mogelijk bij elkaar te brengen: de proceseigenaar, risk en IT, kijkend vanuit risicoperspectief met IT als de oplossingsrichting om de risico's te mitigeren. Hier komen twee processen bij elkaar: de risicomanagementcyclus en het ontwikkelproces. Dit zijn dan ook de plekken om het gedachtegoed binnen je organisatie te verankeren.

We onderkennen vier belangrijke randvoorwaarden voor het succes van Control by Design. De eerste randvoorwaarde is Control by Design toe te passen tijdens het implementeren van nieuwe systemen en het digitaliseren en/of het aanpassen van processen. Daarvoor is het ontwikkelproces van toepassing. Het ontwikkelproces doorloopt de verschillende fasen van intake, analyse en bepaling van de requirements, om vervolgens deze requirements te bouwen en implementeren. Of je nu volgens een waterval-, Agile- of andere ontwikkelingsmethodiek werkt, het komt er altijd op neer dat je tijdens het ontwikkelproces ook meerdere stappen van de risicomanagementcyclus doorloopt, van het identificeren van je risico's tot aan het mitigeren en bepalen van je monitoringstrategie. Met Control by Design wil je aanhaken bij deze stappen en gericht kijken waar systeemondersteuning kan plaatsvinden om je risico's te verkleinen of, beter nog, weg te nemen. Om dat te kunnen doen moet helder zijn welk onderdeel je aan het ontwikkelen of veranderen bent binnen het gehele proces (end-to-end procesbenadering). Om vervolgens bij het identificeren en uiteindelijk mitigeren

van de risico's gebruik te maken van de brede expertise (business, risk en IT). Voor het mitigeren van het risico is het van belang dat je echt de grondoorzaak van het risico scherp hebt. Hiervoor kun je methodieken als de 'BowTie' en 'Five Times Why' gebruiken. De BowTie-methode splitst de risicobeschrijving in een oorzaak, gebeurtenis en gevolg ([Culw16]). De oorzaak kun je vervolgens verder uitdiepen door meerdere malen de vraag te stellen waarom het risico hierdoor ontstaat. Zo kom je tot de uiteindelijke grondoorzaak ([Serr17]).

Dat brengt ons bij de tweede randvoorwaarde: zorg ervoor dat je tijdens het ontwerp, over de gehele breedte van de keten, weet waar de key risico's zich bevinden. Het end-to-end inzicht vanuit de brede expertise is op dat moment nodig, omdat de werkelijke grondoorzaak van een risico in een heel ander deel van het proces kan voorkomen dan waar op het moment van de verandering de focus op ligt. Hierbij kan bijvoorbeeld gedacht worden aan onvolledige documentaanlevering door een klant met het risico op non-compliance in het uiteindelijke advies of fiatteringsproces voor een productaanvraag. Dit risico kan in de afsluitfase worden gemitigeerd, terwijl de oorzaak van het risico in de intakefase kan worden weggenomen. Met de end-to-end procesbenadering worden risico's over de gehele keten geïdentificeerd en kunnen beheersingsmaatregelen worden geïmplementeerd op (of zo dicht mogelijk bij) de plaats waar ze ontstaan. Naast het risicomanagementmodel en ontwikkelproces is de end-to-end procesbenadering een derde invalshoek waar Control by Design aan gekoppeld moet worden. Hiermee wordt voorkomen dat beheersingsmaatregelen die hetzelfde risico mitigeren dubbel worden geïmplementeerd. Vanuit de traditionele risicoanalyse is deze stap voor Control by Design van extra belang om het ontwerp op de juiste plaats en tijdig vorm te geven. Je kunt de rioleringsbuis vervangen waar de straat opengaat, maar als het werkelijke probleem is dat veel te veel water moet worden afgevoerd, kun je beter zorgen dat de tegels vervangen worden door stadstuintjes.

De derde randvoorwaarde is dat wordt uitgegaan van standaardisatie alvorens te digitaliseren. Voor Control by Design is het principe dat hoe meer je standaardiseert, hoe simpeler het proces en hoe eenvoudiger het wordt om een risico te voorkomen. Dit is niet nieuw en blijft de basis, maar dit is niet altijd mogelijk. Een indicatie hiervoor is te veel afwijkingen in het proces. Verderop in het artikel gaan wij hier dieper op in.

