MAB MAANDBLAD VOOR ACCOUNTANCY EN BEDRIJFSECONOMIE

Maandblad voor Accountancy en Bedrijfseconomie 98(4) (2024): 121–129
DOI 10.5117/mab.98.110223

Research Article

Monitoring SoD-controles; een oplossing voor complexe autorisatiestructuren in SAP?

Lieke-Rosa Koetsier

Received 29 July 2023 | **Accepted** 27 August 2024 | **Published** 18 September 2024

Samenvatting

Het autorisatieconcept van SAP ECC en SAP S4 is complex, en veel bedrijven hebben moeite om dit op een effectieve manier in te richten. Hierdoor is het vaak niet duidelijk of de essentiële functiescheidingen wel op orde zijn, die traditioneel worden afgedwongen door autorisaties. Om meer inzicht te verkrijgen in de ingerichte functiescheiding, wordt echter steeds vaker gekeken naar controles op uitgevoerde acties dan naar ingerichte autorisaties, omdat ingerichte autorisaties moeilijk inzichtelijk te maken zijn. SAP biedt verschillende producten met deze functionaliteiten aan om hun klanten te ondersteunen bij deze monitoring. Dit artikel onderzoekt het effect van het (gedeeltelijk) vervangen van autorisaties door monitoring SoD-controles, de hieraan verbonden voordelen en risico's en welk type monitoring SoD-controle het meest bruikbaar is in welke situatie.

Hiertoe is literatuuronderzoek gedaan en er zijn interviews gehouden met verschillende professionals in dit vakgebied, onder wie medewerkers van SAP.

Relevantie voor de praktijk

Het tijdperk van monitoringcontrole is pas net begonnen; de mogelijkheden om realtime of zelfs preventief te kunnen monitoren staan nog in de kinderschoenen. Naarmate de mogelijkheden steeds meer zullen worden uitgebreid, zal dit voordelen en risico's met zich meebrengen voor organisaties. Het is belangrijk om over de mogelijke gevolgen na te denken, om eventuele risico's al tijdens het ontwikkelen van de tools te identificeren en te mitigeren, nog voor de programmatuur op de markt komt.

Trefwoorden

SAP ECC, SAP S4, autorisatie, functiescheiding, Segregation of Duties (SoD), monitoring

1. Inleiding

Het meest gebruikte ERP-pakket is het welbekende Duitse product SAP (Martens 2019). Zoals aangegeven door Vreeke and Hallemeesch (2006) en Van der Zon et al. (2013) is het autorisatieconcept van SAP ECC en SAP S4[1] complex. Veel bedrijven hebben moeite om dit op een effectieve manier in te richten, waardoor er geen overzicht is van welke gebruikers welke rechten hebben. Hierdoor is het vaak niet duidelijk of de essentiële functiescheidingen wel op orde zijn. Zo kan het bijvoorbeeld gebeuren dat de crediteurenadministrateur via de ene taak de autorisatie voor een betaalrun krijgt en via een andere taak toegang tot stamdata van crediteuren. Los van elkaar vormen deze autorisaties geen probleem, maar in samenhang leveren ze een conflict op (Fluitsma 2018).

Binnen SAP ECC en SAP S4 zijn er verschillende methoden om autorisaties toe te kennen aan gebruikers. Zo moet er rekening worden gehouden met profielen, groepen en verschillende soorten rollen, zoals enkele rollen, afgeleide rollen en samengestelde rollen (SAP 2021). Dit maakt het autorisatieconcept extra ingewikkeld.

Daarnaast zijn er binnen de SAP S4-standaard al 3700 autorisatieobjecten beschikbaar. Het toekennen van rechten in SAP ECC en SAP S4 verlangt een balans binnen het bedrijf dat de software gebruikt. Zoals aangegeven door Roest and De Rooij (2008) ontstaan er conflicten indien er te veel rechten worden vergeven en kunnen gebruikers hun werk niet doen als er te weinig rechten worden vergeven.

Aan de basis van dit probleem ligt het onderhouden van rollen in SAP ECC en SAP S4. Radkowski* (2021) geeft aan dat er in veel gevallen een wildgroei aan rollen ontstaat die niet meer te overzien is, wat het toekennen van de juiste rechten bemoeilijkt en het kunnen bepalen of gebruikers de juiste rechten hebben. Van der Voort* (2021) geeft aan dat wanneer er geen duidelijke structuur is in de rollen, het erg moeilijk is om deze te onderhouden.

Vanuit het oogpunt van interne controle gezien, dienen organisaties functiescheiding te controleren in processen waar geen applicatiecontroles of manuele controles zijn ingericht. Traditioneel wordt deze functiescheiding afgedwongen door autorisaties. Om meer inzicht te verkrijgen in de ingerichte autorisaties, wordt echter steeds vaker gekeken naar controles op uitgevoerde acties dan naar ingerichte autorisaties, omdat ingerichte autorisaties moeilijk inzichtelijk kunnen worden gemaakt. Zoals aangegeven door Van der Zon et al. (2013) zijn hiervoor verschillende SAP access control-applicaties ontwikkeld. In deze tools kunnen vooraf regels worden gedefinieerd, zoals ‘gebruikers mogen geen betaalrun uitvoeren voor crediteuren van wie zij zelf het bankrekeningnummer hebben aangepast’.

De effectiviteit van deze controle kan vervolgens worden gemonitord door rapportages te genereren, meldingen te geven en/of door verdachte transacties te blokkeren. Om hun klanten te ondersteunen bij deze monitoring, biedt SAP verschillende producten aan die deze functionaliteiten bieden, waaronder SAP Access Violation Management (Frenehard 2021), SAP Business Integrity Screening (SAP 2017) en SAP UI Masking (SAP 2020). Deze functionaliteiten zijn momenteel geen onderdeel van de SAP-standaardprogrammatuur. De verschillende tools zijn los van elkaar ontwikkeld en zijn niet standaard met elkaar geïntegreerd.

