



FOCUS
ONLINE

8 T/M 12 NOVEMBER 2021

Welkom

Mitigieren van risico's toegangsbeveiliging

Meta Hoetjes, SAP Security expert - CSI Tools





Mitigieren van risico's toegangsbeveiliging

Customer story:
De gehanteerde aanpak voor het opschonen (en schoon houden) van de toegangsbeveiligingsrisico's.

Meta Hoetjes

meta.hoetjes@csi-tools.com

Agenda

- Begin situatie
- Aanpak
- Knelpunten en oplossingen
- Quick wins
- Alternatieve aanpak

Begin situatie

- Al live met SAP ECC
- In de planning: migratie naar S4/HANA
- Opmerkingen en aanmerkingen
Jaarrekeningcontrole
- Geen eigen risico analyse / ruleset
- Autorisatiebeheer extern
- ServiceNow als ticketing systeem

Get
clean

Stay
clean



Aanpak

1. Inzicht krijgen in de huidige risico's
2. Risico's omzetten in een regelset
3. Detectieve analyse
4. Opschoning

5. Preventieve maatregelen



1. Inzicht in de huidige risico's

Knelpunten

- Geen inzicht aanwezig
- Geen input van hoger management

2. Risico's omzetten in een regelset Knelpunten & oplossingen

- Geen inzicht aanwezig
 - Geen input van hoger management
-
- Oplossing : best practice regelset als startpunt
 - Focus op functiescheidingsconflicten