De vierde randvoorwaarde is te beschikken over de juiste data om een goed functionerende geautomatiseerde beheersingsmaatregel (Application Control) te kunnen hanteren. Je moet dus weten welke data je op welk moment in je proces nodig hebt. En deze data moeten juist zijn om je ingerichte maatregel goed te laten functioneren. Er geldt immers: garbage in = garbage out. Data dienen te worden opgehaald bij betrouwbare bronnen, waarna de juistheid van de data moet worden vastgesteld voordat je die verder in je keten brengt.

Figuur 1. Vier randvoorwaarden voor Control by Design.

Voorbeeld

Klantbeheer is belangrijk binnen de totale klantbediening. Heeft de klant nog steeds het best passende product? Om klantbeheer goed te kunnen inrichten is het nodig om contactmomenten met de klant te plannen, gesprekken te voeren, de vastlegging goed te administreren en de benodigde acties die uit het gesprek komen te plannen. Hoge werkdruk en operationele fouten vormen risico's voor dit proces. Gebruikmakend van een goede systeemondersteuning zijn meerdere procesrisico's te verkleinen. De CRM-software bouwt triggers in voor het inplannen van het beheergesprek. Tijdens het gesprek doorloopt de adviseur met de klant een beheerstappenproces binnen het systeem, vult direct de vragen in en legt de keuzes in het systeem vast. Het gespreksverslag kan systeemtechnisch niet worden afgerond voordat de medewerker zij/haar toelichting heeft gegeven bij een uitzondering of klantkeuze. Vervolgens slaat het systeem het verslag automatisch op in het klantdossier en e-mailt het naar de klant zelf. Veel handelingen worden zo door het systeem overgenomen. Het risico dat niet tijdig in gesprek wordt gegaan met de klant, dat niet wordt zorg gedragen voor een goed gesprek en voor vastlegging daarvan, en dat de relevante informatie niet daadwerkelijk wordt ontvangen, is verkleind.

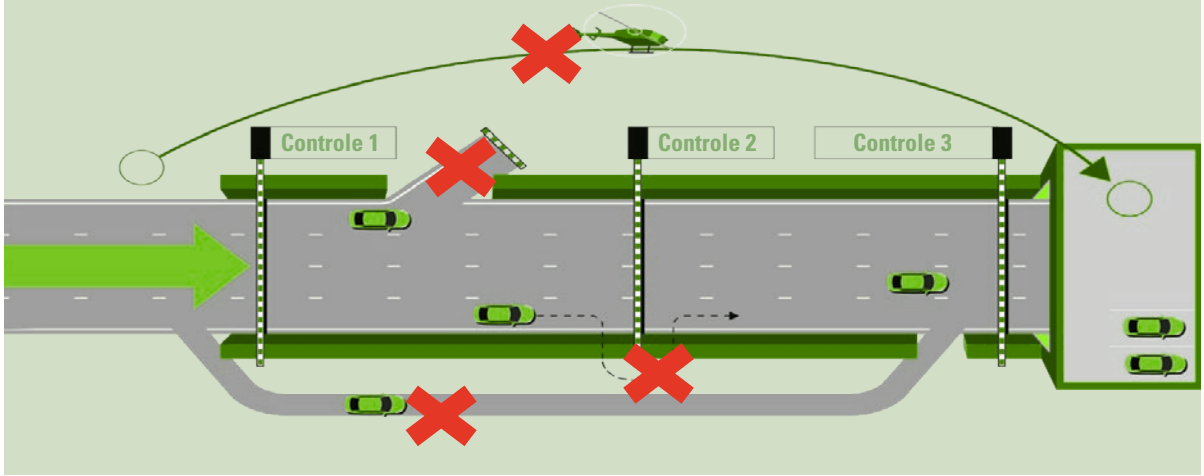
Toepassen van Control by Design is makkelijker gezegd dan gedaan

Op papier ziet het er eenvoudig uit en vindt het idee veel medestanders die er de voordelen van inzien, niet in de laatste plaats vanuit het perspectief van kostenbesparing. Wie wil nu niet meer gebruikmaken van geautomatiseerde beheersingsmaatregelen om handwerk te voorkomen of het maken van fouten überhaupt onmogelijk te maken? De praktijk is echter weerbarstig, zeker in een complexere organisatie en een ingewikkeld IT-landschap waar al jaren geen sprake meer is van een greenfieldsituatie. Zonder specifiek rekening te houden met de dilemma's die Control by Design opwerpt, loopt de kans op een succesvolle toepassing sterk terug.

