



**Transformation S/4 HANA :
saisissez l'opportunité de renforcer
votre dispositif de Contrôle Interne !**

Webinaire

29 Février 2024

Avec vous aujourd'hui



Pauline Eckert
Associée
Risk Consulting



Guillaume Cuisset
Associé
Risk Consulting



Ozgur Brand
Head of Business System
Controls & Data Analytics



Toufik Benaissa
Senior Manager
Risk Consulting



Diane Richli
Senior Manager
Risk Consulting



Contents

01	Contexte	04
02	Les clés du 'Control by design'	09
03	Les enjeux de la gestion des accès	15
04	Vers la digitalisation des contrôles	24
05	Conclusion	29



01

Contexte

Contexte

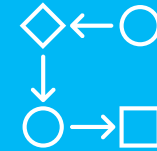
La migration vers SAP S/4HANA est au centre des préoccupations de nos clients déjà sous SAP. Ces projets diffèrent d'une entreprise à une autre. Ils mobilisent des ressources importantes et sont une opportunité de modernisation des processus métiers

2027

Année annoncée par l'éditeur SAP de la fin de maintenance de la version actuelle de l'ERP SAP ECC

>10M€

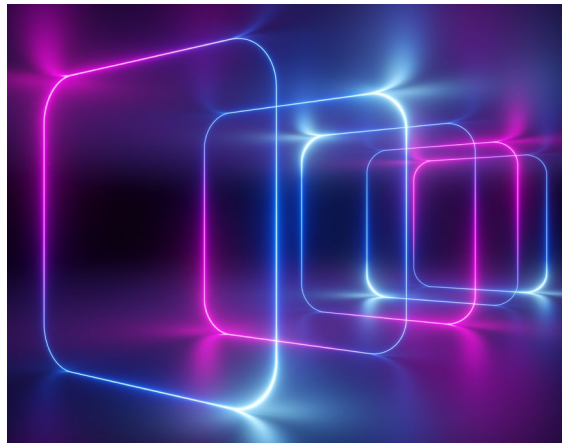
Des investissements consentis très conséquents



Ces projets peuvent être de simples migrations techniques (Brownfield), ou des projets de refontes des processus métiers (Greenfield)



L'architecture technique est également propre à chaque projet (SAP Rise, Cloud). Outils Satellites hors SAP S/4



Comment tirer tous les bénéfices attendus de ce type de projet ?

Le momentum pour sécuriser les processus

“Pourquoi embarquer le contrôle interne le plus tôt possible dans un projet de transition SAP S/4?”

01

Nécessité de faire évoluer les contrôles

02

Mobilisation de l'ensemble des fonctions métiers

03

Rationalisation des coûts projets

04

Une approche intégrée

05

Réponse aux enjeux de conformité et de sécurité

Les attentes sur le Contrôle Interne

Attentes récurrentes du contrôle interne



Déficiences récurrentes ou significative de contrôle



Multiplicité des fonctions assurances et conformité



Besoin d'efficience accru



Manque de prise en compte des enjeux de conformité et sécurité dans les projets



Une ambition de digitalisation parfois insatisfaite

Définir son business case

Il est important de définir les objectifs à atteindre en termes de Contrôle Interne afin de les intégrer au business case du projet SAP S/4.

KPMG Internal controls – Maturity Model

	Immature / Poor	Developing / Fair	Average / Standard	Mature / Good	Advanced / Excellent
Functional Process & controls	Disaggregated processes and absence of embedded controls. 1 ▼	Low degree of processes standardization and automation. Limited and disparate controls. 2	Common framework and processes but partially applied. Core controls are implemented. 3	Processes are harmonized and standardized. Controls are integrated into operational activities and monitored. 4	Processes are streamlined and optimized. Technology enables automated controls fully integrated. 5
Adoption & Culture	No sponsorship and absence of training. 1	Limited engagement of specific team. Weak culture of risk management. 2	Top management and specific teams engaged. Ad-hoc trainings. 3	Culture shared by top management and dedicated training implemented. 4 ▼	Shared vision and ownership of all lines of defense. Strong culture of risk management. 5
Organization & Governance	Undefined 3 lines of defense and governance. 1	Limited coordination between 3 lines of defense and governance. 2	Basic Coordination between lines of defense and governance. 3 ▼	Fully integrated 3 lines of defense and governance established. 4	Fully integrated 3 lines of defense leveraging on SSCs and CoEs and clear governance. 5
Technology & Reporting	No specific systems or tools to perform and monitor controls. No reporting. 1	Disparate systems and tools depending on processes and entities. Disparate reporting. 2	Standardized systems and tools covering core controls & monitoring. Basic reporting. 3	Advanced technologies for controls automation, monitoring and follow-up. Advanced dashboard. 4 ▼	Fully integrated systems and reporting tools across the organization and the 3 lines of defense. Continuous Control Monitoring. 5
Control testing	No testing strategy and coverage. 1	Disparate or limited testing strategy and coverage. 2	Basic Testing standards not risk oriented. 3	Standard and risk-based Testing approach. 4	Harmonized and automated testing 5 ▼