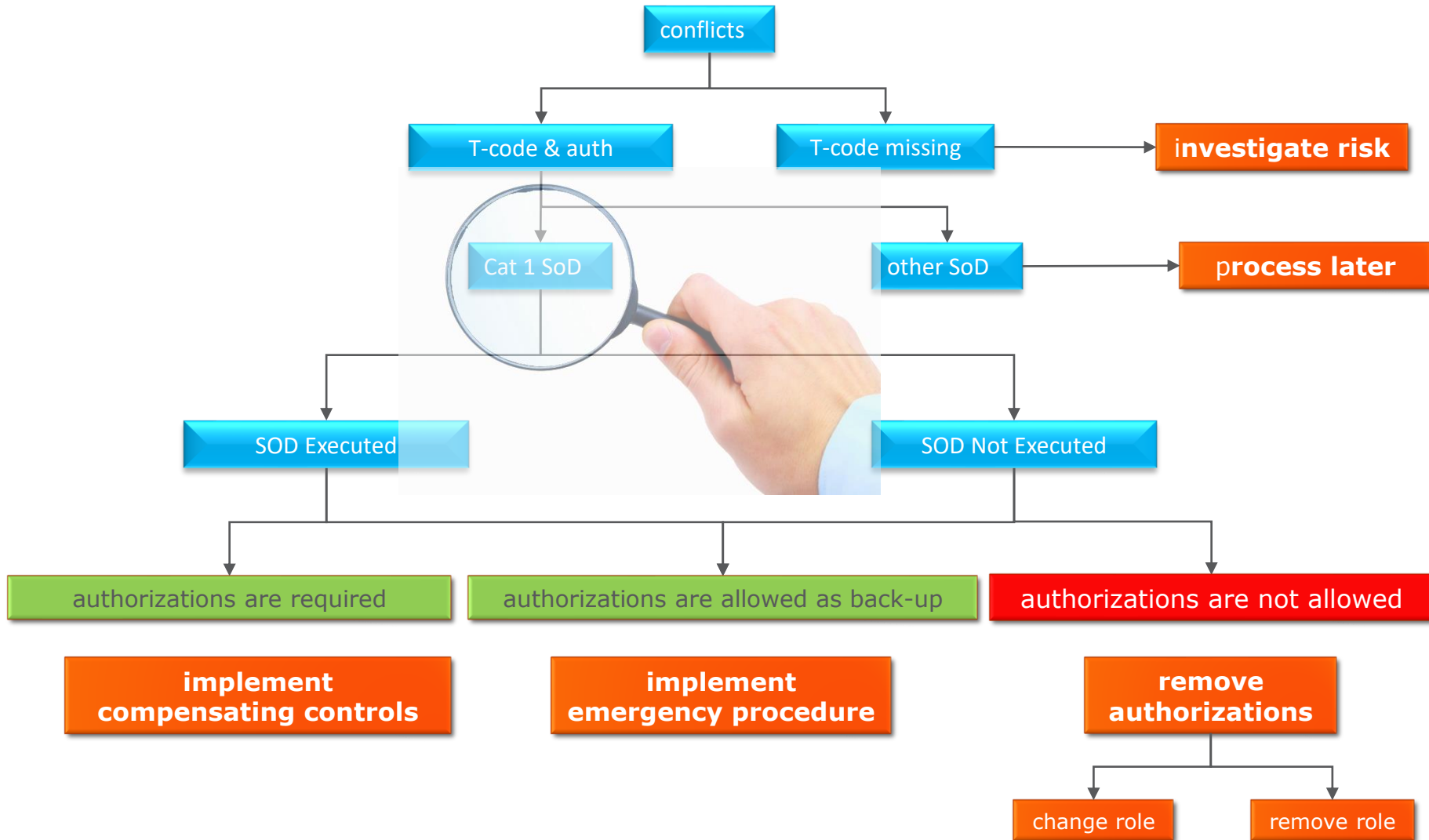
3. Detectieve analyse

Get clean



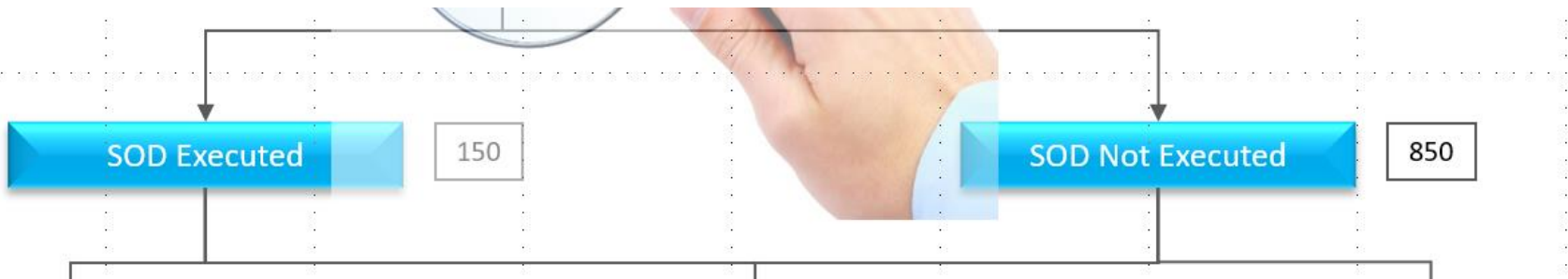
3. Detectieve analyse

Get clean remediation decision tree



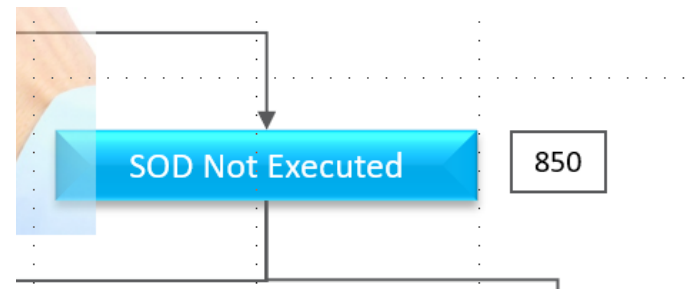
3. Detectieve analyse Regelset

- Eerste analyse met alle SOD conflicten werd gedaan:



1. SoD conflicts Not executed
2. SOD conflicts Executed

3. Detectieve analyse SOD Not Executed (1)



Geen enkele functionaliteit van het SOD conflict is uitgevoerd, door niemand van de organisatie

- Functionaliteit(en) wordt niet gebruikt binnen de organisatie.
- SOD criticiteit: **LOW** (conflict moet worden opgelost, maar lage prioriteit).

RC SoD results

https://c

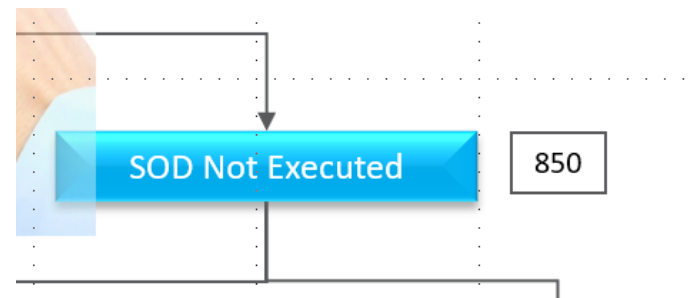
CSI Web Requests Concept Ruleset Info Corner Result Container Cockpit META

RC SoD results

Enter text to search

Logical sy...	Variant	SoD rule	Description	E	Reason code	User id	Username	User group	Type	Status	Norm	Reason c...
>	<NA>	170 SD BACKORDER PROCESSING AND A/R POSTINGS WITH CLEARING	User is able to perform activities in sales flows and pure financial flows	<input type="checkbox"/>	Laag				Dialog user	Locked user		
>	<NA>	171 SD BACKORDER PROCESSING AND A/R INCOMING PAYMENT POSTIN...	User is able to perform activities in sales flows and pure financial flows	<input type="checkbox"/>	Laag				Dialog user	Locked user		
>	<NA>	174 BILLING PROCESS AND A/R PAYMENT ADVISE	User is able to enter billing documents and post fictitious or wrong payment advices	<input type="checkbox"/>	Laag				Dialog user	Locked user		
>	<NA>	177 BILLING PROCESS AND A/R INCOMING PAYMENT POSTINGS	User is able to create fraudulent credit memo and make unwanted payments	<input type="checkbox"/>	Laag				Dialog user	Active user		

3. Detectieve analyse SOD Not Executed (2)



- Gedeeltelijk uitgevoerd – de functionaliteit(en) wordt wel gebruikt binnen de organisaties, maar wordt niet door dezelfde persoon gecombineerd gebruikt.
- SOD criticiteit: **CRITICAL** (conflict moet worden opgelost met hoogste prioriteit).

RC SoD results

Logical sy...	Variant	SoD rule	Description	E	Reason code	User id	Username	User group	Type	Status	Norm	Reason c...
>	<NA>	130 ASSET M.D. AND DEPRECIATION RUN	User is able to create a fictitious asset and execute a depreciation run on the fictitious asset	<input checked="" type="checkbox"/>	Kritisch				Dialog user	Active user		
>	<NA>	130 ASSET M.D. AND DEPRECIATION RUN	User is able to create a fictitious asset and execute a depreciation run on the fictitious asset	<input type="checkbox"/>	Kritisch				Dialog user	Active user		
>	<NA>	130 ASSET M.D. AND DEPRECIATION RUN	User is able to create a fictitious asset and execute a depreciation run on the fictitious asset	<input type="checkbox"/>	Kritisch				Dialog user	Locked user		
>	<NA>	131 ASSET M.D. AND ASSET MANUAL POSTINGS	User is able to create a fictitious asset and process an invoice on the fictitious asset	<input type="checkbox"/>	Kritisch				Dialog user	Active user		
>	<NA>	131 ASSET M.D. AND ASSET MANUAL POSTINGS	User is able to create a fictitious asset and process an invoice on the fictitious asset	<input type="checkbox"/>	Kritisch				Dialog user	Active user		
>	<NA>	131 ASSET M.D. AND ASSET MANUAL POSTINGS	User is able to create a fictitious asset and process an invoice on the fictitious asset	<input checked="" type="checkbox"/>	Kritisch				Dialog user	Active user		
>	<NA>	131 ASSET M.D. AND ASSET MANUAL POSTINGS	User is able to create a fictitious asset and process an invoice on the fictitious asset	<input checked="" type="checkbox"/>	Kritisch				Dialog user	Active user		

