Secureway

Diagnostic des autorisations SAP

Sommaire

Secureway

Contexte

XXXXXXX utilise SAP depuis XXX et couvre les besoins fonctionnels des 1000 utilisateurs du site de XXXXXXXXXX.

En XXXX, un projet de migration a été réalisé et les autres grands sites du groupe (principalement XXXXXX et XXXXXX) seront progressivement migrés entre 2025 et 2026 dans l'environnement XXX afin d'uniformiser les processus de gestion et de centraliser le SI.

Le nombre d'utilisateurs passera ainsi d'environ 1000 actuellement à plus de 3000 à l'horizon 2026.

Les intégrateurs ayant participé à ces projets ont successivement adapté les autorisations existantes, puis délivré un nouveau modèle d'autorisations pour gérer la transition et les déploiements dans le nouvel environnement S/4HANA®.

C'est dans ce contexte que XXXXXXX a sollicité SECUREWAY et SWAWE Labs afin de déterminer leur exposition aux risques SoD (Segregation of Duties) & données critiques et d'évaluer le modèle de rôles actuels.

Démarche proposée

Secureway

Démarche proposée

Définition des risques SOD et accès sensibles

- Proposition de matrice de risques SOD et accès sensibles basée sur les standards SAP
- Personnalisation de trois risques d'accès critiques propres à XXXXXXX
- Validation de la conception de la matrice

Construction de la matrice

- Implémentation de la matrice SOD et des accès critiques
- Tests unitaires et ajustements
- Rédaction de la documentation

Diagnostic

- Définition et création de query pour simplifier les analyses
- Analyses SOD et accès critiques au niveau utilisateurs / rôles / profils
- Identification des améliorations possibles
- Qualification et classification des risques
- Rédaction du compte rendu

Restitution et Transfert

- Présentation des conclusions, du plan d'action, échanges sur les avantages et inconvénients des différentes solutions
- Remise des livrables :
  - Documentation
  - Compte rendu détaillé
  - Recommandation de plan d'action

Secureway

Séparation des tâches (SOD)

Lors de la réalisation de cet audit, SECUREWAY a conçu la matrice des risques SOD suivante avec l'approbation des interlocuteurs interviewés :

SOD Matrix	FI-VEND-PAY	FI-VEND-POST	FI-VEND-CHECK	FI-CUST-PAY	FI-CUST-CASH	FI-CUST-CLEARING	FI-CUST-CREDIT	FI-CUST-BILLING	FI-CUST-CRED-MEMO	FI-CUST-POST	FI-ASSET-POST	FI-ASSET-MD	FI-BANK-RECO	FI-BANK-MD	FI-TREAS-POST	FI-TREAS-TRAD	MM-IM-DIFF-CLEAR	MM-IM-COUNT	MM-IM-CLEAR-COUNT	MM-GOODS-MOVT	MM-GOODS-RECEIPT	WM-COUNT	WM-DIFF-CLEAR	MM-VEND-MD	MM-PURCH-ORDER	MM-SERV-MASTER	MM-PO-APPROV	MM-PURCH-AGREE	MM-SERV-ACCEPT	PS-PROJ-WBS	PS-OVERHEAD-POST	PS-PROJ-SETTLE	SD-CUST-MD	SD-DELIV	SD-REBATES	SD-SALES-RELEASE	SD-SALES-ORDER	SD-SALES-PRICE
FI-VEND-PAY - Vendor Invoice Payment		X											X	X										X	X	X	X	X	X										
FI-VEND-POST - Vendor Invoice Postings	X		X								X		X								X			X	X		X	X											
FI-VEND-CHECK - Vendor Check Processing		X											X	X										X	X	X	X	X	X										
FI-CUST-PAY - Customer Invoice Payment									X					X																				X					
FI-CUST-CASH - Customer Cash Application							X	X		X			X	X																				X	X	X	X		
FI-CUST-CLEARING - Customer Clearing								X	X																									X				X	
FI-CUST-CREDIT - Customer Credit Management					X					X																										X		X	
FI-CUST-BILLING - Customer Billing Document					X	X																												X			X	X
FI-CUST-CRED-MEMO - Customer Credit Memos				X		X																																
FI-CUST-POST - Customer Invoices Postings					X		X																											X			X	X
FI-ASSET-POST - Assets Postings		X																			X																	
FI-ASSET-MD - Asset Master Data																					X																	
FI-BANK-RECO - Finance Bank Reconciliation	X	X	X		X																																	
FI-BANK-MD - Finance Bank Master Data	X		X	X	X																																	
FI-TREAS-POST - Finance Treasurery Postings																X																						
FI-TREAS-TRAD - Finance Treasurery Trade															X																							
MM-IM-DIFF-CLEAR - MM Inventory Management Difference Clearing																				X					X		X											
MM-IM-COUNT - MM Inventory Management Counts																																						
MM-IM-CLEAR-COUNT - MM Inventory Management Clearing & Counts																				X					X		X											
MM-GOODS-MOVT - MM Goods Movements																	X	X				X																
MM-GOODS-RECEIPT - MM PO Goods Receipt		X									X	X													X		X	X										
WM-COUNT - Warehouse Management Counts																				X					X		X											
WM-DIFF-CLEAR - Warehouse Management Difference Clearing																																						
MM-VEND-MD - Vendor Master Data	X	X	X																						X		X	X										
MM-PURCH-ORDER - Material Purchase Order	X	X	X														X	X		X	X	X					X											
MM-SERV-MASTER - Service Master	X		X																																		
MM-PO-APPROV - Material Purchase Order Approval	X	X	X														X	X		X	X	X	X															
MM-PURCH-AGREE - Material Purchase Agreement	X	X	X																	X			X															
MM-SERV-ACCEPT - Service Acceptance	X		X																																			
PS-PROJ-WBS - Projects and WBS Element Management																															X	X						
PS-OVERHEAD-POST - Project System Overhead Postings																													X			X						
PS-PROJ-SETTLE - Project Settlement																													X	X								
SD-CUST-MD - Customer Master Data				X	X	X		X		X																									X		X	
SD-DELIV - Customer Delivery Processing					X																																X	
SD-REBATES - Customer Rebates					X		X																											X				
SD-SALES-RELEASE - Customer Sales Document Release					X																																	
SD-SALES-ORDER - Customer Sales Order						X	X	X		X																								X	X			X
SD-SALES-PRICE - Customer Pricing Conditions								X		X																												X	

Matrice SOD

Legende des risques :	
X	Système de base (EN :Basis)
X	Comptabilité financière (EN :Finance)
X	Gestion des articles (EN :Materials Management)
X	Processus d'approvisionnement (EN :Procure to Pay)
X	Gestion des commandes (EN :Order to Cash)

- 76 risques SOD
- 44 risques BASIS
- 3 risques d'accès sensibles / critiques spécifiques :
  - PM: Type d'Ordre XXXX
  - Gestion des stocks magasins « clients »
  - Consultation des stocks magasins « clients »

Analyse SOD – Rôles

Rôles	Type	Nombre de risques
[illegible]	SINGLE	120
[illegible]	SINGLE	120
[illegible]	SINGLE	119
[illegible]	SINGLE	106
[illegible]	SINGLE	103
[illegible]	SINGLE	95
[illegible]	SINGLE	86
[illegible]	SINGLE	80
[illegible]	COLLECTIVE	71
[illegible]	COLLECTIVE	70
[illegible]	COLLECTIVE	65
[illegible]	COLLECTIVE	65
[illegible]	COLLECTIVE	55
[illegible]	COLLECTIVE	54
[illegible]	COLLECTIVE	48
[illegible]	COLLECTIVE	47
[illegible]	COLLECTIVE	47
[illegible]	COLLECTIVE	47
[illegible]	COLLECTIVE	47
[illegible]	COLLECTIVE	44
[illegible]	COLLECTIVE	43
[illegible]	COLLECTIVE	42
[illegible]	COLLECTIVE	41
[illegible]	COLLECTIVE	40
[illegible]	SINGLE	39
[illegible]	SINGLE	37
[illegible]	COLLECTIVE	37
[illegible]	COLLECTIVE	37
[illegible]	COLLECTIVE	37
[illegible]	COLLECTIVE	35
[illegible]	COLLECTIVE	35