L'approche « S/4 in Control »



Sécuriser le dispositif projet

Sécurisation du programme de transformation S/4



Compliance & Control by Design



Gouvernance & migration des données



Maitrise des risques Cyber Sécurité & Data Privacy



Adapter, simplifier et digitaliser les lignes de maitrise des risques



Assistance à la transformation des processus avec le Process Mining



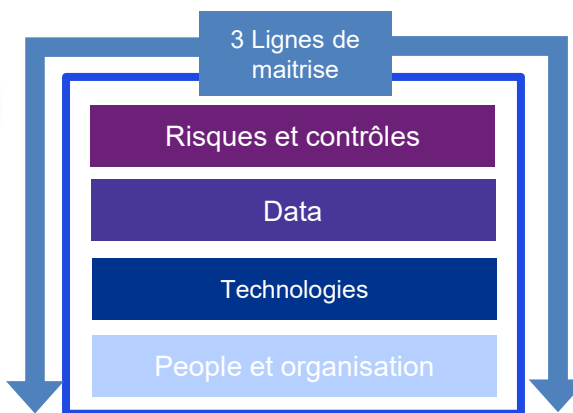
Gestion des accès & SoD en environnement S/4



Digitalisation de la maitrise des risques et du Contrôle Interne



Readiness des entités et déploiement du dispositif de maitrise





02

**Les clés du
« Control by design »**

Changements et risques liés aux processus



Les changements majeurs

Refonte du modèle de données

Expérience utilisateur intuitive

Evolution des flux métier

Solution connectée

Les nouveaux risques

Inefficacité des contrôles « Legacy »

Perte de qualité des données

Manque de maîtrise des accès aux données

Non prise en compte des outils satellites

Mauvaise appropriation de la solution



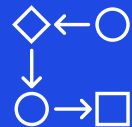
'Control by design' : les principes clés



**Au plus tôt et tout au long
de votre projet**



**S'appuyer sur des contrôles
embarqués**



**Intégrer les contrôles dans
les flux métiers**



**Privilégier la revue des
exceptions**



**Assurer l'adoption des
contrôles**

Quelques exemples de contrôles embarqués



Le **Journal Universel** réconcilie les mondes S/4 “by design”

Validation des écritures manuelles via la tuile Fiori « Verify General Journal Entries »