Enkele belangrijke zaken om op voorhand rekening mee te houden:

1. **Control by Design is niet noodzakelijkerwijs het automatiseren van de bestaande manual controls**
   Handmatige controls in het proces worden op een andere manier uitgevoerd dan Application Controls of IT Dependent Manual Controls. Er kan bijvoorbeeld meer sprake zijn van professional judgement, informatie die nodig is voor de uitoefening van de control kan op verschillende manieren via verschillende applicaties bij de beoordelaar moeten komen, informatie is vastgelegd in documenten, enzovoort. Het automatiseren van de handeling die de controleur uitvoert is niet het doel van Control by Design: de stap moet idealiter overbodig worden (bijvoorbeeld via een preventieve control op de juiste plek in de keten). Dit verschil moet duidelijk zijn om teleurstelling in de uitwerking van Control by Design te voorkomen en daarmee het succes daarvan in de weg te staan.
2. **Te veel afwijkingen in het proces zijn ook voor Control by Design niet goed op te lossen**
   Een complex proces is lastiger te beheersen. Wanneer er veel product-/procesvariaties zijn, is het veel werk om op alle afwijkingen een geautomatiseerde, preventieve beheersingsmaatregel te implementeren die ook werkelijk het risico in de keten mitigeert. Open normen, benodigde professional judgement in de behandeling en veel ruimte voor overrules maken dat het systeem slecht dicht te zetten is. Theoretisch kan alles worden geautomatiseerd, maar dan wel tegen onverantwoorde kosten en met als gevolg dat de systemen op hun beurt weer te complex worden.
   Hoe beter de processen zijn gestandaardiseerd en hoe meer productrationalisatie heeft plaatsgevonden, des te beter de systemen kunnen worden ingericht op preventieve geautomatiseerde controls.
3. **Control by Design kost ook verandercapaciteit en vereist dus prioriteit**
   Het implementeren en toepassen van Control by Design vereist commitment en een investering voorafgaand aan de concrete IT-implementatie, die ten koste gaan van de beschikbare verandercapaciteit zelf. Agile development teams met overvolle backlogs sturen aan op het realiseren van zo veel mogelijk business value. Een bewuste prioritering van de requirements van Control by Design is dus

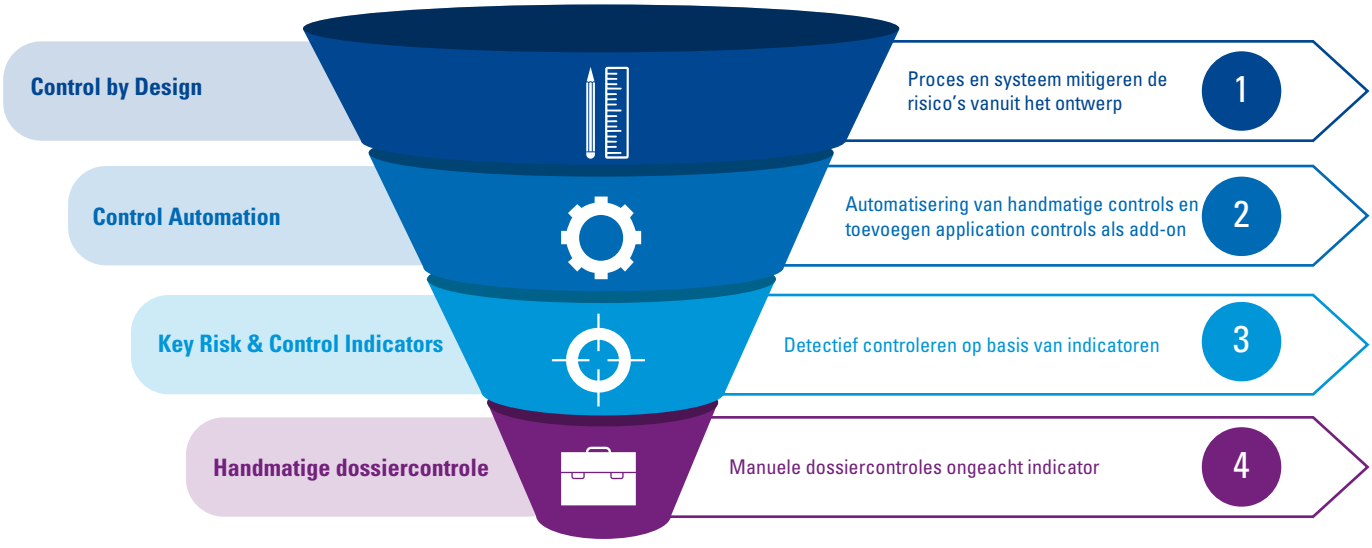
Figuur 2. De snelweg. Control by Design standaardiseert het primaire proces en elimineert of monitort zo mogelijke afwijkingen waarmee controls omzeild kunnen worden.