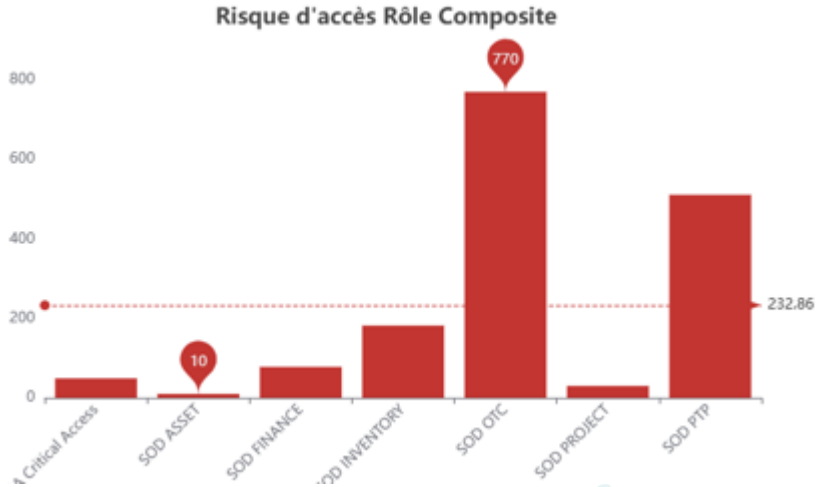
L'analyse montre que 738 rôles présentent des conflits SOD :

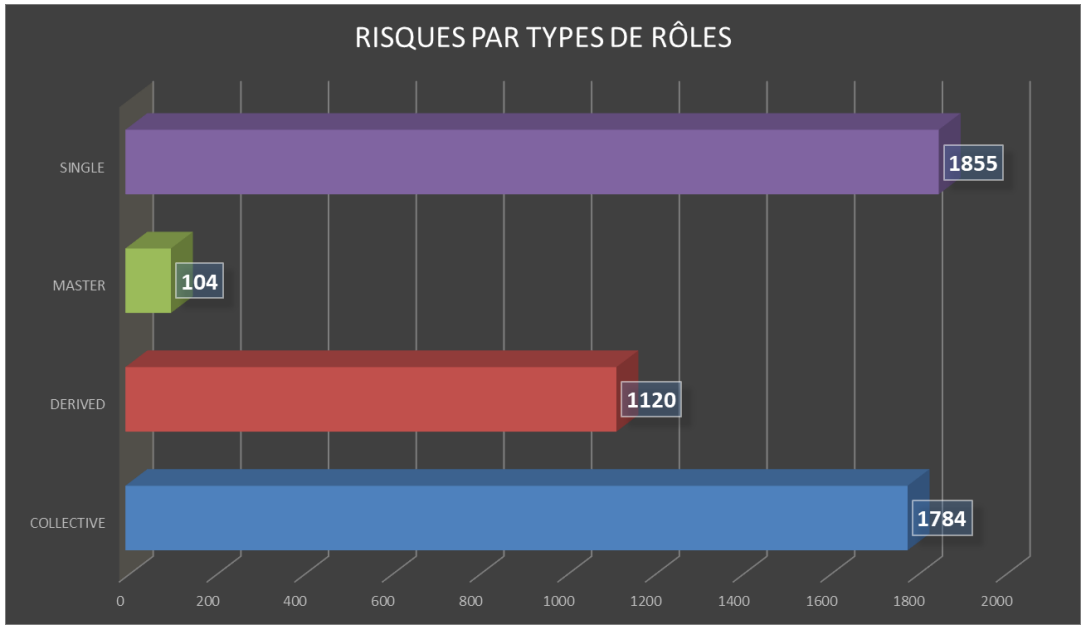
- 537 rôles conflictuels sur 2352 assignés à des utilisateurs.

À gauche, les 35 rôles présentant le plus grand nombre de risques.

À droite, la répartition des risques par processus au niveau rôles composites.

Ci-dessous la répartition des risques par type de rôles.





Secureway

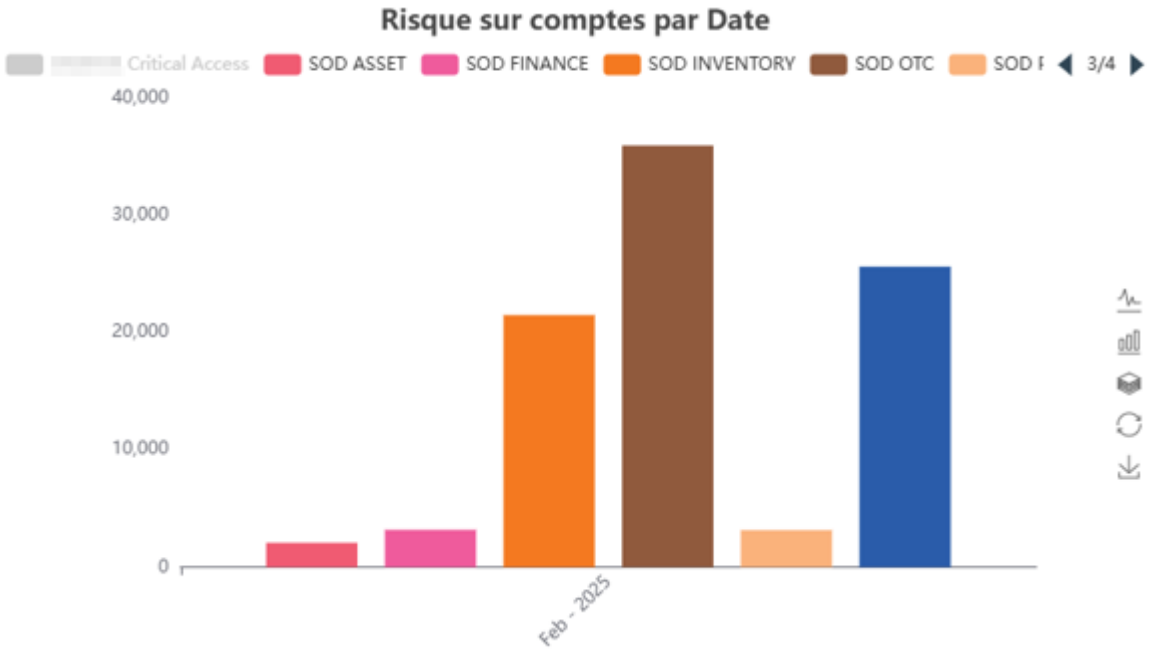
Analyse SOD – Utilisateurs

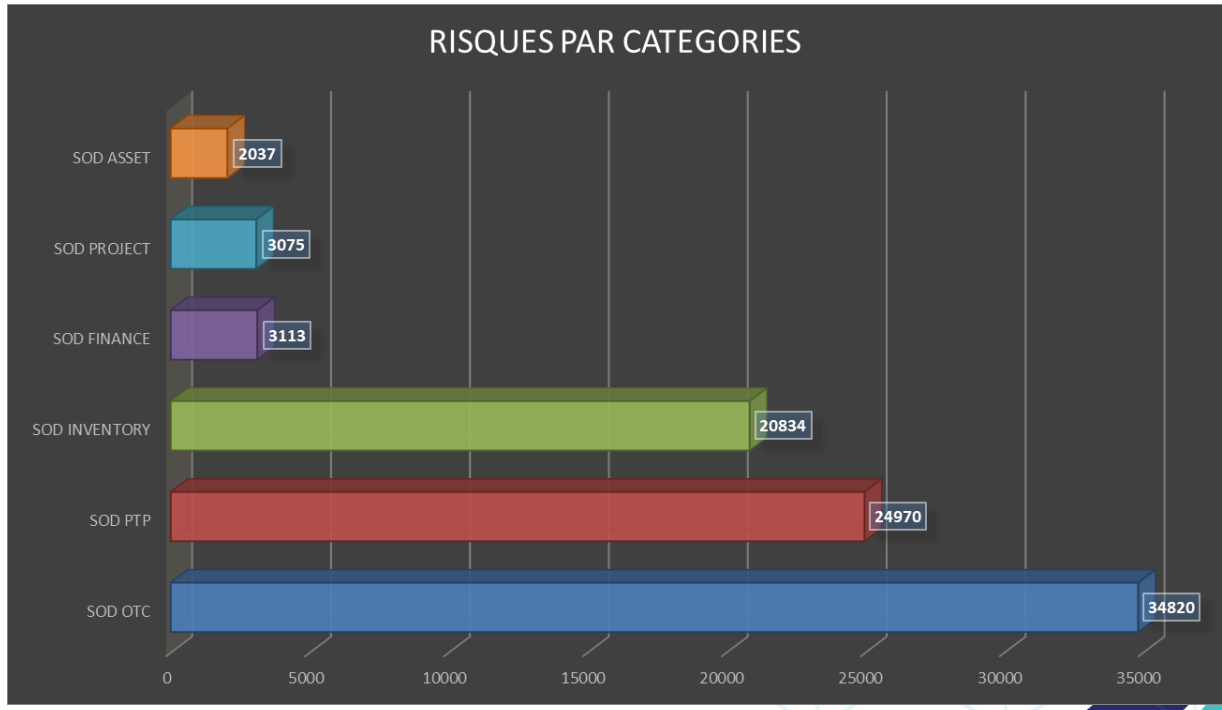
88849 risques SOD détectés pour l'ensemble des utilisateurs du système XXX.