Dit onderzoek bekijkt de mogelijke effecten van het (gedeeltelijk) vervangen van autorisaties door monitoringcontroles, welke voordelen en risico’s hieraan verbonden zijn en welke van deze controles in welke situaties het meest bruikbaar zijn. In het verleden was het vervangen van autorisaties door monitoringcontroles niet mogelijk, maar door de ontwikkeling van nieuwe technologie bestaat deze mogelijkheid nu wel. Veel van deze problematiek speelt ook in andere ERP-pakketten, maar in het kader van dit onderzoek is er specifiek gekeken naar SAP ECC en SAP S4 (hierna afgekort tot SAP). Monitoringtools zijn toepasbaar op tal van controles, maar binnen dit onderzoek is gefocust op SoD-controles. Hierbij spreken we dan specifiek over SoD-controles die standaard met autorisaties worden ingericht en dus niet over applicatiecontroles, zoals het 4-ogenprincipe.

Box 1. Begrippenlijst.

- Controle: een door een organisatie uitgevoerde preventieve of detectieve controle.
- Controle-eigenaar: de verantwoordelijke voor het uitvoeren van de controle.
- Continuous monitoring: het automatisch continu monitoren van een IT-omgeving.
- Data-gebonden autorisaties: autorisaties op basis van de acties die een gebruiker heeft uitgevoerd in het systeem. Voorbeeld: wanneer er gebruik wordt gemaakt van niet-data-gebonden autorisaties, kan een gebruiker wel of niet geautoriseerd zijn om een factuur goed te keuren. Wanneer er gebruik wordt gemaakt van data-gebonden autorisaties, is het ook mogelijk om de gebruiker te autoriseren om facturen goed te keuren – op voorwaarde dat de gebruiker deze niet zelf heeft ‘ingelegd’.
- SAP ECC en SAP S4: veelgebruikte versies van het softwarepakket SAP.
- Transactie: een uitgevoerde actie die behoort te worden gedocumenteerd in het systeem. Bijvoorbeeld een order, ontvangen factuur, betaling, goederenontvangst, goederenafgifte, etc.

1.1. Monitoringcontroles

De volgende vormen van monitoring SoD-controles zijn in dit onderzoek bekeken:

1. Controle 1: periodieke rapportages
   Uitzonderingen worden periodiek gerapporteerd in de vorm van rapportages. De controle-eigenaar inspecteert de rapportages en onderneemt actie indien nodig.
2. Controle 2: realtime meldingen
   Direct wanneer zich een uitzondering voordoet, wordt deze gemeld aan de controle-eigenaar, die meteen actie kan ondernemen.
3. Controle 3: realtime melding, blokkeren en een workflow
   In navolging van de realtime melding bij de controle-eigenaar van een uitzondering die zich voordoet, worden de transacties geblokkeerd waarin een uitzondering is geconstateerd. De controle-eigenaar inspecteert de uitzondering, neemt maatregelen indien nodig en deblokkeert de transacties indien dit wenselijk is.
4. Controle 4: melding, blokkeren nog voor er op verzenden is geklikt en een workflow
   Als een gebruiker gegevens in een transactie invoert die tot een uitzondering zouden leiden, wordt de transactie geblokkeerd, nog voor er op verzenden is geklikt. De ingevoerde gegevens worden niet in een transactie opgeslagen, maar in een aparte tabel. De controle-eigenaar wordt realtime op de hoogte gesteld. Hij inspecteert de uitzondering, bepaalt welke acties er moeten worden ondernomen en deblokkeert eventueel de transactie. Indien ervoor wordt gekozen om te deblokkeren, worden de gegevens vanuit de aparte tabel overgenomen in de transactie, waarmee verder gewerkt kan worden. Controle 4 kan ook worden uitgevoerd zonder de workflow. In dit geval spreken we over de volgende controle: wanneer een gebruiker gegevens in een transactie invult die tot een uitzondering zouden leiden, wordt de transactie geblokkeerd, nog voor er op verzenden is geklikt. De gegevens worden in dit geval niet opgeslagen en het is onmogelijk om deze transactie aan te maken.

1.2. SAP tools

In dit onderzoek worden drie SAP tools bekeken, namelijk SAP Access Violation Management, SAP Business Integrity Screening en SAP UI Masking.[2] Hierna is per tool een korte toelichting gegeven.

1.2.1. SAP Access Violation Management

De SAP Access Violation management tool is geschreven door Pathlock (voorheen Greenlight), een partner van SAP. Dit is gedaan in reactie op de invoering van de SOx-wetgeving. De tool geeft meldingen, waarmee de organisatie inzicht krijgt wanneer de SoD (functiescheiding) doorbroken wordt. Deze worden traditioneel gegeven in de vorm van periodieke rapportages. De tool kan ook gebruikt worden om de financiële impact van specifieke toegangsrisico's te bepalen.

1.2.2. SAP Business Integrity Screening

De SAP Business Integrity Screening tool is door SAP geschreven om het gemakkelijker te maken om verdachte transacties te detecteren. Dit was voor het eerst mogelijk na de introductie van de HANA database (de naam die SAP aan de database achter SAP ECC en SAP S4 heeft gegeven). De tool geeft inzicht door de grote hoeveelheden data te analyseren die beschikbaar zijn in SAP. Op basis van deze data wordt bepaald welke transacties potentieel verdacht kunnen zijn, zodat de organisatie dit kan beoordelen en actie kan ondernemen indien nodig. De incidenten worden weergegeven in dashboards om overzicht te creëren. Ook kunnen er meldingen worden gegeven wanneer uitzonderingen zich voordoen en verdachte transacties kunnen worden geblokkeerd.

Box 2. Geïnterviewde personen.

In het kader van dit onderzoek heeft de auteur 11 personen geïnterviewd. In de loop van dit artikel wordt naar uitspraken en/of inzichten van hen verwezen. Om duidelijk te maken dat het om een verwijzing naar een geïnterviewde persoon gaat – en niet om een literatuurverwijzing – is de naam van de betreffende persoon steeds gemarkeerd met een asterisk.