Workflow flexible pour la validation des commandes d’achat

Flux de validation des fiches « Business partner » dans MDM

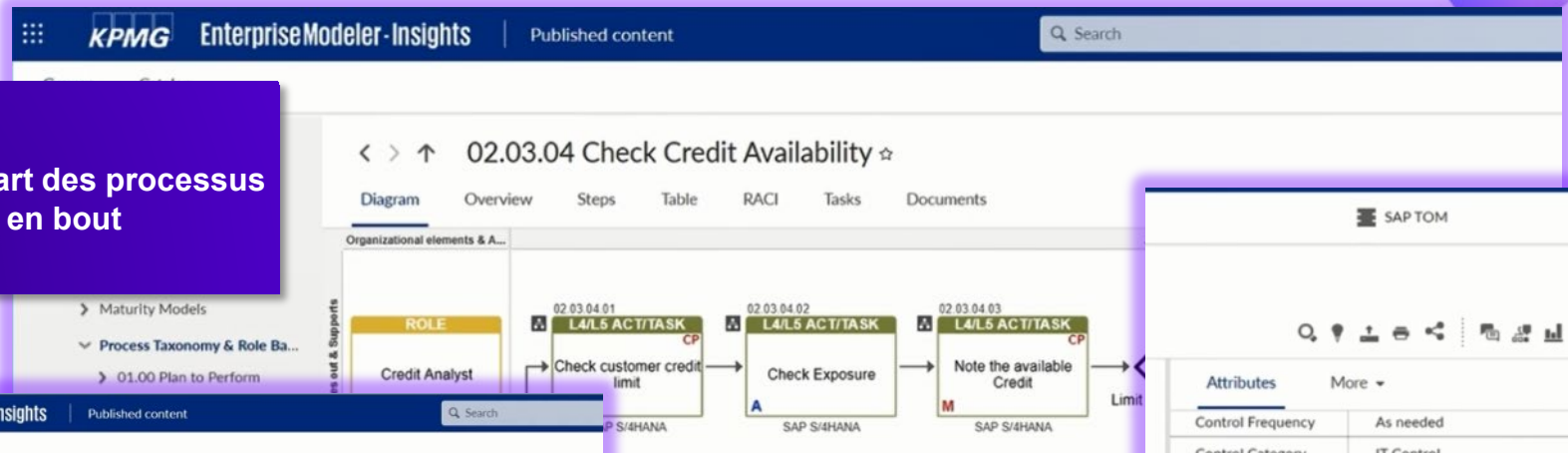
Des tuiles et rapports personnalisables pour réaliser certains contrôles



Powered Controls, l'accélérateur KPMG



 **Flowchart des processus de bout en bout**



 **Matrice de risques et de contrôles intégrés**


02.00 Quote to Cash - Controls Library

Control ID	Description
OTC.CON.001	Normal process is in place to review the customer master hierarchy.
OTC.CON.002	Access to maintain customer hierarchies is restricted to Demand MD Owner.
OTC.CON.003	Access to maintain customer master data is appropriately restricted.
OTC.CON.004	Access to mark customers for deletion and/or block/unlock customers is...
OTC.CON.005	Account receivable ledgers are reconciled and reviewed.
OTC.CON.006	Account receivable ledgers are reconciled and reviewed.
OTC.CON.007	Account receivable ledgers are reconciled and reviewed.
OTC.CON.008	Account receivable ledgers are reconciled and reviewed.
OTC.CON.009	Account receivable ledgers are reconciled and reviewed.
OTC.CON.010	Account receivable ledgers are reconciled and reviewed.
OTC.CON.011	Account receivable ledgers are reconciled and reviewed.
OTC.CON.012	Authorized release of sales orders.
OTC.CON.013	Automatic creation of invoices.
OTC.CON.014	Collections strategies are validated and approved in a timely basis.
OTC.CON.015	Credit Card and Wire Payment file upload.
OTC.CON.016	Cross-functional customer alignment meeting is conducted.
OTC.CON.017	Import/Upload of period transactions to identify errors.
OTC.CON.018	Incentive negotiations are performed as per policy.
OTC.CON.019	Interfaced sales data interfaced from other systems is complete and accurate...
OTC.CON.020	Invoice is Auto generated against shipping documents.
OTC.CON.021	Payment terms at transaction level is valid and accurate.
OTC.CON.022	Periodic Reconciliation between general ledger and AR sub...
OTC.CON.023	Periodic reconciliation between invoices and lease revenue.
OTC.CON.024	Periodic revenue and receivables variance analysis.
OTC.CON.025	Periodic review of customer order batch job.
OTC.CON.026	Record bad debt reserve journal entries in general ledger.
OTC.CON.027	Record payment receipts to sub-ledger and match to invoices.
OTC.CON.028	Report generation for statutory requirements as applicable.
OTC.CON.029	Returned goods are reviewed and authorized by appropriate...
OTC.CON.030	Revenue mapping is accurately configured in the system.
OTC.CON.031	Review and approval of forward looking aging reports.
OTC.CON.032	Review and approval of late payment penalties calculation.
OTC.CON.033	Review and approval of sales forecasts.
OTC.CON.034	Review and approval of Sales Order / Backorder / Stock Reserves.
OTC.CON.035	Review and resolution of errors identified in reconciliation and recording of...