En ne considérant que les utilisateurs actifs, ce nombre atteint 13716 risques, répartis sur 991 utilisateurs sur les 1541 actifs.

47 utilisateurs disposent de profils générant le nombre maximum de conflits, soit 76 risques (via SAP_ALL ou équivalent).

La répartition des conflits est nettement plus importante pour les processus Order To Cash, Procure To Pay et Inventory Management comme le montrent les graphiques ci-dessous :





Secureway

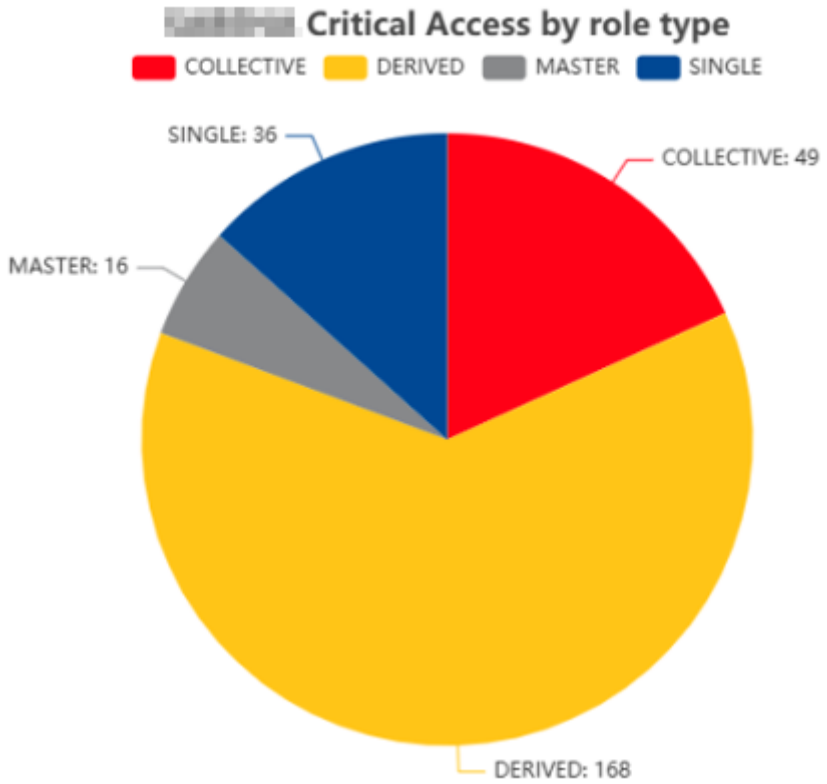
Analyse Risques spécifiques XXXXXXX

21/02/2021

Nous avons seulement pu évaluer le risque « Maintain XXX Order » (« Accès Critique Besoin sur Ordre XXX »).

3220 violations ont ainsi été détectées pour l'ensemble des utilisateurs du système XXX durant l'analyse réalisée le 21/02/2025. En ne considérant que les 1516 utilisateurs actifs, ce nombre atteint 1247 risques.

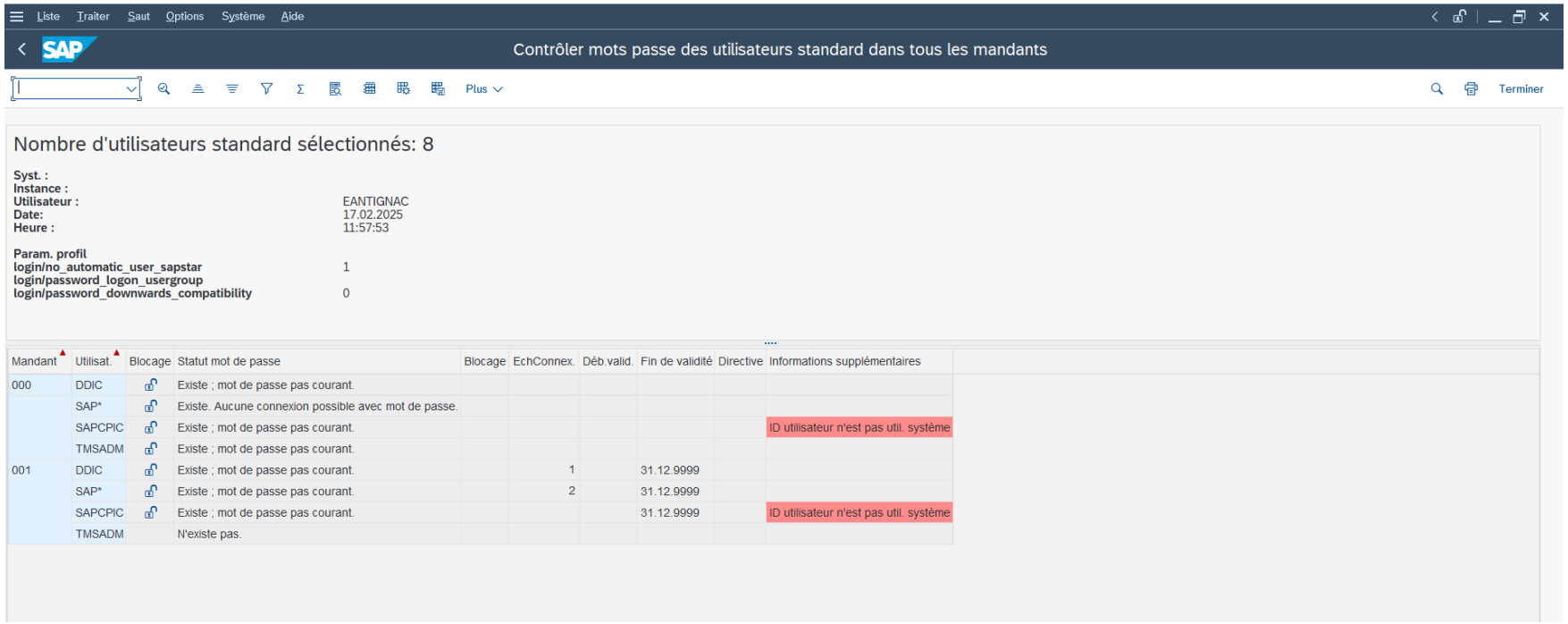
269 rôles donnent accès au risque Accès Critique Besoin sur Ordre XXX, avec la répartition suivante entre rôles maîtres, rôles dérivés, rôles composites et rôles simples :



Secureway

Sécurité des utilisateurs standards SAP

La sécurité des utilisateurs standards SAP est bien maitrisée, aucun mot de passe connu :



Note 2383

Note 29276

Note 68048

Sécurité des utilisateurs standards SAP maîtrisée

Secureway

Paramètres de Sécurité SAP

Les paramètres de sécurité ci-dessous sont convenablement gérés et pourraient être améliorés en appliquant les recommandations de la diapositive suivante :

Parameter Name	User-Defined Value	System Default Value	System Default Value(Unsubstituted Form)	Comment
login/accept_sso2_ticket		1	1	Accept SSO tickets for this (component) system
login/certificate_mapping_rulebased		0	0	enable / disable rule-based X.509 certificate mapping
login/certificate_request_ca_url		https://tcs.mySAP.com/inv	https://tcs.mySAP.com/invoke/tc/usercert	URL of the certificate authority (for certificate requests)
login/certificate_request_subject		CN=&UNAME, OU=&WPOU,	CN=&UNAME, OU=&WPOU, O=mySAP.com User, C=DE	Template for the subject of a certificate request
login/create_sso2_ticket		3	3	Create SSO tickets on this system
login/disable_cpic	1	1	1	Disable Incoming CPIC Communications
login/disable_multi_gui_login	1	1	1	disable multiple sapgui logons (for same SAP account)
login/disable_password_logon		0	0	login/disable_password_logon
login/failed_user_auto_unlock		0	0	Enable automatic unlock off locked user at midnight
login/fails_to_session_end		3	3	Number of invalid login attempts until session end
login/fails_to_user_lock		5	5	Number of invalid login attempts until user lock
login/isolate_rfc_system_calls		1	1	isolate RFC system calls
login/logon_category_restriction		0	0	Logon Restriction based on Logon Category
login/min_password_diff		3	3	min. number of chars which differ between old and new password
login/min_password_digits		1	1	min. number of digits in passwords
login/min_password_letters		1	1	min. number of letters in passwords
login/min_password_lng		10	10	Minimum Password Length
login/min_password_lowercase		1	1	minimum number of lower-case characters in passwords
login/min_password_specials		0	0	min. number of special characters in passwords
login/min_password_uppercase		1	1	minimum number of upper-case characters in passwords
login/multi_login_users				list of exceptional users: multiple logon allowed
login/no_automatic_user_sapstar		1	1	Control of the automatic login user SAP*
login/password_change_for_SSO		1	1	Handling of password change enforcements in Single Sign-On situations
login/password_change_waittime		1	1	Password change possible after # days (since last change)
login/password_charset		1	1	character set used for passwords
login/password_compliance_to_current_policy		0	0	current password needs to comply with current password policy
login/password_downwards_compatibility	0	0	0	password downwards compatibility (8 / 40 characters, case-sensitivity)
login/password_expiration_time		0	0	Dates until password must be changed
login/password_hash_algorithm	encoding=RFC2307, algorithm=iSSHA	encoding=RFC2307, algorit	encoding=RFC2307, algorithm=iSSHA-512, iterations=15000, saltsize=256	encoding and hash algorithm used for new passwords
login/password_history_size		15	15	Number of records to be stored in the password history
login/password_logon_usergroup				users of this group can still logon with passwords
login/password_max_idle_initial	7	7	7	maximum #days a password (set by the admin) can be unused (idle)
login/password_max_idle_productive	180	180	180	maximum #days a password (set by the user) can be unused (idle)

Paramètres de Sécurité SAP

XXXXXXX ayant activé le SNC, la plupart des utilisateurs se connectent sans mot de passe et ne sont pas concernés par ces paramètres.