- C. Dommerholt (Hoofd Business Risk services bij Grant Thornton), 12 november 2021.
- G. Hafner (Chief Product Owner for SAP Business Integrity Screening), 16 juli 2021.
- D. Hallemeesch (Partner Enterprise Solutions bij KPMG), D. Ashruf (Director Advisory bij KPMG), I. Spruit I (Senior manager IT Advisory bij KPMG), 3 november 2021.
- T. Keller (Product manager for UI Masking at SAP), A. Verma (Product owner of the UI Masking tool at SAP), 8 september 2022.
- R. Lagendijk (Partner Assurance bij Grant Thornton), 24 september 2021.
- C. Radkowski (Solution manager for SAP Identity Access Governance and Access Control), 2 juli 2021.
- S. Stapleton (Vice president, Customer Advisory at Pathlock), 7 juli 2021.
- J. van der Voort (2021, 9 juli) (SAP S&A Consultant bij Heineken), 9 juli 2021.

1.2.3. SAP UI Masking

De SAP UI Masking tool is ontwikkeld door SAP in reactie op de invoering van de GDPR-wetgeving. De tool wordt gebruikt om potentieel gevoelige data onzichtbaar te maken voor specifieke gebruikers. Hiermee geeft het organisaties de mogelijkheid om beter te controleren welke gebruiker welke data kan inzien. Naast deze Masking functionaliteit is het met de UI Masking tool ook mogelijk om de functionaliteit van specifieke knoppen te blokkeren in specifieke gevallen met de 'Data Exploit Prevention' functionaliteit. De huidige versie van de Data Exploit Prevention functionaliteit heeft de mogelijkheid om het aanmaken van specifieke transacties te blokkeren in specifieke gevallen. De gebruiker krijgt in dat geval een melding dat deze transactie niet kan worden aangemaakt. De data die de gebruiker in dit geval ingeeft in de transactie, zal dan niet worden opgeslagen. Keller en Verma* (2022) geven aan dat mogelijkheden voor configuratie van de acties die kunnen worden gemonitord op dit moment nog beperkt zijn, maar dat deze mogelijkheden in de toekomst zullen worden uitgebreid om onder andere ook SoD-conflicten te kunnen monitoren. Om de terminologie van dit onderzoek aan te halen, betreft het dan controle 4 zonder workflow. Ook geven Keller en Verma* (2022) aan dat de Data Exploit Prevention functionaliteit een workflowfunctionaliteit zal krijgen, die als volgt werkt: indien een gebruiker inputvariabelen ingeeft die tot een uitzondering zouden leiden, krijgt hij een melding dat deze transactie een uitzondering veroorzaakt. De gebruiker krijgt vervolgens de optie om een workflow op te starten om de autorisatie te verkrijgen om deze transactie toch te kunnen invoeren. Hij kan hierbij ook een bericht sturen om aan te geven waarom hij deze transactie wil aanmaken. Vervolgens wordt er een melding gestuurd naar een controle-eigenaar, die op basis van de inputdata en het bericht kan bepalen om deze transactie al dan niet eenmalig te deblokkeren voor deze gebruiker.

In Tabel 1 is per tool aangegeven welke monitoring-controles hierin geïmplementeerd zijn.

Tabel 1. Eigenschappen van SAP monitoring tools.

	SAP Access Violation Management	SAP Business Integrity Screening	SAP UI Masking
Controle 1: Periodieke rapportages	1	1	
Controle 2: Real time meldingen	2	1	
Controle 3: Real time meldingen, blokkeren en een workflow	3	1	
Controle 4: Melding en blokkeren nog voor er op verzenden is geklikt en een workflow	3	3	4

Legenda:
1. Dit is een standaardonderdeel van deze software.
2. Het is mogelijk om meldingen (vrijwel) realtime te genereren, maar de toepassing is hier niet specifiek voor ontwikkeld.
3. Het is mogelijk om deze functionaliteit toe te voegen middels het schrijven van maatwerk. Deze functionaliteit is geen onderdeel van de standaardsoftware. Naast de aanschafkosten van de tool zijn hier nog extra kosten aan verbonden.
4. Deze functionaliteit is in beperkte vorm opgenomen in de tool, maar zal nog worden uitgebreid.

Hierbij is het belangrijk om op te merken dat deze monitoringcontroles geen onderdeel zijn van SAP-standaardprogrammatuur. Deze tools zijn apart geprogrammeerd en een organisatie die deze wil gebruiken, moet hiervoor een aanvullende licentie kopen. De functionaliteit van het blokkeren van meldingen nog voor er op verzenden is geklikt (controle 4) is vervolgens weer geen standaardonderdeel van de tool en moet hier weer als maatwerk in gebouwd worden. Keller en Verma* (2022) geven aan dat controle 4 naar verwachting wel een standaardfunctionaliteit zal worden van de UI Masking tool, maar dit is op dit moment nog niet volledig beschikbaar. De verschillende tools zijn los van elkaar ontwikkeld en niet standaard met elkaar geïntegreerd. Er zijn geen certificeringen beschikbaar die de gebruiker zekerheid geven over het correct functioneren van de tools. De tools zijn op de applicatielaag van de SAP-standaardapplicatie geprogrammeerd. Meldingen en blokkades worden niet op databaseniveau gegeven.

1.3. Technische uitdagingen

Technisch gezien is de ene monitoringcontrole makkelijker in te richten dan de andere. Hierna is een beschrijving gegeven van de mogelijkheden en beperkingen per controle.

Controle 1: Periodieke rapportages

Periodieke rapportages zijn relatief eenvoudig te produceren uit loggegevens. Dit is over het algemeen niet belastend voor het systeem en deze controle wordt dan ook al sinds jaar en dag gebruikt om meer inzicht te verkrijgen.