SAP TOM

Attributes More

Control Frequency	As needed
Control Category	IT Control
Associated KRIs (Key Risk Indicator)	N/A
Platform Specific Configuration	<p>SAP is configured to automatically perform credit checks for all Service orders except for donations, returns, credit memo and debit memo request prior to processing. 1.) Extract the list of applicable sales order types and delivery types in the system 2.) Use transaction OVAK to determine the type of credit checks performed for the corresponding sales document types in order processing. 3.) Use transaction OVA7 to determine whether a credit check is performed for item categories being used. 4.) Use transaction OVAD to display the credit groups that have been assigned to the delivery types being used. 5.) Use transaction OVA8 to display overview of defined credit checks for credit control areas. 6.) Determine that these are configured as per the business requirements and company policy.</p> <p>QTC.CON.084</p> <p>SAP is configured to automatically perform credit checks for all Service orders except for donations, returns, credit memo and debit memo request prior to processing.</p>

 **Détail de la configuration des contrôles automatiques**





L'adoption des contrôles : un enjeu majeur



03

Les enjeux de la gestion des accès

Comment adresser les enjeux autour de la SoD et la gestion des accès dans un programme S/4



Une nouvelle solution suppose...

- | Nouvelles fonctionnalités, processus, risques et contrôles à considérer
- | Nouvelles transactions et méthodes d'accès au système (Fiori) à sécuriser : une revue des business roles, des autorisations et de la matrice SOD est nécessaire pour refléter les changements apportés par S/4



Le Momentum

- | La gestion des accès utilisateur doit être alignée au design des processus et l'organisation cible
- | Une approche "Start Clean" est à intégrer dès les prémisses du projet:
 - | Pour éviter les efforts fastidieux d'adaptation des rôles et de résolution des conflits post le go-live : en tirant parti de SAP GRC Access Control pour réduire les coûts, améliorer l'expérience utilisateur, renforcer la sécurité et faciliter la migration vers SAP S/4HANA.
 - | Pour être conforme dès le 1er jour du go-live

SoD et gestion des accès : les points clés



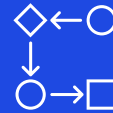
01

Définir et documenter une matrice SoD avec des processus cibles, incluant FIORI et les nouvelles fonctionnalités de S/4 Hana



02

Faire adopter les enjeux de la SoD et **améliorer** la compréhension des métiers sur le contenu du catalogue des business rôles



03

Définir ou Adapter vos rôles SAP en fonction de l'évolution des business process et des nouveautés apportées par S/4



04

Former et faire tester aux futurs end-users leur accès cibles remédiés durant les phases de trainings et d'UAT



05

Lancer des analyses SoD à chaque étape clé du processus de design et d'implémentation des rôles, et définir des dashboards pour monitorer les KPIs SoD