SSO mis en place via SNC

Pour les autres utilisateurs (administrateurs, externes,…), il est habituellement recommandé d'accroitre le niveau de sécurité en renseignant les valeurs suivantes pour :

Login/min_password_special : Ce paramètre définit le nombre minimum de caractères spéciaux d'un mot de passe (), !, \, $, %,:,', “, ;, =, &, #, },],{,[, >, < . Valeur recommandée = 1.

En outre, vous pouvez également utiliser le paramètre login/password_max_idle_productive afin de désactiver le mot de passe des utilisateurs inactifs. Valeur recommandée = 90.

Login/password_expiration_time : Ce paramètre détermine le nombre de jours avant qu'il soit obligatoire de changer le mot de passe. Valeur recommandée = 90.

La table des mots de passe triviaux (USR40) n'est pas maintenue, il est habituellement recommandé de lister les mots de passe communs qu'il ne sera plus possible de renseigner :

Par exemple *XXXXXXX*, BONJOUR*, HELLO*, 123*,…

Voici une note SAP expliquant ces différents éléments liés à la sécurité des mots de passe :

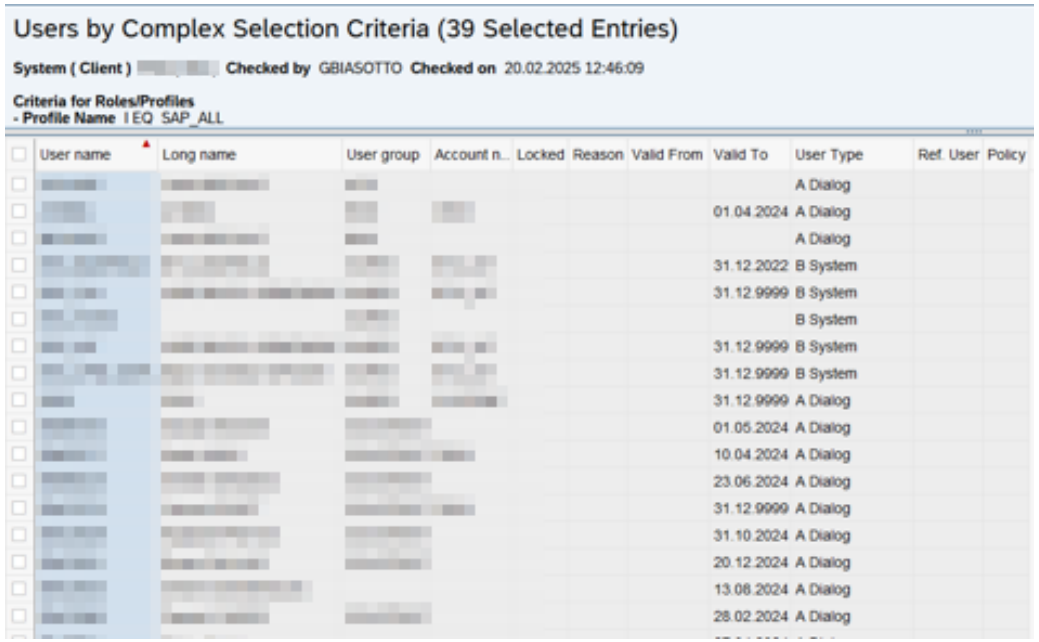
Paramètres de sécurité à renforcer

Secureway

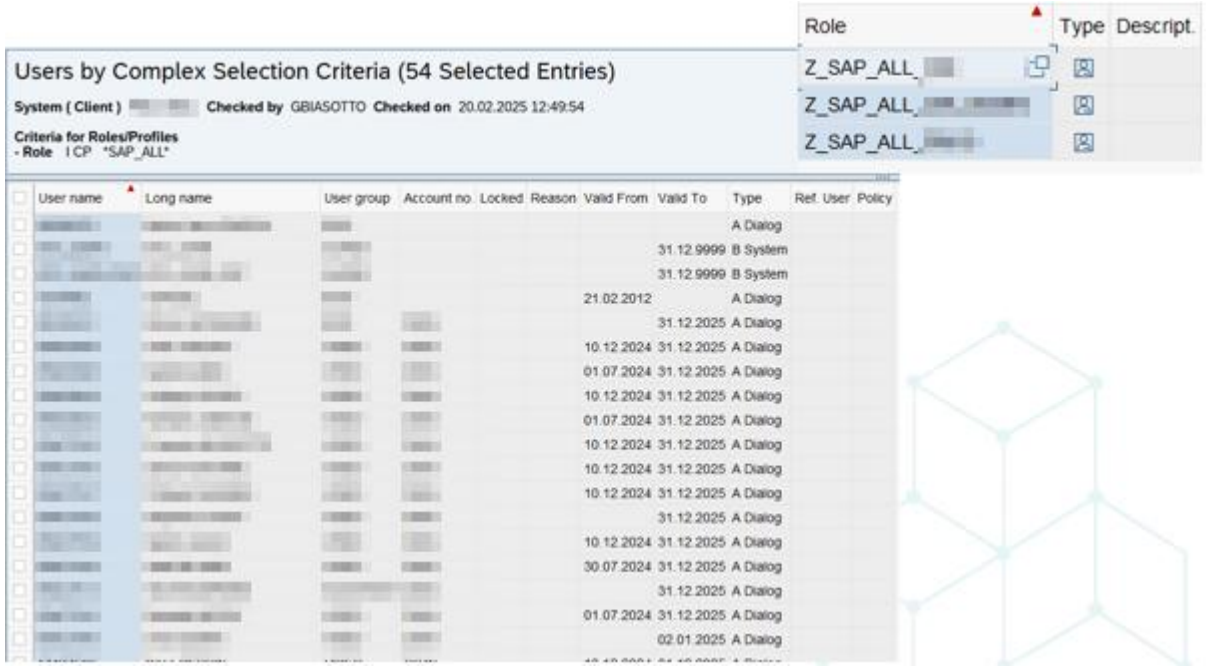
Attribution du profil SAP_ALL

Le profil SAP_ALL donne accès à pratiquement toutes les fonctionnalités disponibles dans SAP, ce qui en fait un danger en termes de sécurité pour les risques de fraudes éventuellement, mais également pour la destruction des données et donc l'intégrité du système.

39 utilisateurs disposant du profil SAP_ALL :



39 users disposent de SAP_ALL,
29 sur les 39 sont des users interactifs (29 dialogues),
16 sur les 29 sont actifs (date de fin encore valide et non bloqués).