3. Detectieve analyse SOD Executed



2. SOD conflicten die door personen zijn uitgevoerd:

- SOD criticiteit: **HIGH**

RC SoD results

Logical sy...	Variant	SoD rule	Description	E	Reason code	User id	Username	User group	Type	Status	Norm	Reason c...	Lock status
<NA>		152 A/P MANUAL POSTINGS AND A/P OUTGOING PAYMENT POSTINGS	User is able to release a fraudulent payment for a document the user has posted or changed	<input type="checkbox"/>	Hoog				Dialog user	Active user	N	NC	Not locked
<NA>		153 A/P OUTGOING PAYMENT POSTINGS AND GRIR CLEARING ACCOUNT	User is able to subsequently create and change GIL recurring document and create and cha...	<input type="checkbox"/>	Hoog				Dialog user	Active user	N	NC	Not locked
<NA>		207 GOODS ISSUES AND ENTER INVENTORY COUNT WITH DOCUMENT	User is able to post incorrect goods issues and create inventory counts	<input type="checkbox"/>	Hoog				Dialog user	Active user	N	MPHICN not ...	Not locked
<NA>		208 GOODS ISSUES AND PROCESS LIST OF DIFFERENCES	User is able to post incorrect goods issues and clear inventory differences	<input type="checkbox"/>	Hoog				Dialog user	Active user	N	MPHICN not ...	Not locked
<NA>		209 GOODS ISSUES - SCRAPPING AND ENTER INVENTORY COUNT WITH ...	User is able to post incorrect goods issues and create inventory counts	<input type="checkbox"/>	Hoog				Dialog user	Active user	N	MPHICN not ...	Not locked

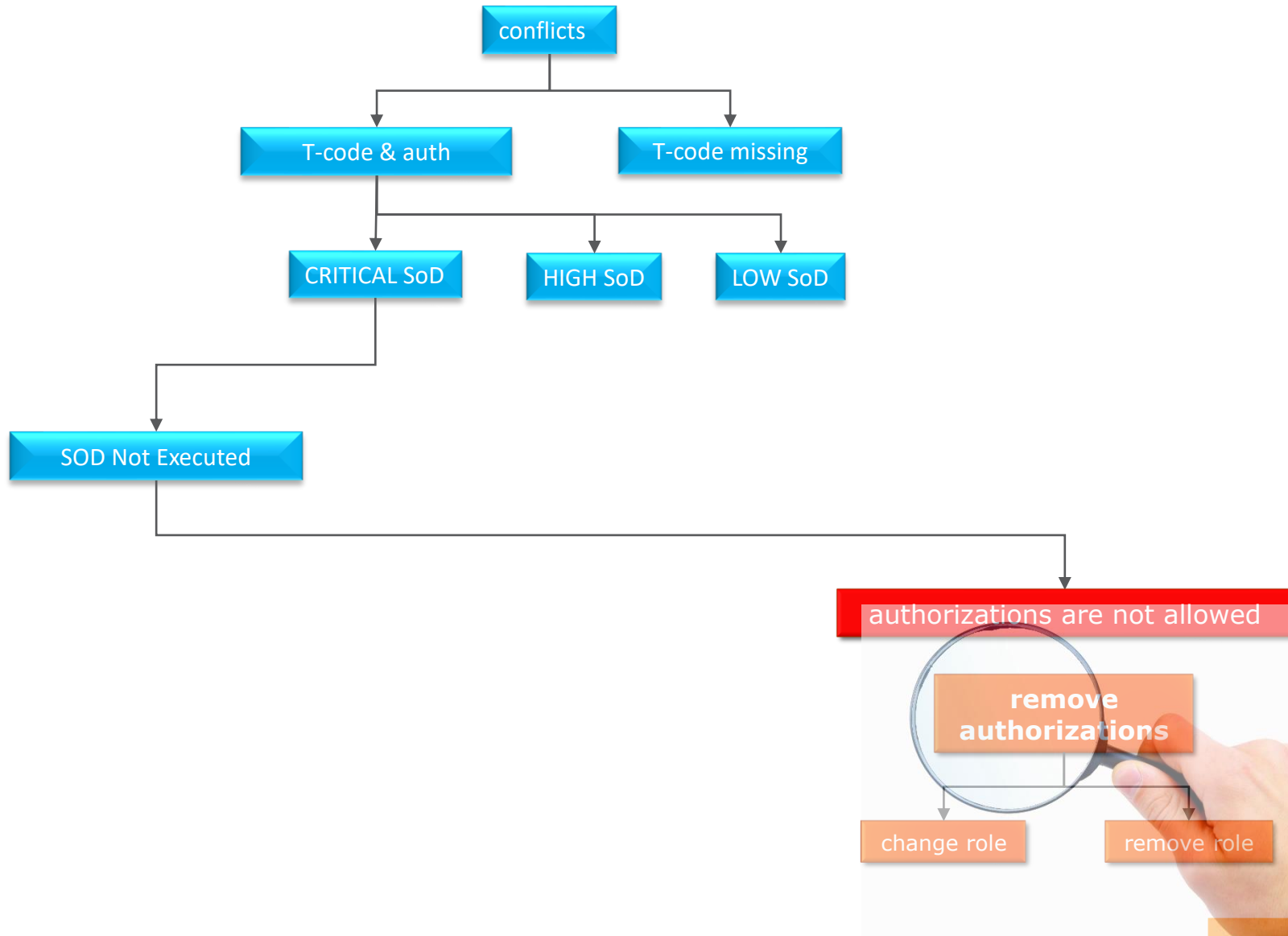
3. Detectieve analyse

Resultaat regelset

SOD conflicten regelset met toegewezen SOD criticiteit:

- **Critical:** SOD conflict mag niet voorkomen in de organisatie.
- **High:** SOD conflict mag voorkomen, maar compenserende controle maatregel moet actief aanwezig zijn.
- **Low:** SOD conflict mag niet voorkomen in de organisatie, maar laag risico.