Controle 2: Realtime meldingen

Het genereren van realtime meldingen is meer belastend voor het systeem. Dommerholt* (2021) geeft aan dat er veel meer rekenkracht nodig is om continu te monitoren of er ergens in het systeem een uitzondering heeft plaatsgevonden. Hedendaagse computersystemen kunnen dit over het algemeen wel aan, maar Van der Voort* (2021) benadrukt dat dit afhankelijk is van verschillende factoren, zoals de hoeveelheid data in het systeem, de hoeveelheid nieuwe transacties die wordt aangemaakt per tijdseenheid, de hoeveelheid monitoringcontroles, het soort monitoringcontroles en de hoeveelheid beschikbare capaciteit van het systeem. Het genereren van de meldingen op zich is technisch gezien niet erg ingewikkeld. Hiervoor kunnen de beschikbare loggegevens worden gebruikt.

Controle 3: Realtime meldingen, blokkeren en een workflow

Dommerholt* (2021) geeft aan dat het genereren van realtime meldingen en vervolgens het blokkeren van relevante transacties over het algemeen niet veel meer belastend of complex is dan alleen het genereren van realtime meldingen. Wanneer eenmaal is bepaald dat er zich een uitzondering heeft voorgedaan, is het blokkeren van de relevante transactie relatief eenvoudig.

Controle 4: Meldingen, blokkeren nog voor er op verzenden is geklikt en een workflow

Het geven van een melding en het blokkeren nog voor er op verzenden is geklikt, is de meest belastende controle die in dit onderzoek wordt omschreven. Dit moet niet alleen realtime gebeuren, maar er moeten ook meerdere checks worden gedaan om te bepalen óf een transactie geblokkeerd moet worden of niet.

Ook het programmeren van deze controle is complex. De transactie bestaat namelijk nog niet op het moment dat er al moet worden bepaald of deze moet worden geblokkeerd. Volgens Van der Voort* (2021) is SAP hier niet standaard op ingericht. Hierdoor is het programmeren van deze controle een stuk ingewikkelder dan het programmeren van een controle waarbij de criteria voor het al dan niet blokkeren zijn vastgelegd in een transactie die al in het systeem vastligt.

Wat het programmeren van deze controle extra ingewikkeld maakt, is de workflow die hierin is opgenomen. Om dit mogelijk te maken, moeten de gegevens die de gebruiker invoert in een aparte tabel worden opgeslagen, zodat deze vervolgens aan de controle-eigenaar getoond kunnen worden. Indien de controle-eigenaar de transactie goedkeurt, moeten deze gegevens vervolgens alsnog in een transactie worden opgenomen waarmee verder kan worden gewerkt. Keller en Verma* (2022) geven aan dat dit op dit moment technisch mogelijk is, maar het staat allemaal nog erg in de kinderschoenen. Daarom kan er ook voor worden gekozen om controle 4 zonder de workflow te implementeren. Dit leidt echter tot aanvullende risico's waarmee rekening moet worden gehouden (zie ook paragraaf 3.2).

2. Methodologie

Aan de hand van het uitgevoerde onderzoek is de volgende hoofdvraag beantwoord:

> *Wat zijn de voordelen en risico's van het gebruik van verschillende vormen van monitoring SoD-controles in SAP en welke controles kunnen het best worden gebruikt in welke situatie?*

Deze hoofdvraag is opgesplitst in de volgende twee deelvragen:

Deelvraag 1

Wat zijn de voordelen en risico's van het vervangen van autorisaties door monitoring SoD-controles?

Om deze vraag te beantwoorden, is er onderzoek gedaan naar de eigenschappen van de verschillende vormen van monitoring SoD-controles en de risico's van het

(gedeeltelijk) vervangen van preventieve SoD controles door monitoring SoD-controles. Hiertoe is in de literatuur gekeken naar wat hierover al is geschreven. Daarnaast is er een interview gehouden met Product Architecten van de onderzochte SAP tools.

Deelvraag 2

Welke soort monitoring SoD-controles kunnen het beste worden gebruikt in welke situatie?

Om deze vraag te beantwoorden, is literatuuronderzoek gedaan naar monitoringcontroles en access control. Vervolgens is een interview gehouden met Product Architecten van de onderzochte SAP tools. Ook is er een interview gehouden met een SAP-autorisatieconsultant, een Technology Advisor en een ervaren RE en RA om te bepalen hoe zij kijken naar het gebruik van monitoring.

3. Onderzoeksresultaten

Ten eerste moet worden bepaald of het mogelijk is om autorisaties gedeeltelijk door monitoringcontroles te vervangen. Indien dit mogelijk is, biedt dit verschillende voordelen en risico's voor de organisatie. Deze worden hierna beschreven. Ook wordt beschreven hoe het beste een keuze kan worden gemaakt uit de verschillende monitoringcontroles.

3.1. Kan een controle worden vervangen door een monitoringcontrole?

Controle 1: Periodieke rapportages

Periodieke rapportages zijn in het algemeen een detectieve controle. De uitzonderingen hebben al plaatsgevonden, dus het is vaak niet meer mogelijk om deze nog (volledig) te herstellen. Deze controle moet dus niet worden gebruikt om autorisaties te vervangen, maar juist om de inrichting van autorisaties te verbeteren. Het voordeel van het implementeren van deze controle is dat SoD-conflicten eerder zullen worden opgespoord en kunnen worden verholpen.

Controle 2: Realtime meldingen

Ook realtime meldingen zijn een detectieve controle. Zowel Van Leeuwen and Bergsma (2014) als Van Der Voort* (2021) geven aan dat ook deze controle daarom niet kan worden gebruikt om autorisaties (volledig) te vervangen. Deze controle is een vorm van continuous monitoring. Zowel Proctor et al. (2007) als Turner and Owhoso (2009) geven aan dat continuous monitoring het beste kan worden gebruikt om SoD-uitzonderingen in de verstrekte autorisaties op te sporen en vervolgens aan te passen. Het inperken van autorisaties is bij gebruik van deze controle dus niet aan de orde.