Attention, 3 rôles Z_SAP_ALL* (probablement copie du profil SAP_ALL attribué à 54 utilisateurs)

Attribution SAP_ALL et copies à maîtriser

Secureway

Gestion des utilisateurs inactifs

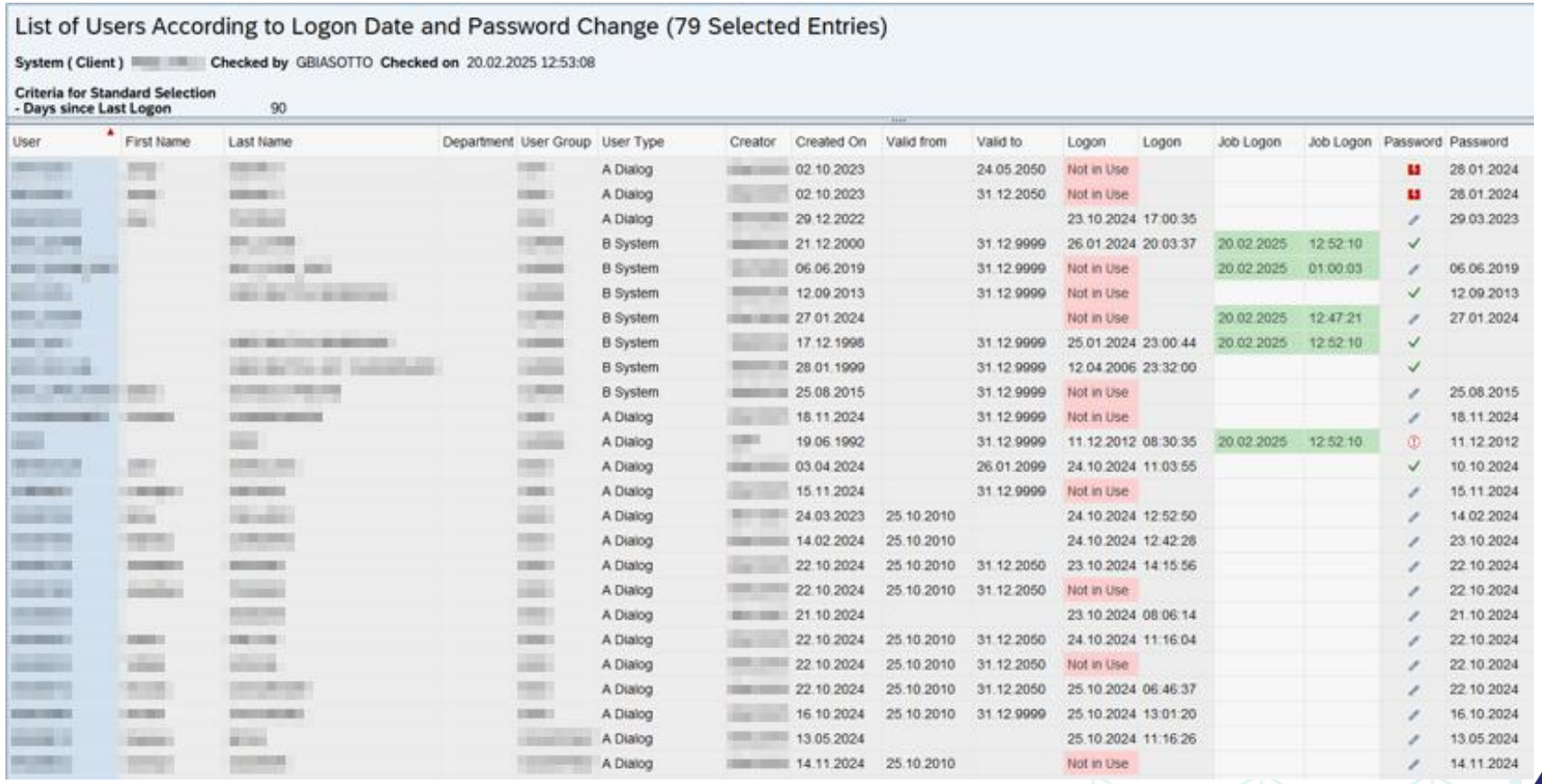
En date du 20/02/2025, le système de production compte 1516 utilisateurs valides dont 79 qui ne sont pas actifs ou qui ne se sont pas connectés depuis plus de 3 mois.

Parmi ces 79 utilisateurs, 65 sont de type dialogue ou service et devraient sans doute être archivés (sauf SAP*, DDIC, …)

Concernant les utilisateurs inactifs avec une date de fin dans le passé, les rôles sont restés attribués, ce qui représente un volume important de risques potentiels en cas de copie ou de réactivation.

Il conviendrait de finir de les archiver via la procédure suivante (ceci permet de mieux maitriser les coûts de licence et de réduire considérablement le nombre de risques SOD):

- ✓ Apposer une date de fin de validité
- ✓ Bloquer l'utilisateur
- ✓ Supprimer les rôles et profiles de la fiche utilisateur SAP
- ✓ Renseigner le groupe « Archive »
- ✓ Supprimer le code licence SAP



List of Users According to Logon Date and Password Change (79 Selected Entries)

System (Client) [redacted] Checked by GBIASOTTO Checked on 20.02.2025 12:53:08

Criteria for Standard Selection
- Days since Last Logon 90

User	First Name	Last Name	Department	User Group	User Type	Creator	Created On	Valid from	Valid to	Logon	Logon	Job Logon	Job Logon	Password	Password
[redacted]					A Dialog		02.10.2023		24.05.2050	Not in Use					26.01.2024
[redacted]					A Dialog		02.10.2023		31.12.2050	Not in Use					26.01.2024
[redacted]					A Dialog		29.12.2022			23.10.2024	17:00:35				29.03.2023
[redacted]					B System		21.12.2000		31.12.9999	26.01.2024	20:03:37	20.02.2025	12:52:10	✓	
[redacted]					B System		06.06.2019		31.12.9999	Not in Use		20.02.2025	01:00:03		06.06.2019
[redacted]					B System		12.09.2013		31.12.9999	Not in Use				✓	12.09.2013
[redacted]					B System		27.01.2024			Not in Use		20.02.2025	12:47:21		27.01.2024
[redacted]					B System		17.12.1998		31.12.9999	25.01.2024	23:00:44	20.02.2025	12:52:10	✓	
[redacted]					B System		28.01.1999		31.12.9999	12.04.2006	23:32:00			✓	
[redacted]					B System		25.08.2015		31.12.9999	Not in Use					25.08.2015
[redacted]					A Dialog		18.11.2024		31.12.9999	Not in Use					18.11.2024
[redacted]					A Dialog		19.06.1992		31.12.9999	11.12.2012	08:30:35	20.02.2025	12:52:10	ⓘ	11.12.2012
[redacted]					A Dialog		03.04.2024		26.01.2099	24.10.2024	11:03:55			✓	10.10.2024
[redacted]					A Dialog		15.11.2024		31.12.9999	Not in Use					15.11.2024
[redacted]					A Dialog		24.03.2023	25.10.2010		24.10.2024	12:52:50				14.02.2024
[redacted]					A Dialog		14.02.2024	25.10.2010		24.10.2024	12:42:26				23.10.2024
[redacted]					A Dialog		22.10.2024	25.10.2010	31.12.2050	23.10.2024	14:15:56				22.10.2024
[redacted]					A Dialog		22.10.2024	25.10.2010	31.12.2050	Not in Use					22.10.2024
[redacted]					A Dialog		21.10.2024			23.10.2024	08:06:14				21.10.2024
[redacted]					A Dialog		22.10.2024	25.10.2010	31.12.2050	24.10.2024	11:16:04				22.10.2024
[redacted]					A Dialog		22.10.2024	25.10.2010	31.12.2050	Not in Use					22.10.2024
[redacted]					A Dialog		22.10.2024	25.10.2010	31.12.2050	25.10.2024	06:46:37				22.10.2024
[redacted]					A Dialog		16.10.2024	25.10.2010	31.12.9999	25.10.2024	13:01:20				16.10.2024
[redacted]					A Dialog		13.05.2024			25.10.2024	11:16:26				13.05.2024
[redacted]					A Dialog		14.11.2024	25.10.2010		Not in Use					14.11.2024

Gestion de l'archivage des utilisateur à mettre en place

Secureway

Gestion des utilisateurs

Le processus de gestion des utilisateurs est défini de la façon suivante :

1. Demande formulée par ticket (GLPI) qui arrive au Helpdesk
2. Contrôle de la demande par le Pôle applicatif
3. Transfert à l'équipe qui va gérer l'utilisateur par copie vers le pôle Admin
4. Certains rôles sensibles peuvent être retirés lors du traitement de la demande
5. Les attributions se font en référence à un utilisateur existant

D'après nos échanges, il n'y a pas de processus automatisé de gestion des utilisateurs.

Les bonnes pratiques recommandées consistent à ce que toute demande contienne explicitement les droits à attribuer à l'utilisateur et qu'elle soit approuvée par les personnes responsables (si possible ayant connaissance des risques induits par la demande).

Il serait profitable d'automatiser ce processus afin de s'assurer que toutes les demandes soient effectivement validées et que la traçabilité soit optimale.

De plus, la gestion automatisée des utilisateurs SAP permettrait de soulager les administrateurs de ces tâches chronophages et de sécuriser le circuit avec la possibilité de coupler ce fonctionnement avec des analyses de risque préventives.

Traçabilité des demandes de gestion d'utilisateur

Gestion des utilisateurs

Nous avons identifié un grand nombre d'utilisateurs multiples pour la même personne.

Ce qui rend la maintenance difficile et la maitrise d'un point de vue sécurité pratiquement impossible.

En effet, les droits attribués pouvant être répartis sur 8 comptes SAP différents pour XXX, nous ne sommes pas en mesure d'identifier l'exhaustivité des risques qui lui sont accessibles via tous ses comptes.