4. Opschoning SOD conflicten CRITICAL



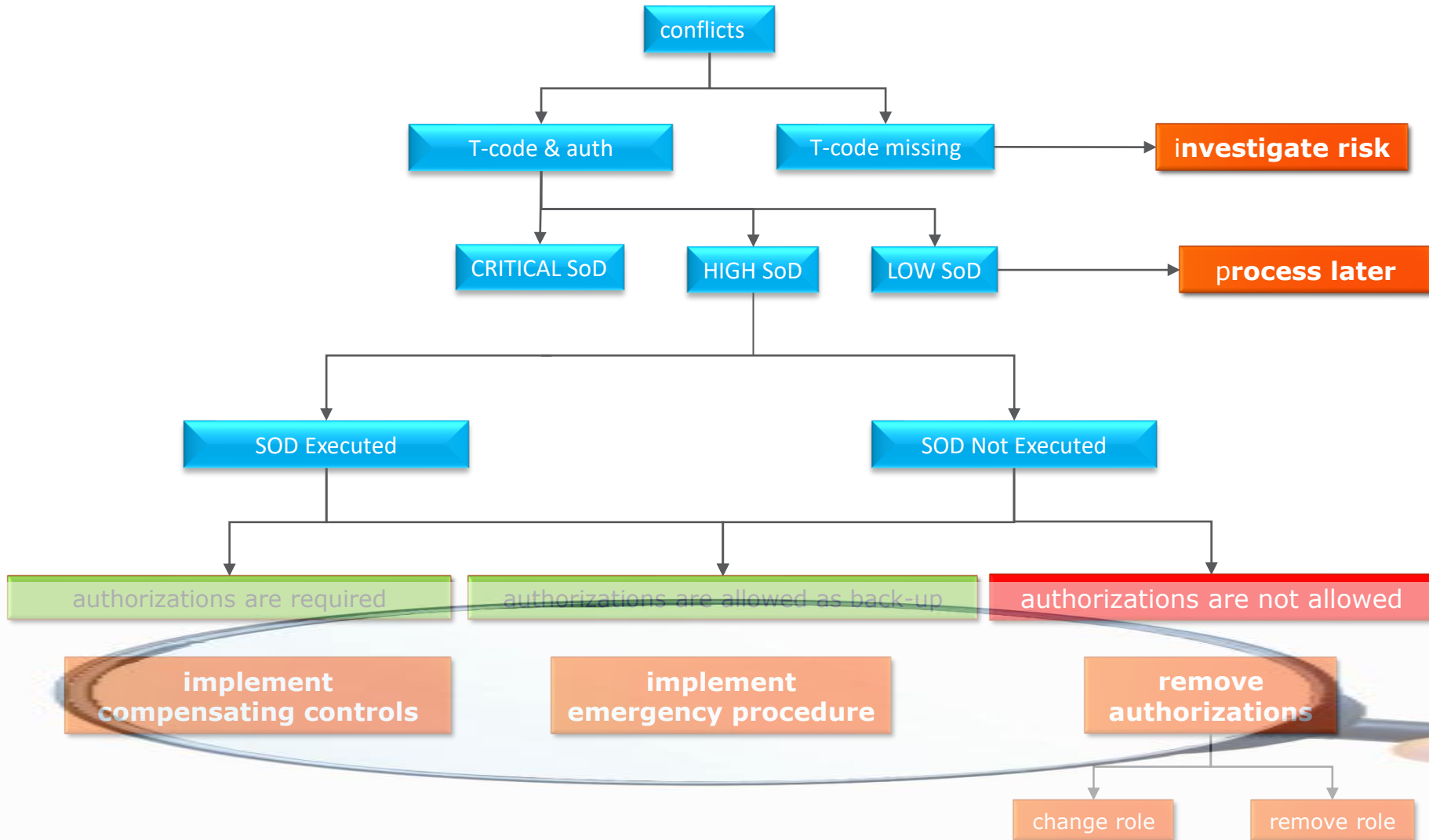
4. Opschoning SOD conflicten CRITICAL

- Analyseren
- Veranderingen in de toegewezen autorisaties.
- Veranderingen in rol concept inconsistenties.

Voordeel:

Hier is input van business nog niet nodig

4. Opschoning SOD conflicten HIGH



4. Opschoning SOD conflicten HIGH

SOD conflicten HIGH oplossen met input van business:

- Web reports
- Direct input

The screenshot shows a web browser window with a tab titled "RC users (SAP)". The address bar shows a URL starting with "https://". The main content area displays a table of users with columns for User group, User id, Username, Type, Status, and Lock status. A modal window titled "Update norm" is open, showing details for a SoD rule: "150 RELEASE PO.INV. VIA FB02 INSTD OF MR02 AND A/P OUTGOING PAYMENT POSTINGS". The rule is associated with the user group "User is able to release invoices in MM and release an unwanted payment". The modal also shows fields for Norm (set to "T") and Reasoncode (set to "NC").

s	User group	User id	Username	c	Type	Status	Lock status	U...
>	[redacted]	[redacted]	[redacted]		System user	Active user	Not locked	[redacted]
>	[redacted]	[redacted]	[redacted]		System user	Active user	Not locked	[redacted]
>	[redacted]	[redacted]	[redacted]		Communicati...	Active user	Not locked	[redacted]
>	[redacted]	[redacted]	[redacted]		System user	Active user	Not locked	[redacted]
>	[redacted]	[redacted]	[redacted]		System user	Active user	Not locked	[redacted]
>	[redacted]	[redacted]	[redacted]		System user	Active user	Not locked	[redacted]
>	[redacted]	[redacted]	[redacted]		System user	Active user	Not locked	[redacted]
>	[redacted]	[redacted]	[redacted]		System user	Active user	Not locked	[redacted]
>	[redacted]	[redacted]	[redacted]		System user	Active user	Not locked	[redacted]
>	[redacted]	[redacted]	[redacted]		System user	Active user	Not locked	[redacted]
>	[redacted]	[redacted]	[redacted]		System user	Active user	Not locked	[redacted]

Update norm

SoD rule: 150 RELEASE PO.INV. VIA FB02 INSTD OF MR02 AND A/P OUTGOING PAYMENT POSTINGS

Ruleset: User is able to release invoices in MM and release an unwanted payment

User: [redacted]

Usergroup: [redacted]