noodzakelijk maar niet populair – de waarde wordt pas duidelijk bij het voorkomen van handmatige (lijn)werkzaamheden waarvan de kosten niet worden afgezet tegen de opbrengst van andere changes die in een sprint worden geprioriteerd. Daarom kan Control by Design niet vrijblijvend worden geïntroduceerd: afwijkingen van de Control by Design-principes en -stappen in het veranderproces moeten zichtbaar worden gemaakt en moeten worden beheerst. Afwijkingen moeten dan formeel worden goedgekeurd en bij tijdelijke acceptatie dient erop te worden gestuurd dat deze de juiste prioriteit op de backlog krijgen. Wanneer je bij een systeemverandering alsnog een handmatige check inregelt in plaats van dat je de grondoorzaak wegneemt, dan is dit een afwijking van de Control by Design-principes. Je zult hiervoor dan een bewuste goedkeuring moeten vragen.

4. **Zicht op de keten en de risico's daarin helpt bij het maken van de juiste ontwerpkeuzes**
   Een belangrijk doel van Control by Design is dat de risico's voorkomen moeten worden op de plek waar zij ontstaan. Maar waar is dat? De ketens zijn vaak lang en complex en overstijgen de verantwoordelijkheid van individuele teams – op zowel functioneel, infrastructureel als applicatieniveau. Onderdelen van de keten of technologie kunnen zijn geoutsourcet. Andere onderdelen van de keten maken misschien gebruik van legacy producten. Veranderingen aanbrengen in die delen van de keten is vaak gecompliceerd, kostbaar en niet toekomstbestendig. In de praktijk is het lastig om alle benodigde kennis op tafel te krijgen om de juiste inzichten te leveren, zeker wanneer dat keteninzicht frequent moet worden verkregen. Procesdocumentatie is verouderd, onvolledig of onvoldoende gedetailleerd. Medewerkers die de hele keten kunnen overzien, zijn schaars. Een (key-)risicoanalyse op ketenniveau met een goed begrip van de grondoorzaken van risico's is hierbij onontbeerlijk. Ook dit benadrukt de betrokkenheid van de driehoek proces, IT en risico met als doel elkaar te versterken en het proces te versnellen. Derhalve dient ervoor gezorgd te worden dat ten tijde van de uitwerking van de (IT-)roadmap echt de tijd wordt genomen voor het goed in kaart brengen van de risico's en oorzaken hiervan. Hiermee kun je duidelijke kaders meegeven voor de ontwikkeling van de losse onderdelen zelf.
5. **De verantwoordelijkheid voor de implementatie kan ergens anders liggen dan waar het risico moet worden beheerst**
   Zelfs wanneer de risicoanalyse de vinger op de zere plek legt en de grondoorzaakanalyse met alle benodigde kennis van de keten en systemen aanwijst wat er moet veranderen om een preventieve maatregel te implementeren, ligt de benodigde wijziging niet altijd in het domein van het team dat de impact voelt van het risico en waar de control is geïmplementeerd.
   Een ander scrum-/ontwikkelteam heeft zijn eigen prioriteiten en zal vaak niet op hetzelfde moment een implementatie starten. Daardoor worden pleisters geplakt op de plek waar de capaciteit op dat moment wél beschikbaar is. Maar met een geplakte pleister is de druk weg om de grondoorzaak aan te pakken (start opnieuw bij punt 3: commitment en prioriteit).
   De plantsoenendienst heeft nu geen tijd om de stadstuintjes aan te leggen, dus misschien toch voor nu maar de rioleringsbuis vervangen?

Figuur 3. Control by Design Funnel.