Capitaliser sur Fiori pour démocratiser les notions d'autorisations



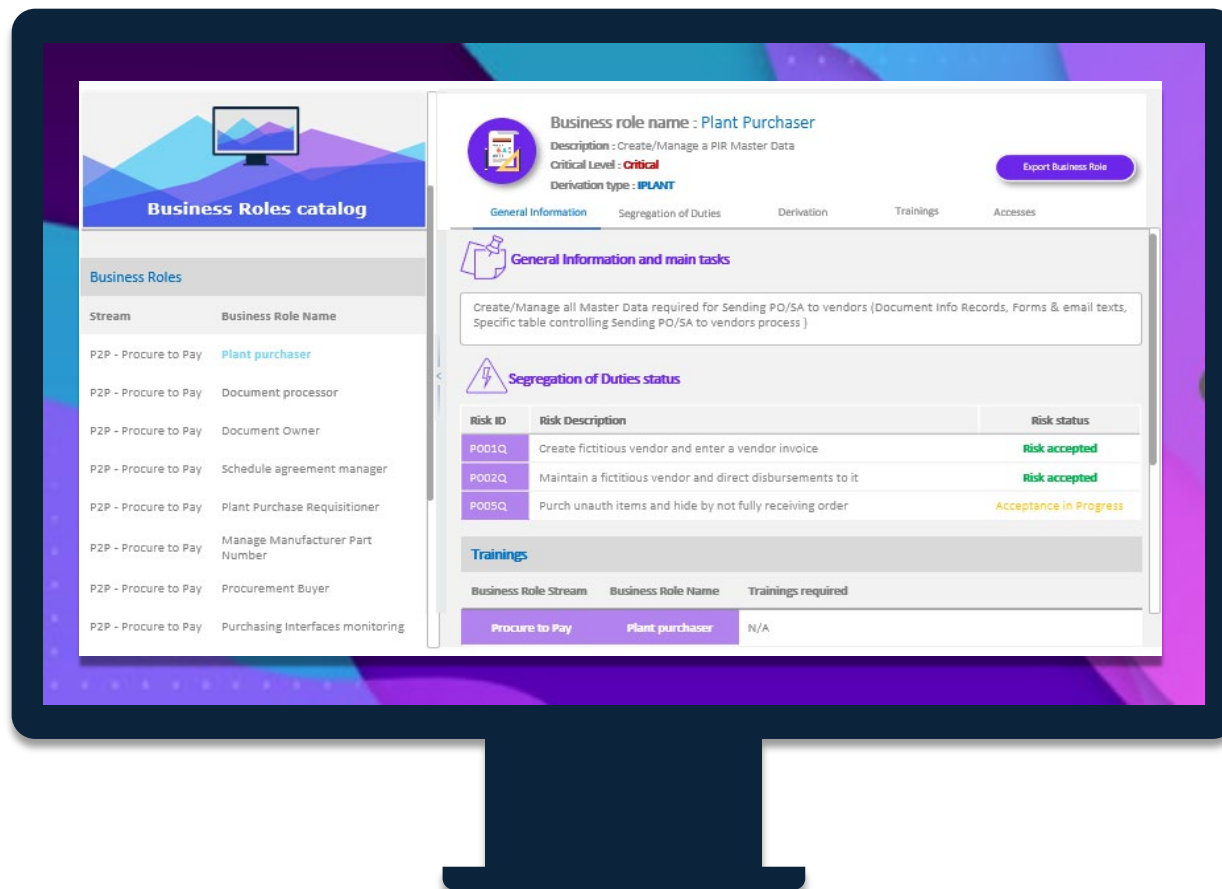
Améliorer la compréhension du business autour de la gestion des accès utilisateur est un facteur clé de succès dans un programme S/4.

1

Évitez les fichiers Excel pour gérer votre catalogue des accès

2

Créez des « Role cards » et des « Risk cards » incluant toutes les informations nécessaires à la compréhension des métiers



3

Profitez de la technologie Fiori pour digitaliser votre catalogue des accès et ainsi renforcer son appropriation par le business de manière user-friendly



Capitaliser sur Fiori pour faire adopter les enjeux de la SoD



Exemple de risk card

Risk : Open closed periods and inappropriately post entries - RF01
Risk Level : High

GENERAL INFORMATION IC BEST PRACTICES RISK DETAILS ADDITIONAL DOCUMENTATION

Fraud Patterns
It enables manipulation over financial statements, cut-off impact.
e.g : Open a period to hide activity in another period (bypassing controls).


IC Best Practices
Mitigating Controls :
Review log for Open/Close accounting period. If an exception is identified, review all entries performed during the re-opening

- Execute YA08 to identify and review entries in previous periods
- Review of posting after an official closing date (transaction s_alr_87012286)

Risk Details

Function ID	Function Description	Transactions
TF01	Open / Close accounting periods	> Function Transactions (5)
TF06	Book manual journal entries	> Function Transactions (77)

Additional Documentation
Document
No data

 Click on the functions to display the transactions that are included



REX SANOFI



Ozgur BRAND

*Head of Business System Controls & Data
Analytics*

The Sanofi logo, featuring the word 'sanofi' in a lowercase, bold, sans-serif font. The dot above the 'i' is a small blue circle. The logo is set against a circular background showing a sunset or sunrise over the ocean with rocks in the foreground.

sanofi

Le programme iShift

Périmètre du projet iShift



CONTEXTE

Le programme Shift de transformation du système financier a été lancé dans le but d'harmoniser les processus back-office dans toutes les entités du groupe au travers de l'implémentation de SAP S/4 HANA et d'outils satellites.