Controle 3: Realtime meldingen, blokkeren en een workflow

Wanneer uitzonderingen in realtime worden gemeld en de bijhorende transacties worden geblokkeerd, hangt het van de situatie af of deze controle kan worden gebruikt om autorisaties te vervangen of niet. Het ligt eraan wanneer in het proces deze controle plaatsvindt en of potentiële fouten op dat moment nog kunnen worden hersteld of niet. Indien er een uitzondering wordt geconstateerd in een actie die tijdens het proces plaatsvindt, is het vaak nog mogelijk om het proces stil te leggen door de juiste transactie te blokkeren. In sommige gevallen is dit de transactie zelf en in sommige gevallen gaat het om een andere transactie, verderop in het proces. Wanneer de uitzondering echter plaatsvindt aan het einde van het proces, bijvoorbeeld bij het uitvoeren van een betaalrun, kan deze niet meer worden geblokkeerd, omdat het geld de organisatie al heeft verlaten. Wanneer ervoor wordt gekozen om gebruik te maken van deze controle, moet rekening worden gehouden met de risico's als beschreven in sectie 3.2.

Controle 4: Melding, blokkeren nog voor er op verzenden is geklikt en een workflow

Wanneer uitzonderingen al worden gedetecteerd nog voordat er op verzenden is geklikt, is dit een preventieve controle. Het is daarom mogelijk om autorisaties te vervangen door deze controle. Hierbij moet rekening worden gehouden met de in sectie 3.2 aangegeven risico's.

3.2. Voordelen en risico's van het vervangen van autorisaties door monitoringcontroles

Het inrichten en onderhouden van het autorisatieconcept kost veel organisaties erg veel middelen. De cost of control is daarom erg hoog. Van der Voort* (2021) geeft aan dat wanneer een organisatie ervoor kiest om het autorisatieconcept in te perken en gebruik te gaan maken van monitoringcontroles, dit kan leiden tot een lagere cost of control, terwijl het restrisico hetzelfde blijft.

Naast de voordelen van een eenvoudiger autorisatieconcept, kan het implementeren van monitoringcontroles ook nog andere voordelen opleveren, zoals meer controle doordat de organisatie actief op de hoogte wordt gesteld van uitzonderingen die zich voordoen, de mogelijkheid om datagebonden autorisaties te verstrekken en een afname van het aantal overtredingen, omdat medewerkers zich ervan bewust zijn dat ze worden gemonitord.

Risico's

Naast deze voordelen moet er rekening worden gehouden met de volgende risico's:

- Overbelasting van het systeem: Van der Voort* (2021) geeft aan dat indien er te veel complexe monitoringcontroles worden ingericht, het risico bestaat dat dit te belastend is voor het systeem. Het systeem

kan hierdoor gaan vastlopen, waardoor de gebruiker bijvoorbeeld elke keer wanneer een transactie wordt ingevoerd een paar seconden moet wachten, voordat het systeem heeft bepaald of de transactie een melding veroorzaakt of niet.
- Incorrecte configuratie: ook de monitoringcontrole moet worden ingericht. Radkowski* (2021) geeft aan dat dit – afhankelijk van de controle – erg complex kan zijn. Ook moet worden getest of de ingerichte controles wel alles blokkeren dat zij horen te blokkeren. Keller en Verma* (2022) geven aan dat alle mogelijke paden om een transactie aan te maken moeten worden doorlopen, om te bepalen of deze allemaal op een juiste wijze worden geblokkeerd. Dit kan behoorlijk tijdrovend zijn en moet ook goed gebeuren, anders is de controle niet waterdicht. De complexiteit hiervan is afhankelijk van de tool die wordt gebruikt en de controle die wordt ingericht. Van Der Voort* (2021) en Hallemeesch c.s.* (2021) geven aan dat vervolgens ook de inrichting van de controle moet worden onderhouden. Dit wordt complexer naarmate er meer monitoringcontroles worden ingericht.
- Onvolledige monitoring of monitoring van onvoldoende kwaliteit: hoe meer meldingen een tool genereert, des te groter de kans dat een beheerder een melding over het hoofd ziet. Zowel Stapleton* (2021), Hafner* (2021) als Hallemeesch c.s.* (2021) geven aan dat het daarom belangrijk is om de tool zo in te richten dat false-positives zoveel mogelijk worden voorkomen. Dit is echter wel een balanceeract; het is namelijk niet de bedoeling dat de tool legitieme meldingen niet meldt, omdat deze worden gezien als een false-positive. Hier moet goed naar worden gekeken bij de inrichting. Het is daarom belangrijk voldoende tijd te steken in het volledig en compleet implementeren van de tool. Dommerholt* (2021) geeft aan dat er ook tijd voor vrij moet worden gemaakt om rapportages te beoordelen en/of meldingen te monitoren.
- Gebruikers met toegang tot de debug-functionaliteit: Hallemeesch c.s.* (2021) geven aan dat gebruikers met toegang tot de debug-functionaliteit mogelijk om de monitoringcontroles heen kunnen werken. Toegang tot de debug-functionaliteit moet daarom zo veel mogelijk worden beperkt. Keller en Verma* (2022) geven aan dat het ook verstandig kan zijn om het gebruik van de debug-functionaliteit zelf te monitoren.

Aanvullende risico's

In het geval dat er transacties geblokkeerd zullen worden (dus wanneer gebruik wordt gemaakt van de controles 3 of 4), moet er rekening worden gehouden met de volgende aanvullende risico's:

