

Index

| | |
|--|----|
| Dankwoord | 3 |
| Index..... | 4 |
| Lijst van figuren en tabellen | 6 |
| Afkortingen | 7 |
| Inleiding | 8 |
| Hoofdstuk 1. Een autorisatie-raamwerk | 10 |
| 1.1. Het belang van het beheer van autorisaties en autorisatie-concept | 10 |
| 1.2. Externe invloeden en regelgeving..... | 10 |
| 1.2.1. Voorbeeld: Sarbanes-Oxley introductie (Sox / J-Sox) | 11 |
| 1.2.2. Cobit-raamwerk..... | 13 |
| Hoofdstuk 2. Autorisaties in een SAP R/3-omgeving | 15 |
| 2.1. SAP R/3 ERP, beveiliging en audit | 15 |
| 2.2. Het autorisatie-model van SAP in een notedop..... | 16 |
| 2.3. SAP security terminologie | 17 |
| 2.3.1. Authenticatie en identificatie | 17 |
| 2.3.2. Autorisaties en autorisatie-componenten: een meer technische zijsprong | 17 |
| Hoofdstuk 3. GRC in autorisaties: scheiding van functies | 29 |
| 3.1. Scheiding van functies: bouwsteen van interne controle | 29 |
| 3.2. 'Scheiding van functies'-matrix als een richtlijn..... | 31 |
| 3.3. GRC-software: compliance in access control..... | 33 |
| 3.4. Remediëren: opschonen van bestaande SoD-conflicten | 38 |
| 3.5. Mitigeren of compenseren: opschonen via compenserende controles . | 39 |
| 3.6. Beheer van autorisatie-aanvragen (workflow) | 41 |
| Hoofdstuk 4. Een praktische en logische aanpak voor het invoeren en beheer van scheiding van functies in een SAP-omgeving | 42 |
| 4.1. Bedrijfsbeleid rond autorisaties | 42 |
| 4.2. Business-definities rond het autorisatie-concept..... | 45 |
| 4.3. SAP-autorisatie-concept vanuit een business-oogpunt | 46 |
| 4.4. Eigenaarschap over de toe te kennen rollen..... | 48 |

| | | |
|--------|---|----|
| 4.4.1. | Task ownership | 48 |
| 4.4.2. | Activity ownership | 49 |
| 4.5. | De rol van de Authorization Officer | 50 |
| 4.6. | De rol van de Authorization Administrator | 51 |
| 4.7. | Cleanup van de bestaande (ontspoorde) situatie: review concept..... | 52 |
| 4.8. | Continu monitoring: Invoeren van een proces voor nieuwe aanvragen | 56 |
| 4.8.1. | Standaard autorisatie-aanvragen | 57 |
| 4.8.2. | Change requests | 61 |
| 4.8.3. | Nieuwe gebruiker aanvraag – ‘kopieer van ...’ | 61 |
| 4.8.4. | Aanvraag voor een generieke of speciale gebruikers..... | 62 |
| 4.8.5. | Indienen en controleren van de aanvraag en workflow | 62 |
| 4.8.6. | Uitvoeren van de aanvraag | 64 |
| 4.9. | Rapportering: periodieke review van autorisaties door owners | 64 |
| | Conclusie | 66 |
| | Referenties | 68 |
| | Bijlage 1 : Workflow standaard autorisatie-aanvraag..... | 69 |
| | Bijlage 2 : Workflow change request..... | 70 |

Lijst van figuren en tabellen

| | | |
|---------------|--|----|
| Figuur I. | Coso-raamwerk en J-Sox-kubus..... | 12 |
| Figuur II. | Voorbeeld van autorisatie-objecten voor transactie MM01 | 19 |
| Figuur III. | Structuur van een rol | 21 |
| Figuur IV. | Structuur van een autorisatie-object | 22 |
| Figuur V. | Voorbeeld van een autorisatie-object en autorisatie-veldwaarden in transactie MM01 | 22 |
| Figuur VI. | Structuur van een autorisatie | 23 |
| Figuur VII. | Structuur van een autorisatie-profiel | 23 |
| Figuur VIII. | Derived roles | 26 |
| Figuur IX. | Autorisatie-raamwerk samengevat | 27 |
| Figuur X. | SAP-SoD-matrix | 32 |
| Figuur XI. | SAP financial impact matrix | 33 |
| Figuur XII. | Vergelijking autorisatie tools op de markt..... | 38 |
| Figuur XIII. | Link gebruikers-activiteiten-taken-transacties : voorbeeld 1 | 47 |
| Figuur XIV. | Link gebruikers-activiteiten-taken-transacties : voorbeeld 2..... | 48 |
| Figuur XV. | De goedgekeurde autorisatie-risico-appetijt..... | 53 |
| Figuur XVI. | Aanvraag workflow voor autorisaties | 56 |
| Figuur XVII. | Sap autorisatie formulier 1..... | 58 |
| Figuur XVIII. | Sap autorisatie formulier 2..... | 59 |
| Figuur XIX. | Sap autorisatie formulier 3 | 59 |
| Figuur XX. | Sap autorisatie formulier 4 | 60 |
| Figuur XXI. | Sap autorisatie formulier 5 | 60 |
| Figuur XXII. | Sap autorisatie goedkeuringen | 63 |