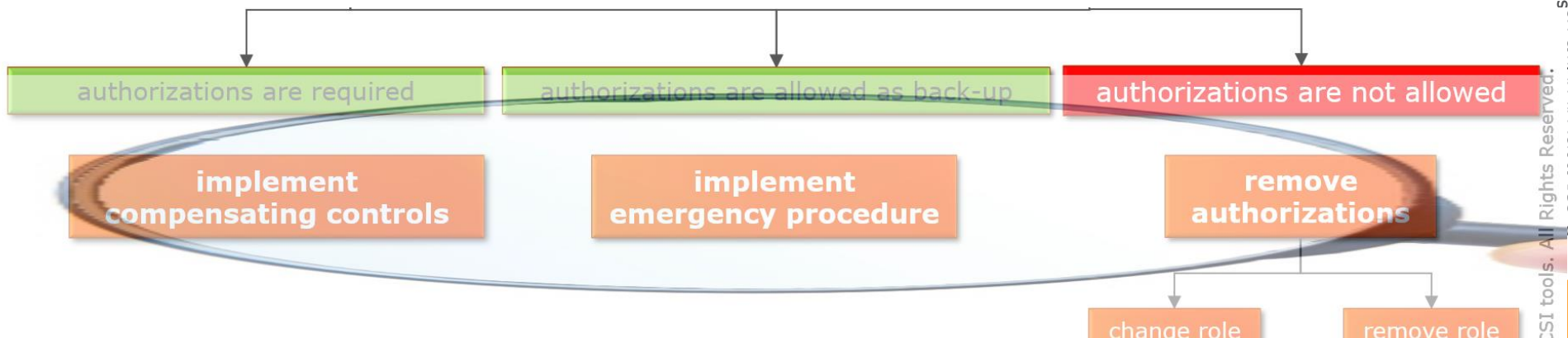
Norm: T
To be defined

Reasoncode: NC

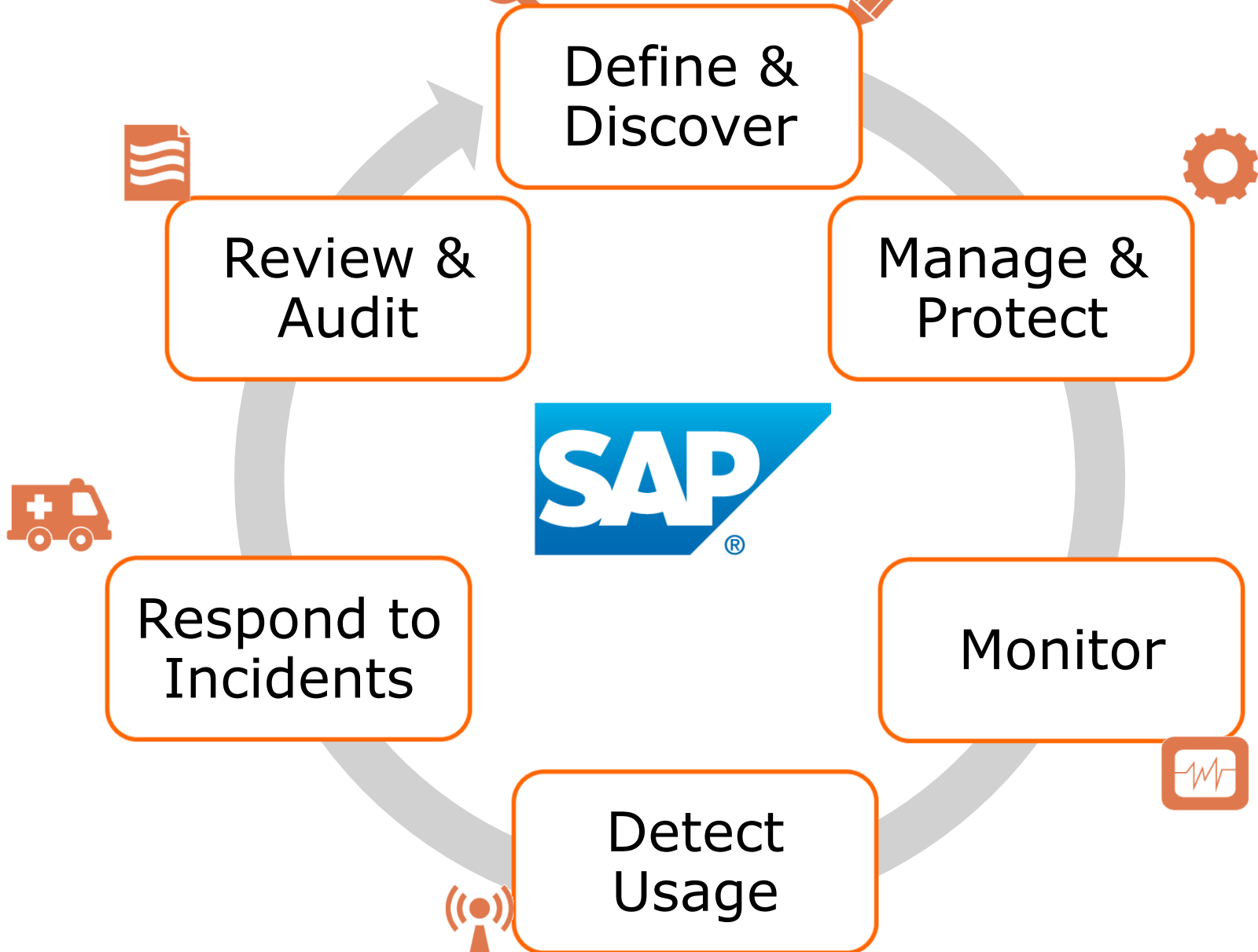
Variant: XVENMA not Mass Maintain Vendor Master Data (Central Remove SOD SOD conflict can be removed, functionality r Contract aanp Contract aanpassing is nodig voor zand.

4. Opschoning SOD conflicts HIGH – Normen

- Norm **Backup**
- Norm **NOK**
- Norm **OK**



4. Opschoning SOD conflicten HIGH– Backup users Implementatie van PAM (CSI ER)



4. Opschoning SOD conflicten HIGH Implementatie van PAM (CSI ER)

CSI ER - Emergency Request

Remote login

ATTENTION: Use the CSI Emergency Procedure only in very specific situations. Enter a short reason, select the required profile and get access to an emergency request.

Once filled out and Profile highlighted, click Remote login on top.

Profile

Profile	FI ACCESS ONLY
	FULL ACCESS

System Help

SAP

Start SAP Easy Access

This will open a new SAP session. Notice user = FF_FI_001 which is the next available FF ID for the requested 'FI ACCESS ONLY' profile

- System AXT (1) 500
- Client 500
- User FF_FI_001
- Program SAPMSYST
- Transaction S000
- Response Time 360 ms
- Interpretation Time 250 ms
- Round Trips/Flushes 1/1

4. Opschoning SOD conflicten HIGH via PAM functionaliteit

- Drie soorten privileged users
 1. Emergency end-users
 2. SAP Privileged users
 3. Backup users

4. Opschoning SOD conflicten HIGH via PAM functionaliteit

1. Emergency end-users (emergency users)
 - Splitsing
 - Goedkeuring
 - Logging
 - Log analyse
 - Geen credential sharing.