- Het stagneren van de business door te veel blokkades: zowel Radkowski* (2021) als Hallemeesch c.s.* (2021) geven aan dat indien transacties automatisch kunnen worden geblokkeerd, het risico bestaat dat legitieme transacties worden geblokkeerd. Indien deze niet tijdig worden gedeblokkeerd, stagneert de business. Daarom is het belangrijk om meldingen continu te monitoren. Hallemeesch c.s.* (2021) en Dommerholt* (2021) merken op dat indien er gebruik wordt gemaakt van controle 4 zonder de workflow, dit risico nog groter is, aangezien bepaalde transacties dan helemaal niet kunnen worden aangemaakt. Indien deze controle niet juist is geïmplementeerd, kan de hele business hierdoor stagneren.
- Het blokkeren van de verkeerde transactie: Van der Voort* (2021) benadrukt dat indien er gebruik wordt gemaakt van controle 3, er moet worden bepaald wat er moet worden geblokkeerd in geval van een uitzondering. Bijvoorbeeld: als er een uitzondering wordt geconstateerd in een inkoopfactuur, zou niet de factuur geblokkeerd moeten worden, maar de bijhorende betaling. Dit kan tot een extra risico leiden wanneer niet de juiste transactie wordt geblokkeerd.
- Onvoldoende kennis bij medewerkers die mogen deblokkeren: volgens Van der Voort* (2021) moeten de gebruikers die het recht krijgen om te deblokkeren, voldoende kennis hebben om te bepalen waarom een transactie is geblokkeerd en of er actie moet worden ondernomen voordat deze kan worden gedeblokkeerd. Ook geeft Lagendijk* (2021) aan dat de medewerker die mag deblokkeren een hogere hiërarchische positie moet hebben dan de medewerkers die de transacties hebben aangemaakt. Van Der Voort* (2021) stelt dat dit risico groter wordt wanneer er gebruik wordt gemaakt van controle 3, en ervoor is gekozen om niet de transactie zelf te blokkeren, maar een andere transactie verderop in het proces. In dit geval kan een transactie geblokkeerd zijn wegens een uitzondering in een andere transactie. Voor een controle-eigenaar wordt het daarom nog complexer om te bepalen of een transactie weer gedeblokkeerd kan worden.
- Frustratie bij medewerkers: zowel Lagendijk* (2021) als Hallemeesch c.s.* (2021) geven aan dat indien medewerkers zich er niet van bewust zijn dat er gebruik wordt gemaakt van een tool waarbij transacties automatisch worden geblokkeerd, het risico bestaat dat dit leidt tot verwarring en irritatie. Daarom is het belangrijk dat medewerkers geïnformeerd zijn over het feit dat er gebruik wordt gemaakt van een dergelijke tool. Goede communicatie is hierbij noodzakelijk. Voorkomen moet worden dat medewerkers de indruk krijgen dat het systeem hen blokkeert, waardoor ze gaan proberen 'om het systeem heen te werken', bijvoorbeeld door meer handmatige boekingen te gaan maken, of door een geblokkeerde transactie nog eens aan te maken, maar dan net iets anders vast te leggen, in de hoop dat deze niet geblokkeerd wordt. Het zou bijvoorbeeld kunnen helpen om het blokkeren van een transactie richting de medewerker niet te communiceren als een blokkade, maar als een workflow waarin een tweede

persoon meekijkt met transacties die potentiële uitzonderingen kunnen vormen.
- De mogelijkheid dat het systeem te erg geblokkeerd is in geval van een calamiteit: Van der Voort* (2021) neemt hierbij het standpunt in dat het in geval van een calamiteit altijd mogelijk moet blijven om geblokkeerde transacties snel weer te deblokkeren. Daarom is het belangrijk om een firefighterprocedure in te richten. In deze procedure moet worden beschreven hoe, in geval van nood, geautoriseerde gebruikers tijdelijk toegang krijgen tot een noodaccount met hoge, maar gereguleerde rechten. Hierdoor kunnen zij het incident oplossen, zonder dat zij hierbij worden tegengehouden door eventueel geblokkeerde transacties.

Om de bovenstaande risico's te mitigeren, kunnen verschillende maatregelen worden genomen, zoals voldoende aandacht schenken aan de implementatie en het onderhoud van de monitoringcontroles, een degelijk proces voor het opvolgen van uitzonderingen, gebruikmaken van logging, goede communicatie richting medewerkers en het inrichten van een firefighterprocedure.

3.3. Keuze voor een monitoringcontrole

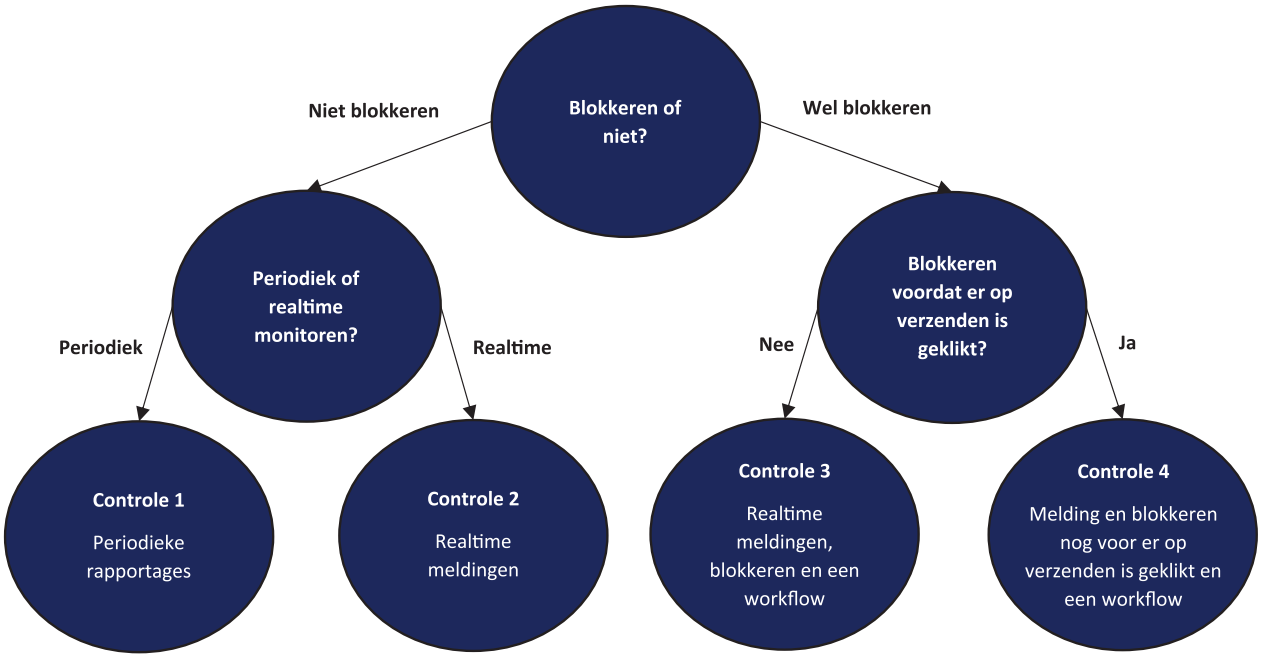
Bij het maken van de keuze voor de in te zetten monitoringcontroles die een organisatie wil gaan gebruiken, moet het uitgangpunt altijd een risk assessment zijn. Per geïdentificeerd risico moet worden bepaald welke monitoringcontrole het beste gebruikt kan worden. Om te bepalen welke monitoringcontrole het meest geschikt is, kan gebruik worden gemaakt van de beslisboom in Figuur 1. In deze boom worden drie keuzes weergegeven. Per keuze is beschreven hoe deze het beste kan worden gemaakt.