Ceci pose également des problèmes de traçabilité, si des flux sont exécutés via des comptes SAP différents par la même personne.

Par ailleurs, 3 comptes de type « service » ont été identifiés, ce type de compte représente des risques en termes de connexion multiple et ne respectent pas les paramètres concernant les mots de passe :

User name	Full Name
[redacted]	bgRFC Supervisor Destination
[redacted]	service Système
[redacted]	stock et doc Consultation

Pour finir, 2 utilisateurs héritent des autorisations d'un utilisateur de « référence » en complément de leurs droits directs.

Nombre de User SAP	Actifs		
Nom complet	No	Yes	Total général
[redacted]		8	8
[redacted]		7	7
[redacted]	1	7	8
[redacted]		7	7
[redacted]		7	7
[redacted]	1	4	5
[redacted]		3	3
[redacted]		3	3
[redacted]		3	3
[redacted]	4	3	7
[redacted]	5	3	8
[redacted]		3	3
[redacted]		3	3
[redacted]	5	3	8
[redacted]	4	3	7
[redacted]	5	2	7
[redacted]	1	2	3
[redacted]	2	2	4
[redacted]		2	2
[redacted]	1	2	3
[redacted]	2	2	4
[redacted]		2	2
[redacted]	5	2	7
[redacted]	5	2	7
[redacted]	1	1	2
[redacted]	1	1	2

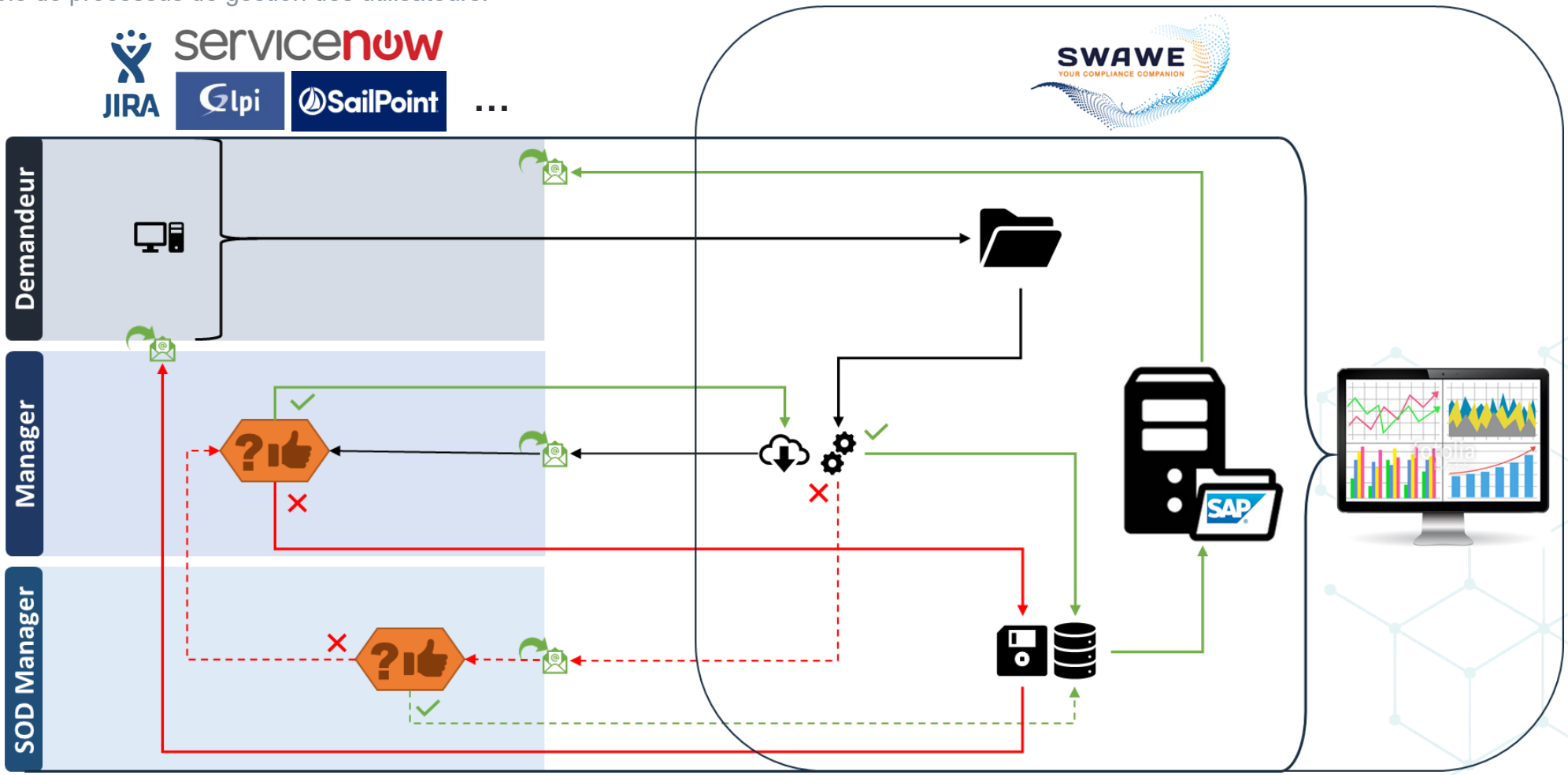
⛔ **Comptes SAP multiples pour un grand nombre d'utilisateurs**

⚠ **S'assurer que la maitrise du concept d'utilisateur de référence est assurée**

Secureway

Gestion des utilisateurs

Exemple de processus de gestion des utilisateurs:



Secureway

Gestion des autorisations

135 rôles standards commençant par "SAP" attribués à 56 utilisateurs :

Il n'est pas recommandé d'utiliser directement les rôles standards SAP, lorsque l'on souhaite s'en inspirer, il est préférable de les copier. (Une montée de version SAP écrase les modifications apportées)

La personnalisation du fonctionnement du générateur de profile semble avoir été géré, la transaction SU24 contient des valeurs client pour les transactions spécifiques et les tables ont été mise à jour lors de l'upgrade de 2024, ce qui représente une aide précieuse :

⇒ Lorsqu'un administrateur de rôles ajoute une transaction spécifique dans le menu d'un rôle, alors si la SU24 est bien paramétrée, les objets d'autorisations liés à cette transaction remontent automatiquement valorisés.

253 rôles ont l'objet « S_TCODE » est inséré manuellement, est-ce une volonté ?

⇒ Ceci pourrait se justifier s'il y a un souhait de donner des accès sans pour autant que la transaction apparaisse dans le menu de l'utilisateur (ou dans le cas de transactions qui font appel à d'autres transactions).

Mais attention, ce mode de gestion peut engendrer une charge de maintenance plus élevée étant donné que l'on ne bénéficie plus du fonctionnement standard de la transaction PFCG (avec les propositions d'objets et de valeurs).

Secureway

Gestion des autorisations

Seuls 3 rôles typés « IT » ont l'objet S_SERVICE valorisé avec « * » ce qui correspond parfaitement aux bonnes pratiques.

Tuiles FIORI insérées manuellement dans les rôles (S_SERVICE)

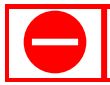
242 rôles apparaissent en erreur en termes de synchronisation des autorisations de profils liés à des relations Maîtres / Dérivés incohérentes ou des versions de profils non générées.

Ce qui entraine généralement des dysfonctionnements et anomalies pour les utilisateurs, mais surtout des difficultés pour maintenir les rôles au quotidien.

Le gestion des autorisations n'est pas homogène / cohérente

126 rôles dont la description indique que ce sont des rôles d'affichage contiennent pourtant des valeurs d'activité permettant d'effectuer des créations, modifications.

=> Notamment sur des objets donnant accès à des données sensibles comme les partenaires (fournisseurs, clients,…) ou encore des documents comptables, documents d'achats, de ventes,…



Les différents dysfonctionnements identifiés rendent la maintenance difficile et représentent des risques

Secureway

Gestion des autorisations

Le principe de dérivation n'est actuellement pas systématiquement utilisé, il conviendra de définir si la séparation d'un point de vue organisationnel est une nécessité.

993 rôles contiennent des données organisationnelles « forcées », ce qui engendre une perte de cohérence au niveau de la relation Maître-Dérivé.

⇒ Le système de dérivation dans SAP permet de créer un rôle maître ou modèle ne contenant que les données fonctionnelles (Types de documents, types de pièces, groupes de comptes) et aucune donnée organisationnelle.

Ensuite, des rôles dérivés sont créés à partir du rôle maître, reprenant ainsi automatiquement les données fonctionnelles du maître, en les complétant par les données organisationnelles des différentes entités. (Un rôle dérivé par découpage organisationnel).