En 2018, Sanofi a décidé d'intégrer la gestion de la production au travers du nouvel ERP déployé pour supporter les processus back-office. Au travers de cette décision, Sanofi a souhaité créer un ERP intégré supportant l'ensemble de ses processus, ce nouveau système est appelé iShift

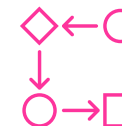
Dans le cadre de ce projet, un périmètre UAM dédié a été identifié afin de garantir l'application des meilleures pratiques et le respect des politiques SANOFI en matière de gestion des rôles métier et des utilisateurs.

Les 3 piliers de la gestion des utilisateurs



Définir un catalogue de rôles métier centralisé

Concevoir un catalogue de rôles métier partagé, sans conflits et unifié à travers les entités afin d'être aligné avec les processus métier cibles.



Assurer la correcte séparation des tâches

Identifier et remédier les risques SoD en utilisant la matrice Sanofi afin de garantir la conformité avec les politiques déployées



Anticiper et planifier la formation des utilisateurs

S'assurer de la bonne planification des formations en lien avec les accès utilisateurs afin de se conformer aux contraintes GxP

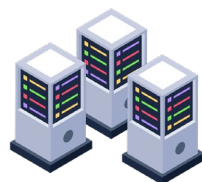
Outillage GRC



SAP GRC
Access Control
12.0

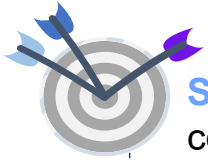


Utilisation des 4
modules de la
solution (ARA,
ARM, EAM, BRM)



82 systèmes
productifs
connectés (SAP &
nonSAP)

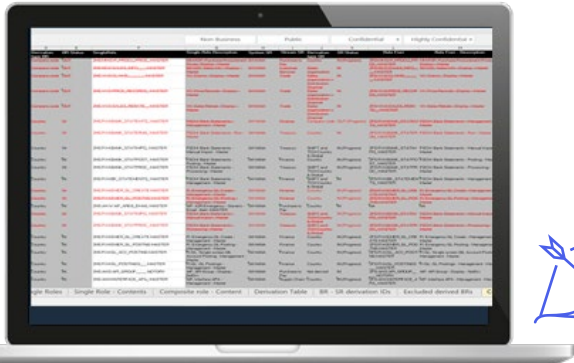
L'approche SOD & business roles



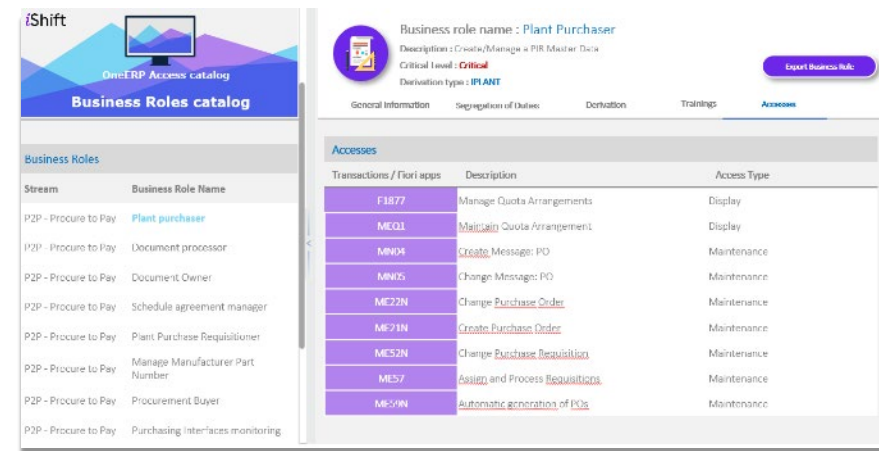
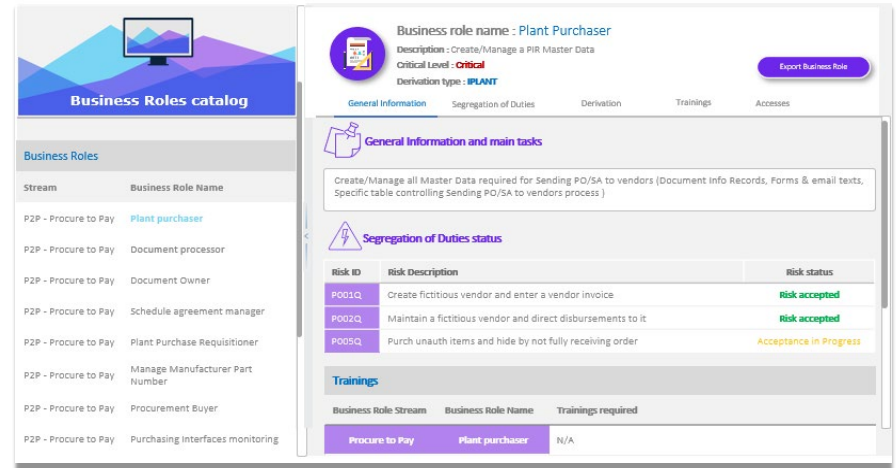
Sécuriser les déploiements IShift tout en **optimisant les efforts** des équipes projet et en facilitant la compréhension du business autour de la gestion des accès utilisateurs