CONTROL BY DESIGN FUNNEL ALS ALTERNATIEF

In het begin van het artikel wordt het verlagen van de 'cost of control' hoofdzakelijk uitgesplitst in twee onderdelen. Met het (geautomatiseerd) voorkomen van het risico krijg je lagere beheerskosten in het primaire proces zelf. Een andere manier om de 'cost of control' te verlagen zit in effectievere monitoring. Monitoring wil zeggen het toezien op de effectieve werking van je beheersingsmaatregel, vaak in de vorm van controles. Handmatige dossiercontrole is hierin de meest arbeidsintensieve vorm van monitoring. Hier kun je de Control by Design Control Funnel toepassen. Dit houdt in dat het hoogst mogelijke niveau van (geautomatiseerde) risicobeheersing wordt gebruikt bij het ontwikkelproces. Een lager niveau wordt enkel onderzocht als hogere niveaus niet mogelijk zijn of de baten niet de kosten dekken.

Voorbeeld

In een ideaal scenario wordt het risico op het missen van het beheergesprek en het vastleggen van de uitkomsten voorkomen door de procesaanpassing zoals benoemd in het vorige voorbeeld. Als dat voor nu een stap te ver is, kan worden gekeken naar een geautomatiseerde monitoring of alle uitgevoerde gesprekken van die week daadwerkelijk een gespreksverslag in het klantdossier hebben zitten (aanwezigheid). En of alle vrije velden binnen het gespreksverslag gevuld zijn (inhoud). Mocht ook deze monitoring niet automatisch in te regelen zijn, dan kun je naar de volgende laag in de funnel kijken, op basis van indicatoren. Vastgesteld is dat de oorzaak van een onjuist gespreksverslag komt door tijdsgebrek van de adviseur. Als het verslag binnen een dag na het gesprek wordt opgesteld, worden bijna nooit fouten geconstateerd. Mocht het langer duren, dan is de foutkans exponentieel gegroeid. Een indicator is dan een middel om te bepalen of de beheersingsmaatregel voldoende werkt. Alleen als de indicator aangeeft dat minder dan 95% van de beheerverslagen binnen 2 dagen na het gesprek is opgeslagen, wordt aanvullend gecontroleerd op de kwaliteit. Dergelijke monitoring vereist wel dat je de juiste informatie uit de systemen kunt halen. De manier van monitoring moet dan ook tijdens het ontwikkelingsproces worden meegenomen en als requirement bij de bouw worden ingebracht. Anders is vaak funnel niveau 4, dossiercontroles, de enige arbeidsintensieve manier om te zien of het proces al dan niet 'in control' is.

Om de funnel goed te kunnen gebruiken is het van belang om tijdens je risicoanalyse niet alleen te kijken naar de beheersingsmaatregelen, maar ook naar de manier van monitoring hierop. Zoals in de introductie benoemd, zien we dat er binnen organisaties steeds meer zekerheid wordt gezocht door het testen van de werking van de beheersingsmaatregelen te intensiveren en te monitoren of bepaalde risico's zich niet alsnog voordoen. Geautomatiseerd testen (funnel optie 2, zie figuur 3) en slimmer testen door gebruik te maken van data (funnel optie 3) zullen in die zin bijdragen aan het verlagen van de 'cost of control'. Om dit goed te kunnen inrichten zul je ook hier al tijdens je ontwikkelproces rekening mee moeten houden en moeten zorgen dat de juiste requirements worden meegegeven aan de softwareontwikkeling.

CONCLUSIE: CONTROL BY DESIGN IS EEN BELANGRIJK CONCEPT VOOR KOSTENBESPARING EN BETERE RISICOBEHEERSING

Voor het implementeren van Control by Design bestaat geen blauwdruk. Organisaties verschillen van elkaar, en de manier waarop Control by Design wordt geïmplementeerd, kan daarom variëren. Dit is onder andere afhankelijk van de tijd, de maturity van de (deel)organisatie en de bereidheid het concept te omarmen. Daarom is het belangrijk toe te werken naar doelstellingen die voor een specifieke organisatie haalbaar zijn.