⚠ **La mise en œuvre du principe de dérivation des rôles permettrait de faciliter la gestion des autorisations**

Secureway

Gestion des autorisations

La convention de nommage des rôles pourrait être améliorée : Ce qui permettrait aux utilisateurs / responsables de domaines de mieux s'approprier les rôles pour formuler leurs demandes.

Les rôles devraient commencer par Z ou Y, nous disposons de 30 caractères pour le nom des rôles, voici un exemple de convention de nommage plus explicite :

Exemple de convention de nommage des rôles

NB Caractères	Rôle maitre	Type	Affichage / Gestion		Module	Processus	Description
18	ZM:G:FI_CF_DOWNPAY	ZM:	G:		FI	CF	DOWNPAY
	Rôle simple	**Type**	**Affichage / Gestion**	**Niveau Orga.**	**Module**	**Processus**	**Description**
28	ZS:A:XXXX_SD_ADV_CDES_VENTES	ZS:	A:	XXXX	SD	ADV	CDES_VENTES
	Rôle composite	**Type**	**Affichage / Gestion**	**Niveau Orga.**	**Module**	**Processus**	**Description**
28	ZC:A:XXXX_SD_ADV_CDES_VENTES	ZC:	A:	XXXX	SD	ADV	CDES_VENTES

Type	Description
ZM	Rôle Maitre
ZS	Rôle simple
ZC	Role composite

Niveau Orga.	Description
XXXX	à déterminer

Module	Description
CO	Contrôle de gestion
FI	Finance
RH	Ressources Humaines

Processus	Description
CF	Comptabilité Fournisseur
CC	Comptabilité Client
BK	Banque
CL	Classes
MRP	Material Requirement Planning
ADV	Administration des ventes
ACH	Achats
LIV	Livraisons
PA	Profitability Analysis
PC	Product Costing

Secureway

Synthèse – Gestion des risques

Périmètre	Contrôle	Résultats	Risque potentiel	Exposition	Criticité	Recommandation
Gestion des risques (SOD et Critiques)	SOD Rôles	L'analyse montre que 121 rôles présentent des conflits SOD : 71 rôles conflictuels sur 1105 assignés à des utilisateurs.	Risque d'erreur, de fraude ou de détournement de fonds ou de marchandise			Procéder à la suppression de tous les profils des rôles non-utilisés et séparer les activités conflictuelles au sein des rôles à risques
Gestion des risques (SOD et Critiques)	SOD Users	12 723 risques SOD détectés pour l'ensemble des utilisateurs du système [redacted] En ne considérant que les utilisateurs actifs, ce nombre atteint 7 400 risques, répartis sur 635 utilisateurs sur les 684 actifs. 35 utilisateurs représentent 1/3 des risques détectés (via SAP_ALL ou équivalent).	Risque d'erreur, de fraude ou de détournement de fonds ou de marchandise			Il serait souhaitable de mener un projet de remédiation visant à réduire au maximum le nombre de risques SOD et d'appliquer des contrôles compensatoires sur les risques résiduels
Gestion des risques (SOD et Critiques)	Risques critiques [redacted]	1990 violations ont ainsi été détectées pour l'ensemble des utilisateurs du système [redacted] durant l'analyse réalisée le 28/08/2025. 85 risques spécifiques [redacted] identifiés concentrés sur 19 rôles individuels dont 13 sont assignés aux utilisateurs.	Risque d'erreur, de fraude ou de détournement de fonds ou de marchandise			
Gestion des risques (SOD et Critiques)	Matrice de risques critiques et SOD	La matrice de risques SOD a été initialisée lors du démarrage de ce diagnostic	La matrice de risque représente le référenciel des contrôles que [redacted] souhaite superviser, sans matrice, il n'est pas possible dévaluer le niveau de sécurité, ni l'évolution des risques dans le temps			Il convient de prévoir des revues périodiques de la matrice qui devrait être maintenue régulièrement pour suivre les évolutions de vos processus SAP

Secureway

Synthèse – Contrôles Généraux IT

Périmètre	Contrôle	Résultats	Risque potentiel	Exposition	Criticité	Recommandation
ITGC	Sécurité des utilisateurs standards SAP	Tous les utilisateurs standards SAP sont sécurisés dans les mandants 000 et 010 du système XXX	N/A	✓	●	N/A
ITGC	Paramètres de sécurité SAP	Les paramètres de sécurité ci-dessous sont convenablement gérés	N/A	✓	●	Renforcer en imposant un caractère spécial via le paramètre : Login/min_password_special
ITGC	Attribution du profil SAP_ALL	26 utilisateurs disposant du profil SAP_ALL Attention, 3 rôles ZSAP_ALL_XXX (probablement des copies du profil SAP_ALL attribués à 10 utilisateurs)	Risque d'erreur, de fraude ou de détournement de fonds ou de marchandise Risque d'altération, de destruction du système ou des données	✗	●	Limiter strictement l'utilisation du profil SAP_ALL ou rôles équivalents et mettre en œuvre un processus de gestion des comptes à privilèges
ITGC	Archivage des utilisateurs sortants	Le système de production compte 17 utilisateurs valides qui ne sont pas actifs ou qui ne se sont pas connectés depuis plus de 3 mois. Parmi ces 17 utilisateurs, 3 sont de type Dialogue et 2 de type Service et devraient sans doute être archivés (sauf SAP*, DDIC, ...)	Risque d'utilisation par une tierce personne et augmentation des coûts de licence	✓	●	Globalement, les comptes SAP sont désactivés dans un délai raisonnable, il serait tout de même pertinent de renforcer le processus d'archivage en effectuant les actions suivantes : - Apposer une date de fin de validité - Bloquer l'utilisateur - Supprimer les rôles et profiles de la fiche utilisateur SAP - Renseigner le groupe «INACTIF» - Supprimer le code licence SAP

Secureway

Synthèse – Gestion des utilisateurs

Périmètre	Contrôle	Résultats	Risque potentiel	Exposition	Criticité	Recommandation
Gestion des utilisateurs	Gestion des utilisateurs SAP	Le processus de gestion des utilisateurs est défini de la façon suivante : Demande formulée par ticket (GLPI) Traitement par les différentes équipes en charge de la gestion des utilisateurs (manque de coordination et de gouvernance) Transfert à l'équipe qui va gérer l'utilisateur par copie Les attributions se font en référence à un utilisateur existant D'après nos échanges, il n'y a pas de processus automatisé de gestion des utilisateurs (à part pour BI qui a un automate « maison » depuis un fichier MS Excel).	Les bonnes pratiques recommandées consistent à ce que toute demande contienne explicitement les droits à attribuer à l'utilisateur et qu'elle soit approuvée par les personnes responsables (si possible ayant connaissance des risques induits par la demande).			Il serait profitable d'automatiser ce processus afin de s'assurer que toutes les demandes soient effectivement validées et que la traçabilité soit optimale. De plus, la gestion automatisée des utilisateurs SAP permettrait de soulager les administrateurs de ces tâches chronophages et de sécuriser le circuit avec la possibilité de coupler ce fonctionnement avec des analyses de risque préventives. Ce sujet est adressé dans le cadre du déploiement de l'IAM XXX) en cours : Il convient de s'assurer auprès de l'éditeur et de l'intégrateur des capacités de la solution pour provisionner l'application SAP dans le respect des bonnes pratiques d'attribution, de validation et de traçabilité.
Gestion des utilisateurs	Utilisateurs multiples	Nous avons identifié un grand nombre (73) d'utilisateurs multiples pour la même personne. Par ailleurs, 4 comptes de type « service » ont été identifiés, ce type de compte représente des risques en termes de connexion multiple et ne respectent pas les paramètres concernant les mots de passe	Risque de perte de maitrise des droits attribués et augmentation du risque de fraude avec des difficultés de traçabilité			Limiter à un compte SAP par utilisateur, même en cas de besoins ponctuels, d'autres solutions existent pour étendre les autorisations temporairement de manière sécuritaire
Gestion des utilisateurs	Utilisateurs génériques	Nous avons constaté un nombre élevé d'utilisateurs génériques > 400 sur les 655 utilisateurs de dialogue actifs. La recommandation de SAP et des auditeurs est de ne pas utiliser de comptes génériques.	Pour la gestion des licences, pour assurer une bonne traçabilité dans les documents SAP. Mais également pour des raisons de gouvernance de gestion des utilisateurs, de leur sécurité, de la fréquence de changement du mot de passe, l'éventuelle mise en place du SSO Et enfin pour le déploiement de l'IAM => Faire le mapping des identités et des utilisateurs SAP devient plus compliqué, donc, gérer les demandes d'accès, identifier le responsable en charge de la validation, etc…			Privilégier l'utilisation de comptes nominatifs, la mise en œuvre d'une solution d'automatisation de la gestion du cycle de vie des utilisateurs permettrait de résoudre durablement ce besoin de flexibilité et permettrait d'améliorer l'expérience utilisateur et leur satisfaction. Tout en garantissant le respect du processus de gestion des utilisateurs et de leur attribution de droits, leur traçabilité et votre capacité à le prouver auprès des CAC / auditeurs.