Définition d'un catalogue des accès **centralisé** et **user-friendly** pour faciliter la compréhension du business autour des autorisations



Définition d'un catalogue de TOM positions **standardisées** pour **accélérer** les déploiements IShift en facilitant la phase de **users mapping**



Facteurs clés de succès



01

Définir un catalogue global de rôles métier SoD compliants à déployer et à appliquer dans l'ensemble des entités avec le minimum spécificités locales.

02

Adopter une approche par profil métier avec une documentation orientée business facile d'accès et de compréhension.

S'assurer que le catalogue de rôles est adopté par les toutes les parties prenantes.

04

Considérer le mapping des End-Users comme une activité critique ayant un impact sur le calendrier de formation et les résultats SoD. Anticiper les jalons et la charge de travail en conséquence.

Réaliser les UAT avec les rôles métier cibles et prendre en compte les principes SoD lors du traitement des anomalies.

03



Effectuer des simulations SoD du mapping des End-Users afin de remédier les conflits SoD avant la phase de "Cutover" et ainsi garantir un go-live SoD compliant

05

04

Accélérer sur la digitalisation des contrôles

Contexte



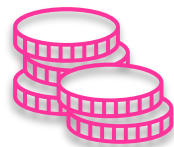
Dans le cœur de métier des entreprises, la digitalisation est déjà une réalité en place...



De manière paradoxale, les métiers du risque et de la conformité n'ont pas toujours pris le virage de la digitalisation avec la même vitesse.

Les initiatives de transformation S/4 HANA reposent souvent sur un business case riches et complexes associés à de fortes attentes métier.

Sécuriser la valeur attendue du programme par le métier du Contrôle Interne doit aussi être inscrit à l'agenda de ce business case :



Efficacité & coûts des contrôles

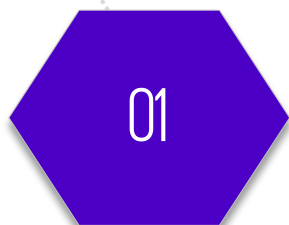


Evolution technologique des processus



Adoption des contrôles par les 3 lignes de Défense

Les bénéfices de la digitalisation



01

AUTOMATISATION



02

**CENTRALISATION
DE L'INFORMATION**



03

TEMPS REEL



04

EFFICACITE



05

TRAÇABILITE



06

FIABILITE



**Pour une meilleure intégration entre les
trois lignes de défense!**

Les enjeux de la digitalisation des contrôles



DEFINITION DU SCOPE



Cadrer

le scope en fonction de la maturité actuelle et cible de son Contrôle Interne : **quel périmètre de contrôles, quelles parties prenantes, quels bénéfices attendus?**



CHOIX DES OUTILS



Saisir

l'opportunité du programme S/4 pour intégrer dans l'écosystème du projet **le ou les bons outils satellites nécessaires** pour atteindre la cible



TRAJECTOIRE DE DEPLOIEMENT



S'aligner

avec la trajectoire du programme S/4 pour adopter une **démarche de déploiement itérative** de la digitalisation des contrôles en identifiant les priorités (Risques & ROI)