3.3.1. Blokkeren of niet?

Bij het maken van een keuze uit een van de vier monitoringcontroles, zal als eerste moeten worden beslist of transacties geblokkeerd gaan worden of niet. Hiertoe moet rekening worden gehouden met drie criteria:

1. Waar in het proces doet het risico zich voor? Indien een bepaalde risicovolle gebeurtenis zich voordoet, kan deze dan nog later in het proces worden gecorrigeerd? Als de gebeurtenis zich voordoet tijdens het proces is het mogelijk niet zo erg als hierin een fout wordt gemaakt, zolang deze later maar gecorrigeerd wordt. Wanneer de gebeurtenis zich tijdens het proces voordoet en later nog gecorrigeerd kan worden, ligt het voor de hand om te kiezen voor niet blokkeren. Het voordeel hiervan is dat er geen rekening hoeft te worden gehouden met de risico's van het blokkeren van transacties (zie paragraaf 3.2). Als de gebeurtenis zich aan het einde van het proces voordoet en niet meer gecorrigeerd kan worden, ligt het echter meer voor de hand om hierbij wel gebruik te maken van blokkeren. Dit is zeker aan de orde wanneer er gebruik wordt gemaakt van een ingeperkt autorisatieconcept.
2. De impact van het risico: als de impact klein is, is het wellicht niet nodig om de transactie te blokkeren, zelfs niet als deze zich aan het einde van het proces voordoet. Indien de impact groot is, is het echter verstandiger om wel gebruik te maken van het blokkeren van transacties.
3. De kans dat een uitzondering zich voordoet: als de kans klein is dat een uitzondering zich voordoet, is het misschien niet nodig om hiervoor een monitoringcontrole met blokkade in te richten. Dit hangt echter ook samen met de impact. Voor een risico met een kleine

Figuur 1. Beslisboom bepaling monitoringcontrole.



kans maar met een potentieel hoge impact, is het wellicht wel verstandig om meer maatregelen te nemen.

Zowel Radkowski* (2021), Stapleton* (2021), Hafner* (2021), Van der Voort* (2021) als Hallemeesch c.s.* (2021) geven aan dat een organisatie in het algemeen moet beseffen dat hoe meer zij blokkeert, des te groter de kans wordt dat bedrijfsprocessen worden stilgelegd. Daarom is het belangrijk niet te veel te blokkeren, en vooral te focussen op gevallen waar dit echt nodig is.

3.3.2. Periodiek of realtime monitoren?

Indien er is gekozen voor niet blokkeren, moet vervolgens worden bepaald of er gebruik zal worden gemaakt van periodieke rapportages of realtime meldingen. Het verschil tussen periodieke rapportages en realtime meldingen zit in de timing waarmee meldingen worden gegeven. De vraag is dus hoe snel de organisatie op de hoogte gesteld wil worden van een mogelijke uitzondering? Hafner* (2021) geeft aan dat wanneer de gebeurtenis tijdens het proces plaatsvindt, het belangrijk is om de melding te geven voordat het proces helemaal is afgerond, zodat er nog correcties kunnen worden doorgevoerd indien nodig.

Indien de impact van het risico laag is en de monitoring meer bedoeld is als informatie dat er iets is gebeurd, en niet om het te corrigeren, dan hoeft er minder vaak te worden gemonitord. Stapleton* (2021) geeft aan dat het in dit geval beter kan zijn om meldingen niet te vaak te genereren. Indien controle-eigenaren worden overspoeld met meldingen, kan de informatie betekenisloos worden en daardoor niet meer goed worden gemonitord.

3.3.3. Blokkeren voordat er op verzenden is geklikt?

Indien er is gekozen voor blokkeren, moet er vervolgens worden bepaald of er gebruik zal worden gemaakt van controle 3 of controle 4. Het verschil tussen deze controles zit in de timing van het blokkeren, en in wat er geblokkeerd wordt. Van der Voort* (2021) geeft aan dat in het geval van controle 3 het blokkeren van de transactie zelf soms al geen zin meer heeft, en dat er zal moeten worden bepaald wat er dan wel geblokkeerd moet worden. Lagendijk* (2021) geeft aan dat dit in de praktijk daarom lastig uitvoerbaar kan zijn. Ook zal er rekening moeten worden gehouden met verschillende aanvullende risico's in dit geval (zie ook paragraaf 3.2). Indien de organisatie zich in de situatie bevindt waarin het blokkeren van de transactie zelf eigenlijk al te laat is, kan er beter worden gekozen voor controle 4. Als het risico wel kan worden weggenomen door de transactie zelf te blokkeren, kan er wel worden gekozen voor controle 3.

Hierbij moet worden opgemerkt dat het programmeren van controle 4 een stuk ingewikkelder is dan het programmeren van controle 3. Het implementeren van controle 4 is hierdoor mogelijk niet haalbaar, waardoor er toch voor controle 3 zal moeten worden gekozen. Het risk assessment zal moeten uitwijzen of dit ook een verstandige keuze is.