Control by Design is een belangrijk concept om je risico's beter te beheersen en de 'cost of control' te verlagen. Het implementeren van het concept klinkt simpel, maar dat is het in de praktijk niet. Er zijn verschillende problemen waar je tegenaan kunt lopen. De implementatie van Control by Design vraagt om veranderprioriteit en een

Voor het implementeren van Control by Design bestaat geen blauwdruk

end-to-end benadering met de juiste expertises aan tafel waarbij niet alle teams en belanghebbenden op hetzelfde niveau zitten. Het is een proces van de lange adem dat inherent is aan het veranderproces. Bij de uitrol komt het aan op kleine stappen in plaats van een radicale verandering. Het is daarbij van belang om wel de juiste keuzes te maken in hoe je omgaat met de spaarzame IT-capaciteit: zorg dat je beheersingsmaatregelen maar één keer hoeft te ontwikkelen door deze op de juiste plek toe te passen. De inspanning tijdens je ontwikkeling verdien je na de implementatie dubbel en dwars terug. Je hebt dan geen continue bijsturing op niet-functionerende beheersingsmaatregelen en voorkomt dure monitoring en dossiercontroles om te zien of het proces goed verloopt.

Dit vraagt om een goede verankering van het gedachtegoed in je bestaande ontwikkel- en risicoprocessen. Maak de stappen en hulpmiddelen daarom zo concreet mogelijk. En maak het niet vrijblijvend: maak het meetbaar en zichtbaar en stuur bij op afwijkingen.

Daarnaast zijn er vaak ook andere initiatieven die met Control by Design samenhangen. Denk daarbij aan Security en Privacy by Design, Business Process Management of implementaties op softwareontwikkelmethoden zoals Agile. Deze initiatieven kunnen elkaar versterken en de beweging versnellen. Maak hier dan ook gebruik van om zo de krachten te bundelen. De initiatieven richten zich op goed zicht op de processen en op het zo veel mogelijk verankeren van de belangrijkste principes in het procesontwerp. Ook zijn deze concepten inherent aan digitalisering. Control by Design biedt hier overkoepelend ondersteuning aan als een paraplu voor verdere versimpeling van de beheersingsomgeving door de kansen te pakken van de digitaliseringsstrategie.

Herken je de wens om dit toe te passen, ben je benieuwd naar de ervaringen of wil je meer weten? Dan roepen wij je van harte op om hierover met ons van gedachten te wisselen.

Literatuur

[CIIA21] Chartered Institute of Internal Auditors (2021). *Position paper: The three lines of defence.* Geraadpleegd op: https://www.iia.org.uk/resources/delivering-internal-audit/position-paper-the-three-lines-of-defence/

[Culw19] Culwick, M.D. et al. (2016). Bow-tie diagrams for risk management in anaesthesia. *Anaesthesia and Intensive Care 44*(6), 712-718. Geraadpleegd op: https://journals.sagepub.com/doi/pdf/10.1177/0310057X1604400615

[ISAC11] ISACA Journal Archives (2011, 1 september). IT General and Application Controls: The Model of Internalization. *ISACA Journal.* Geraadpleegd op: https://www.isaca.org/resources/isaca-journal/past-issues/2011/it-general-and-application-controls-the-model-of-internalization

[Serr17] Serrat, O. (2017). Proposition 32: The Five Whys Technique. In O. Serrat, *Knowledge Solutions* (pp. 307-310). Geraadpleegd op: https://www.researchgate.net/publication/318013490_The_Five_Whys_Technique

Over de auteurs

Ing. Thomas Schoonhoven is Risk Control Partner binnen Rabobank. Na meerdere riskmanagementfuncties in de eerste en tweede lijn is hij is thought leader Control by Design en verantwoordelijk voor de implementatie binnen het Retail NL-domein.

Drs. Robin Polder is Lead Data & Technology voor Coöperatief Klantbelang binnen Retail NL bij Rabobank. Hij heeft een achtergrond in IT-audit en grote IT-transformaties binnen de financiële sector. Binnen Rabobank is hij verantwoordelijk voor de inzet van data-analyse en technologische oplossingen voor het signaleren, voorkomen en indien nodig uitvoeren van (potentiële) herstelprogramma's.

Bart Olieman is Productmanager Bedrijven binnen Rabobank. Hij heeft op het gebied van zakelijke financiering uiteenlopende functies bekleed. Momenteel houdt hij zich bezig met risicomanagement. Hij is er een groot voorstander van om binnen organisaties risico's meer geautomatiseerd en efficiënter te beheren voor een goede risicobeheersing. Binnen de Squad Control by Design geeft hij hier uitvoering aan.

Mourad Fakirou MSc RE is manager binnen KPMG's Digital Transformation-afdeling. Hij heeft de afgelopen vijf jaar ruime ervaring opgebouwd in de financiële en tech-sector. Daarbij combineert hij zijn expertise rondom strategie met IT.