4. Opschoning SOD conflicten HIGH via PAM functionaliteit

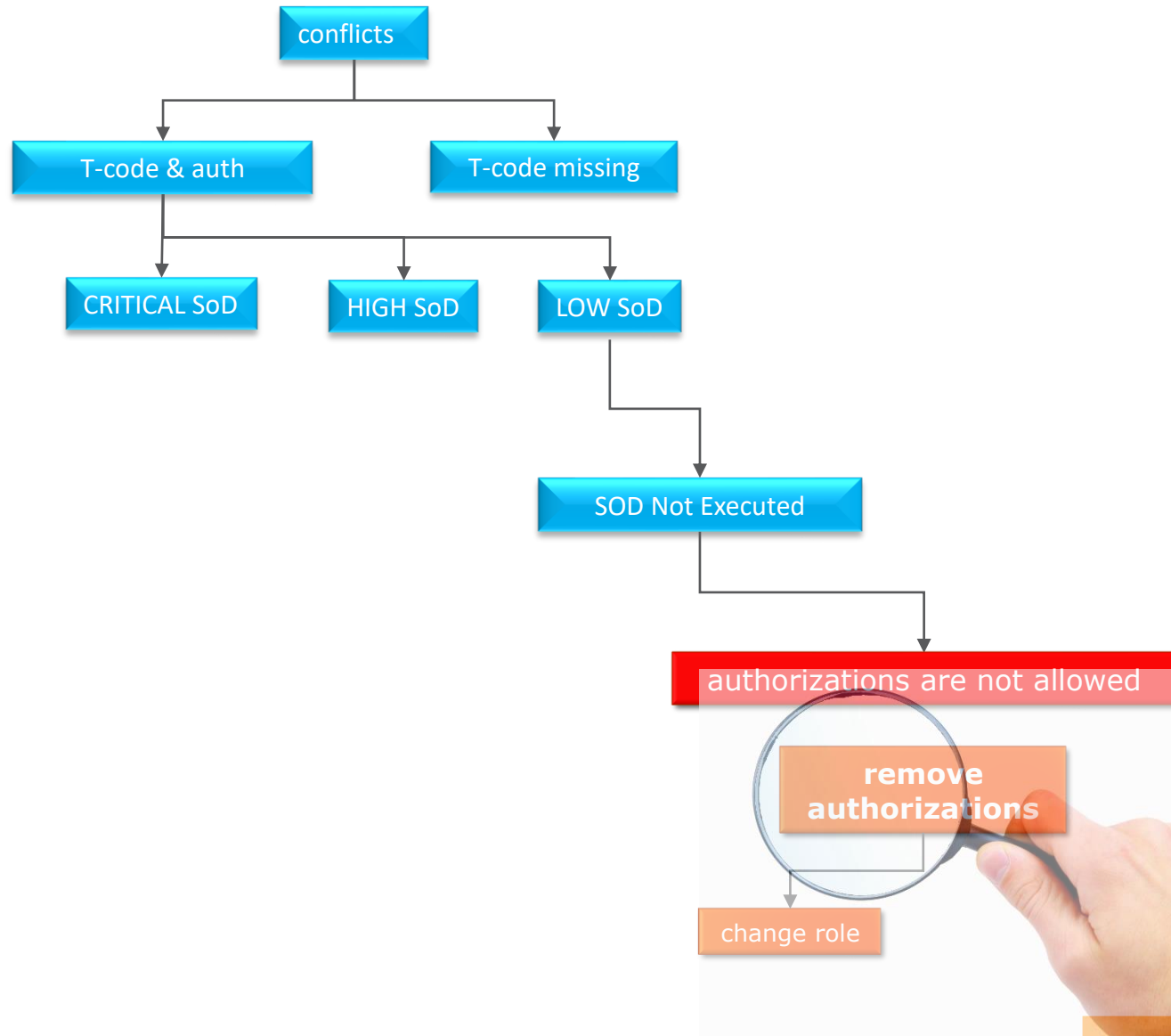
2. SAP Privileged users
 - Logging
 - Log analyse

4. Opschoning SOD conflicten HIGH Backup users – via PAM functionaliteit

3. Backup users

- Eigen emergency profiel
- Beschikbaar
- Complete logging
- Geen credential sharing
- Log analyse