Synthèse – Gestion des autorisations

Périmètre	Contrôle	Résultats	Risque potentiel	Exposition	Criticité	Recommandation
Gestion des autorisations	Conception des Rôles	Convention de nommage des rôles existante Décorrélation des rôles "fonctionnels" et de leurs données organisationnelles Désynchronisation des rôles Maitres / dérivés 27 en erreur	Difficulté de maintenance pour les administrateurs et d'appropriation par le business Défault potentiel de fiabilité de maintenance des données organisationnelles dans les rôles (société, division, magasin,...)	✓	●	Globalement, la maitrise du concept d'autorisation est bonne, il conviendrait éventuellement de revoir certains rôles pour rétablir leur fonctionnement standard pour en faciliter la maintenance et garantir la fiabilité. Action impérative à mener, => S'assurer qu'aucun rôle individuel ne contienne de risque (actuellement => 71 rôles concernés, dont 54 assignés)
Gestion des autorisations	Utilisation des rôles standards SAP	1603 rôles standards SAP sont générés dans XXX 36 rôles standards SAP représentent 241 risques Seuls 2 rôles SAP* sont assignés à 1 utilisateur de type System qui dispose par ailleurs du profile SAP_ALL	Risque de dégradation car les rôles standards peuvent être écrasés lors des montées de version, il est recommandé de ne jamais les utiliser. Risque potentiel d'attribution de ces rôles qui génèrent des risques.	!	●	Supprimer tous les profils des 1603 rôles standards SAP générés
Gestion des autorisations	Personnalisation SU24	La personnalisation du fonctionnement du générateur de profile ne semble pas avoir été géré intégralement, seules deux transactions spécifiques ont été personnalisées.	N/A	✓	●	Il n'y a pas réellement de risque, cette personnalisation représente plutôt une aide quotidienne à la gestion des rôles dans SAP, il est donc recommandé de l'utiliser
Gestion des autorisations	Transactions forcées	148 rôles ont l'objet « S_TCODE » est inséré manuellement	1 - Difficultés à garder la maitrise des transactions attribuées 2 - Défault de fiabilisation de la gestion des rôles et perte du bénéfice des automatismes proposés par SAP	!	●	Si ces ajouts manuels ne sont pas volontaires ou maitrisés : Rétablir le fonctionnement standard SAP en insérant les transactions dans le menu et en gérant les objets
Gestion des autorisations	Données Organisationnelles forcées	217 rôles contiennent des données organisationnelles « forcées », ce qui engendre une perte de cohérence au niveau de la relation Maître-Dérivé.	Défault potentiel de fiabilité de maintenance des données organisationnelles dans les rôles (société, division, magasin,...)	✗	●	Restaurer dans les 217 rôles concernés l'utilisation standard des données organisationnelles
Gestion des autorisations	Rôles générés en production	804 Profiles semblent avoir directement été générés en production	Rôles potentiellement créés directement dans ECC prod sans respecter les meilleures pratiques du circuit DEV => QUAL => PROD et sans validation. Risque d'anomalie si un rôle est transféré et que les données de production sont écrasées.	✗	●	Revenir au comportement standard de gestion des rôles et transférer les rôles depuis le système de développement avec les « profils générés par le développement » par transport.
Gestion des autorisations	Rôles d'affichage contenant des activités de gestion	30 rôles dont la description indique que ce sont des rôles d'affichage contiennent pourtant des valeurs d'activité permettant d'effectuer des créations, modifications. => Notamment sur des objets donnant accès à des données sensibles comme les partenaires (fournisseurs, clients,...) ou encore des documents comptables, documents d'achats, de ventes,...	Risque d'ouverture de droits non maitrisés sur des processus sensibles (Finance, Achat, Vente, Données de base client & fournisseur)	✗	●	Corriger les rôles d'affichage contenant des activités de gestion

Conclusion

Analyse des risques :

Le premier point important à corriger concerne l'attribution du profil SAP_ALL (ou Z_SAP_ALL) qui conviendrait de retirer à tous les utilisateurs et de ne réserver son utilisation que dans des cas d'urgence (avec une traçabilité de ces accès).

Pour pouvoir remplacer le profil SAP_ALL pour les utilisateurs (principalement la DSI), une refonte des droits de la DSI doit être réalisée. Un plan d'actions est proposé dans les diapositives qui suivent.

Au niveau métier, si l'objectif à terme est de maitriser les accès du point de vue SOD et d'accès aux données sensibles, il conviendrait de procéder à une refonte/revue de l'ensemble des rôles individuels et métier. Pour cette partie, vous trouverez aussi un plan d'actions dans les diapositives suivantes.

Les analyses de risque au niveau rôles montrent que le concept d'autorisation (y compris celui conçu pour S/4HANA) contient de nombreux conflits et nécessite la mise en œuvre de corrections pour limiter les conflits SOD à minima au niveau des rôles simples.

Cela induit un nombre de conflits très important au niveau utilisateurs, de part le grand nombre de droits très larges attribués massivement.

Un plan d'action rapide d'archivage des comptes, de suppression des SAP_ALL et de nettoyage des rôles inutilisés permettrait de réduire significativement le nombre de conflits.

Conclusion

Optimisations :

Nous avons détecté plusieurs axes d'optimisation concernant les autorisations, soit :

- ✓Finir d'archiver les utilisateurs inactifs (Date de fin dans le passé) en retirant les rôles qui sont encore assignés,
- ✓Archiver les utilisateurs qui ne sont plus actifs dans le système mais qui sont encore « valides »,
- ✓Ne plus utiliser les rôles standards SAP assignés pour en créer des spécifiques,
- ✓Pour les rôles dont la zone organisationnelle a été forcée, remettre en standard le lien dynamique avec la saisie des données organisationnelles,
- ✓Corriger tous les rôles défectueux,
- ✓Améliorer/automatiser le processus de gestion des utilisateurs.

La recommandation consiste à effectuer une refonte des rôles actuels pour les adapter, il n'est pas possible de respecter les principes de séparation des tâches avec des rôles individuels qui contiennent des conflits.

Les rôles contenant des catalogues FIORI semblent avoir été conçus de façon à répondre à des métiers entiers et ne respectent donc pas les principes de moindre accès.

Plan d'action proposé

Périmètre	Contrôle	Exposition au risque	Criticité	Charge estimée	Profil	Taux	Montant
Gestion des risques (SOD et Critiques)	SOD Rôles	!	●	5	SAP Senior consultant		
Gestion des risques (SOD et Critiques)	SOD Users	!	●	10	SAP Senior consultant		
Gestion des risques (SOD et Critiques)	Risques critiques	!	●	3	SAP Senior consultant		
Gestion des risques (SOD et Critiques)	Matrice de risques critiques et SOD	✓	●	1	SAP Senior consultant		
ITGC	Sécurité des utilisateurs standards SAP	✓	●	0	SAP Experienced consultant		
ITGC	Paramètres de sécurité SAP	✓	●	0	SAP Experienced consultant		
ITGC	Attribution du profil SAP_ALL	✗	●	5	SAP Experienced consultant		
ITGC	Archivage des utilisateurs sortants	✓	●	0,5	SAP Experienced consultant		
Gestion des utilisateurs	Gestion des utilisateurs SAP	!	●	5	SAP Senior consultant		
Gestion des utilisateurs	Utilisateurs multiples	✗	●	3	SAP Junior consultant		
Gestion des utilisateurs	Utilisateurs génériques	!	●	5	SAP Junior consultant		
Gestion des autorisations	Conception des Rôles	✓	●	10	SAP Experienced consultant		
Gestion des autorisations	Utilisation des rôles standards SAP	!	●	2	SAP Junior consultant		
Gestion des autorisations	Personnalisation SU24	✓	●	0	SAP Junior consultant		
Gestion des autorisations	Transactions forcées	!	●	5	SAP Junior consultant		
Gestion des autorisations	Données Organisationnelles forcées	✗	●	5	SAP Junior consultant		
Gestion des autorisations	Rôles générés en production	✗	●	3	SAP Junior consultant		
Gestion des autorisations	Rôles d'affichage contenant des activités de gestion	✗	●	5	SAP Experienced consultant		
TOTAL				67,5			

Secureway

Q & A

Questions et réponses

Secureway

Contacts

Grégory BIASOTTO
gbiasotto@secureway.fr
+33 6 66 63 03 02

SECUREWAY
8 Avenue de Paris
78000 Versailles

Secureway