Als laatste moet worden opgemerkt dat in sommige gevallen controle 4 alleen beschikbaar zal zijn zonder de workflow. Dommerholt* (2021) geeft aan dat deze controle alleen moet worden gebruikt in het geval dat een gebeurtenis echt nooit voor mag komen en de impact groot zou zijn als deze gebeurtenis zich wel zou voordoen. Dit is belangrijk, omdat het met controle 4 zonder workflow echt onmogelijk wordt gemaakt om bepaalde acties uit te voeren.

4. Conclusie

Het inrichten van een effectief autorisatieconcept in SAP kan erg complex en kostbaar zijn. Daarom is in dit onderzoek gekeken naar mogelijke alternatieven in de vorm van monitoring. Door het inrichten van de juiste monitoringcontroles kan er gebruik worden gemaakt van een eenvoudiger autorisatieconcept, waardoor de totale cost of control lager uit kan komen, bij een gelijkblijvend netrisico. Hierbij moet een organisatie op zoek gaan naar de juiste controlemix van eenvoudige autorisaties en geschikte monitoringcontroles om de risico's te beheersen.

Op dit moment is er nog geen tool beschikbaar waarin alle relevante vormen van monitoring zijn opgenomen. Daardoor is het implementeren van een dergelijke controlemix vaak nog ingewikkeld. Ook is er op dit moment nog geen tool die controle 4 (Melding en blokkeren nog voor er op verzenden is geklikt en een workflow) standaard aanbiedt. Dit zal als maatwerk in een andere tool moeten worden geschreven. Het inrichten van monitoring controles is daardoor in de praktijk nog complex. Op dit moment zou het overgaan naar een eenvoudiger autorisatieconcept met aanvullende monitoringcontroles wellicht nog niet tot een lagere cost of control leiden. Om dit echt rendabel te krijgen, zal er eerst een goed werkende tool moeten worden ontwikkeld die alle vormen van monitoring combineert. Dit neemt niet weg dat organisaties er nu al rekening mee kunnen houden dat deze vorm van interne controle in de toekomst een reële optie zal gaan worden. Met de groeiende complexiteit van informatiesystemen als SAP, nieuwe regelgeving en eisen zou dit omslagpunt weleens snel kunnen worden bereikt. SAP werkt zelf aan een tool die functionaliteiten voor controle 4 steeds beter zal gaan aanbieden, waardoor dit een reëlere optie voor de toekomst lijkt te worden.

Om antwoord te krijgen op de vraag of het gebruik van monitoringcontroles en een eenvoudiger autorisatieconcept echt tot een lagere cost of control leidt, zal nader onderzoek moeten worden gedaan, inclusief een kostenanalyse.

■ **L. Broere-Koetsier MSc RE – Lieke-Rosa** is junior manager IT audit en data analyse bij Grant Thornton.

Noten

1. In dit artikel is alleen maar gekeken naar SAP ECC en SAP S4. Om inzicht te krijgen in de mogelijkheden in andere ERP-pakketten is meer onderzoek nodig.
2. Aan de hand van dit onderzoek heeft SAP een nieuwe functionaliteit aan de SAP UI Masking tool toegevoegd, waarmee transacties kunnen worden geblokkeerd nog voordat deze zijn aangemaakt. De hierbij verkregen inzichten zijn meegenomen in het onderzoek dat centraal staat in dit artikel.

Literatuur

- Fluitsma J (2018) [13 januari] GRC wordt steeds belangrijker. Opgehaald van VNSG. https://vnsg.nl/iMIS/VNSGWeb/News/EXPERTTALK/GRC_wordt_steeds_belangrijker.aspx
- Frenehard T (2021) [4 mei] GRC Tuesdays: What really is SAP Governance, Risk, and Compliance (GRC)? Focus on the Identity and Access Governance pillar. Opgehaald van Blog.SAP. https://blogs.sap.com/2021/05/04/grc-tuesdays-what-really-is-sap-governance-risk-and-compliance-grc-focus-on-the-identity-and-access-governance-pillar/
- Martens S (2019) [26 juli] SAP blijft meest gebruikte ERP-leverancier. Opgehaald van Computable. https://www.computable.nl/artikel/nieuws/erp/6771046/250449/sap-blijft-meest-gebruikte-erp-leverancier.html
- Proctor PE, Heiser J, MacDonald N (2007) [9 februari] MarketScope for Segregation of Duties Controls Within ERP. Gardner.
- Roest GA, De Rooij M (2008) [maart] Afweging tussen businessflexibiliteit en control via functiescheiding. Compact.
- SAP (2017) [22 augustus] GRC Tuesdays: SAP Business Integrity Screening Is the New SAP Fraud Management Solution. Opgehaald van Blogs.SAP. https://blogs.sap.com/2017/08/22/grc-tuesdays-sap-business-integrity-screening-is-the-new-sap-fraud-management-solution/
- SAP (2020) [27 november] Feature Scope Description for UI Data Protection Masking for SAP S/4HANA. [Opgehaald van] https://help.sap.com
- SAP (2021) What is Authorization? Opgehaald van SAP Online Tutorials. https://www.saponlinetutorials.com/authorization-sap/
- Turner LD, Owhoso V (2009) Use ERP internal control exception reports to monitor and improve controls. Management Accounting Quarterly.
- Van der Zon AM, Spruit I, Schutte JG (2013) [maart] Access control applicaties voor SAP. Opgehaald van Compact. https://www.compact.nl/articles/access-control-applicaties-voor-sap/
- Van Leeuwen O, Bergsma J (2014) Algemene grondslagen Starreveld. Noordhof Uitgevers.
- Vreeke A, Hallemeesch D (2006) [februari] ‘Zoveel functiescheidingsconflicten in SAP – dat kan nooit’, en waarom is dat eigenlijk een risico? Opgehaald van Compact. https://www.compact.nl/articles/zoveel-functiescheidingsconflicten-in-sap-dat-kan-nooit-en-waarom-is-dat-eigenlijk-een-risico/