4. Opschoning SOD conflicten LOW



4. Opschoning SOD conflicten LOW

SOD conflicten LOW

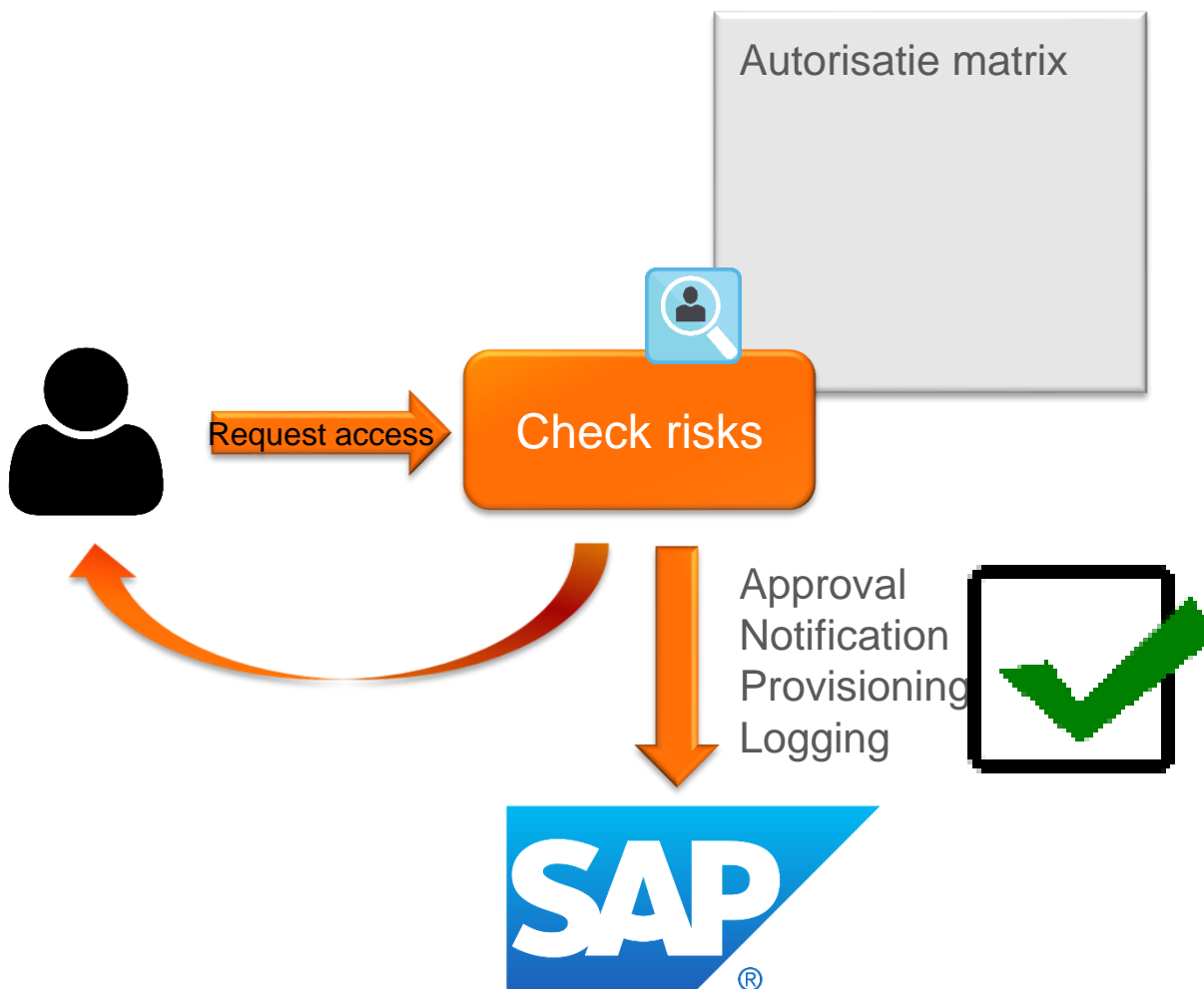
- Autorisaties wegnemen

5. Preventieve maatregelen

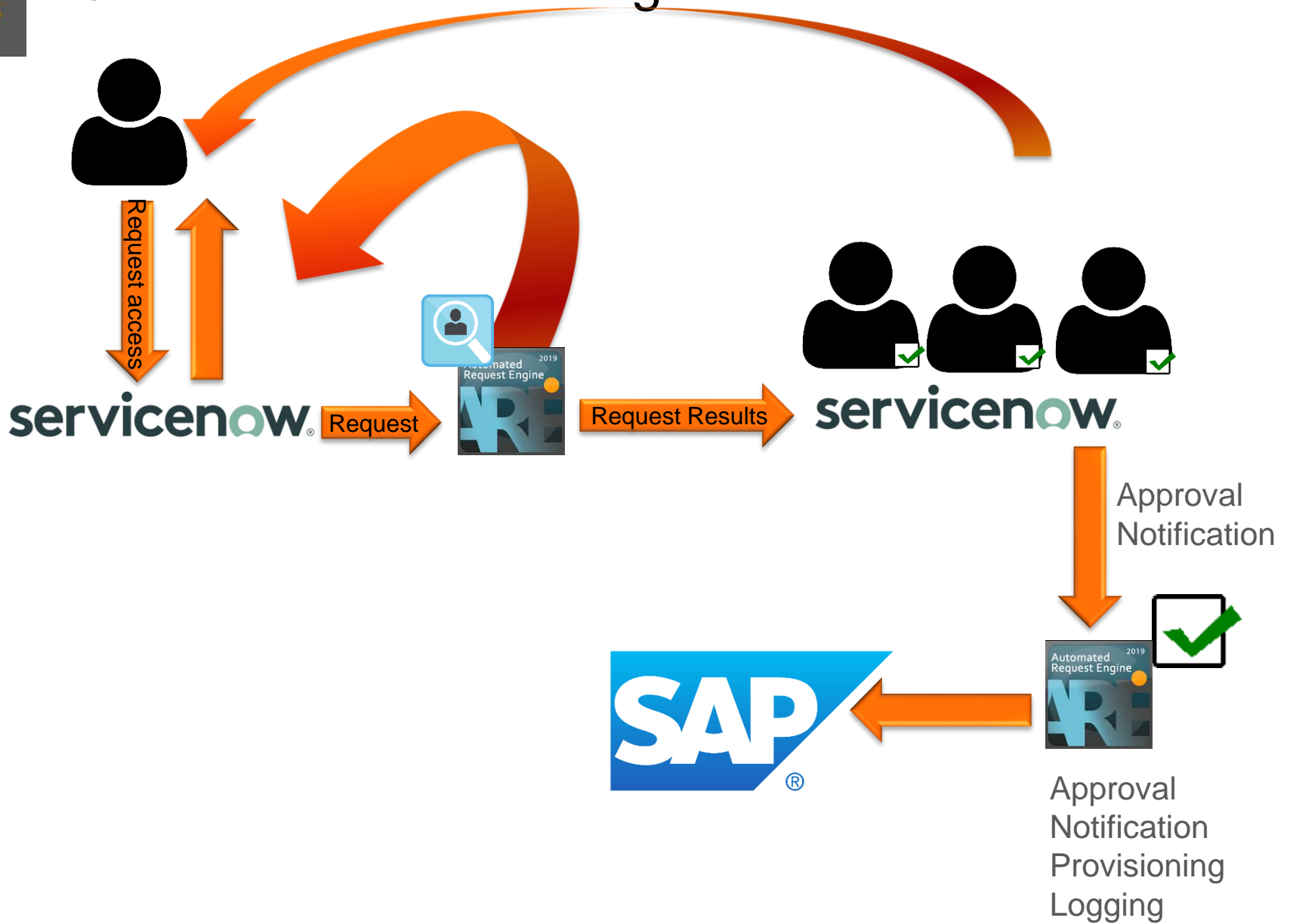
Stay clean



5. Preventieve maatregelen



5. Preventieve maatregelen



5. Preventieve maatregelen Integratie met ServiceNow

- Request in ServiceNow
- Analyse door CSI ARE
- Resultaten wordt terug gestuurd naar ServiceNow
 - Akkoord in ServiceNow – **automatische provisioning** in SAP door CSI ARE
 - Niet akkoord – kritisch conflict. Aanvraag wordt direct afgewezen
 - Niet akkoord in ServiceNow – aanvraag wordt afgewezen en aanvrager ontvangt feedback.