ADHESION UTILISATEURS



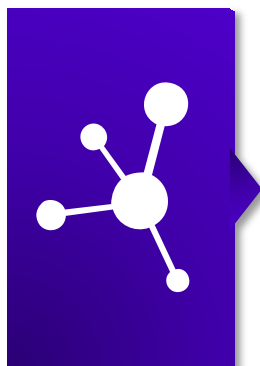
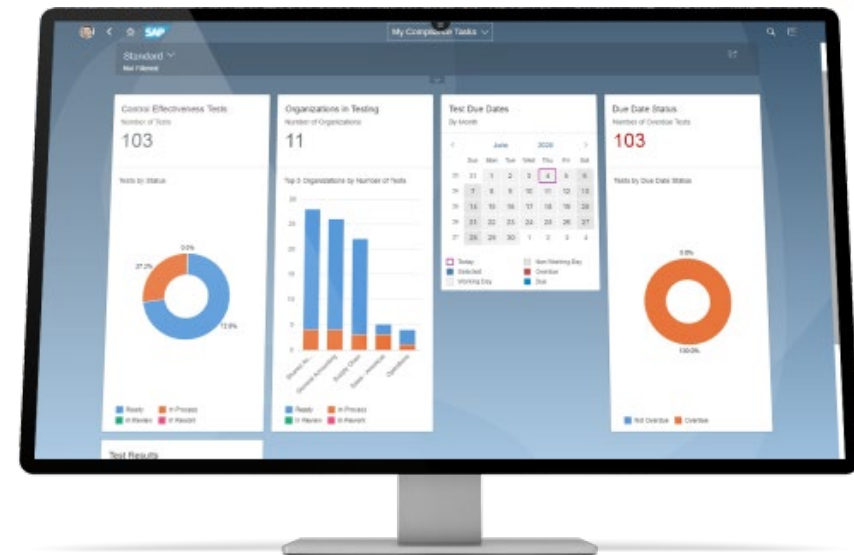
Anticiper

la **gouvernance** qui sous tendra l'utilisation de nouveaux outils et le plan de **formation & communication** associés

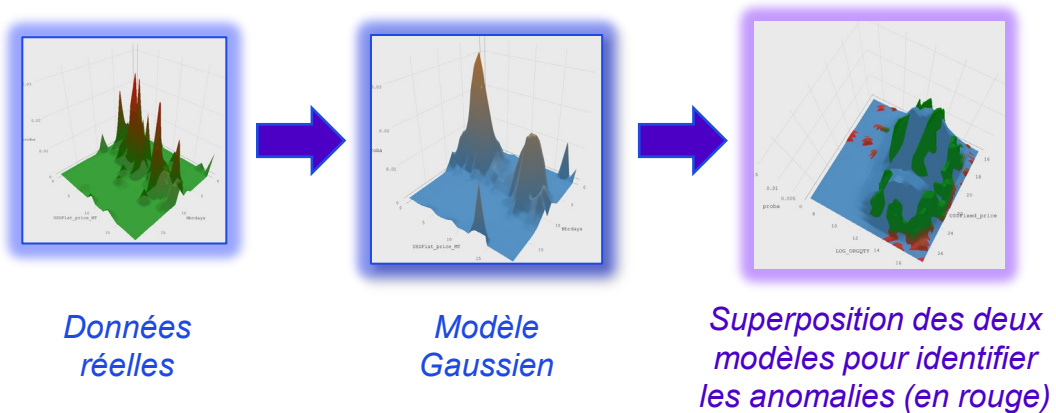
Possibilités offertes par la digitalisation



Approche déterministe basée sur les outils de Control Continuous Monitoring (CCM) du marché



Utilisation du Machine Learning pour compléter une approche « rule based »



05

Conclusion



Conclusion

Profitez du programme S/4 HANA pour renforcer votre dispositif de Contrôle Interne et pour le faire passer à l'ère du digital!

01

Challengez le niveau de maturité de votre Contrôle Interne et alignez la trajectoire d'évolution de vos contrôles avec celle du programme S/4

02

Adressez le Contrôle Interne comme un stream métier à part entière dans l'intégralité de votre programme S/4

03

Saisissez les opportunités offertes par les nouvelles technologies pour digitaliser les contrôles et moderniser la gestion des rôles et de la SOD

Q&A



Avez-vous des questions ?

Ecrivez sur le fil de discussion...



CONTACTS

Pauline Eckert

Associée
Digital Compliance
peckert@kpmg.fr

Guillaume Cuisset

Associé
Tech Risk
gcuisset@kpmg.fr

Toufik Benaissa

Senior Manager
Digital Compliance
tbenaisa@kpmg.fr

Diane Richli

Senior Manager
Tech Risk
drichli@kpmg.fr