5. Preventieve maatregelen Integratie met ServiceNow

Goedkeuringsverzoek Requested Item RITM0159327

[redacted]@service-now.com

To [redacted]

If there are problems with how this message is displayed, click here to view it in a web browser.

sys_attachment.dosys_id=a2b9cc2ddb2af7c0a81e14a05b9619c8
6 KB

RITM0159327 - Accounts en rollen aanvragen voor Bedrijfsapplicaties (SAP, Acto, Basware, etc.)	
Algemene gegevens aanvrager	
Geregistreerd voor (begin zoekopdracht met: *) [redacted]	Geregistreerd door: [redacted]
Aanvraag	
Gewenste actie: Bestaande applicatie gebruiker wijzigen	
Gebruikersgegevens	
Voornaam: [redacted]	Windows gebruikersnaam: [redacted]
	Afdeling: Services Utiliteit
Achternaam: [redacted]	
Personeelnummer: [redacted]	
Email adres: [redacted]	
SAP Gebruikersnaam: [redacted]	
Toegang	
Applicatiennaam: SAP	
Omgeving: Productie omgeving	
Voor welk bedrijf: [redacted]	
Met welke rol(len):	
Rol 1: Inkoper	Toevoegen of verwijderen: Toevoegen
Goedkeuringsstatus rol 1: Aangevraagd	

SOD check: aangevraagde rollen

Rolnaam	Actie
[redacted]	toevoegen
[redacted]	toevoegen
[redacted]	toevoegen
[redacted]	toevoegen

SOD check: conflicten

SOD nummer	SOD omschrijving	Variant	Status
PTP_TT_B2_0072	(Purchase Orders or Mass) AND Release Purchase Orders	NA	A
	Veroorzakende rol: MWESTBUTVA		

Quick wins

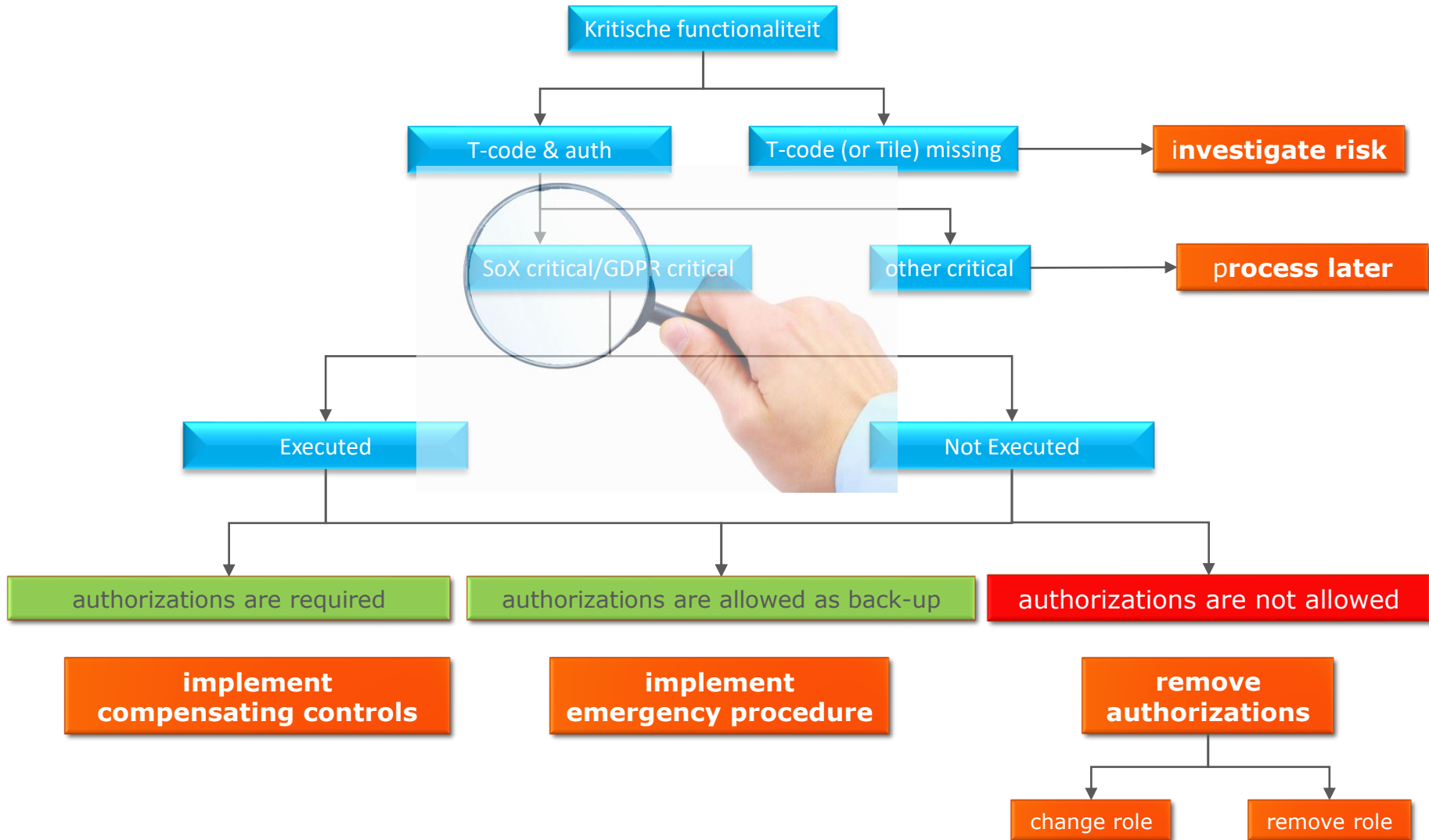
- Display rollen
- * waardes
- Back up users
- SCRUM sessies
- Preventieve analyse
- Compenserende controle maatregelen
- Audit trail
- S/4 readiness

Alternatieve aanpak

- Kritische toegang
- SoX_C, SoX_H
- Kritische toegang met risico's
- Voorbeelden van kritische/sensitieve data:
 - Master data voor debiteuren, crediteuren, grootboek, materialen, prijzen,....
 - HR data zoals persoonlijke adresgegevens, salaris,..

Alternatieve aanpak

Get clean remediation decision tree



Acknowledgements

Microsoft Access, Microsoft .Net and Microsoft SQL are registered trademarks of Microsoft. SAP and other SAP products or services, mentioned herein, are trademarks or registered trademarks of SAP SE. CSI Accelerator, CSI Authorization Auditor, CSI Role Build & Manage, CSI Data Xtractor, CSI Integrate & Collaborate and CSI Automated Request Engine are registered trademarks of CSI tools.



Meta Hoetjes

Meta.hoetjes@csi-tools.com

06-24651761



**FOCUS
ONLINE**

8 T/M 12 NOVEMBER 2021

Bedankt voor je deelname

Bekijk op www.VNSGFocusOnline.nl welke sessies er nog meer zijn!

CSI
tools