KPMG

KPMG France - Digital Compliance

IRISc 3.0

Intelligent Risk & Integrity Screening

Mai 2023

IRISc – Intelligent Risk and Integrity Screening

01 Une solution développée par KPMG France, pragmatique et facile à déployer, pour réaliser un état des lieux des autorisations et des risques de séparation des fonctions.

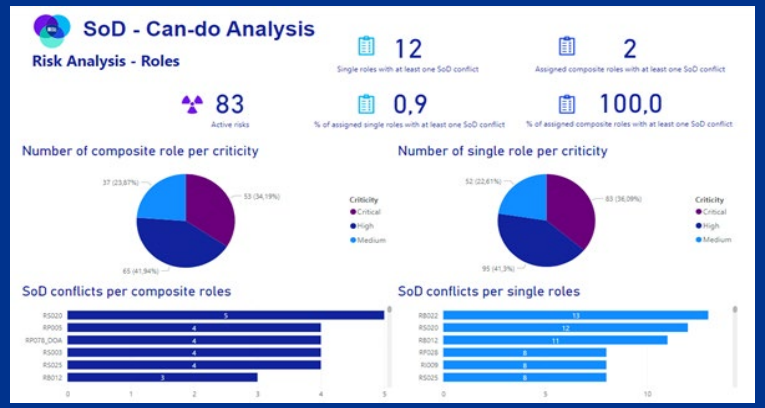
02 Flexible, l'outil est facilement adaptable et son catalogue de contrôles intégré peut être enrichi d'indicateurs spécifiques à chaque contexte.

03 Les tableaux de bords visuels et interactifs permettront à l'ensemble des parties prenantes (DSI, contrôle interne, métiers) de partager une même vision du niveau de risque dans le système.

IRISc – Les fonctionnalités

Diagnostic autorisations & SOD

Un catalogue de contrôles et indicateurs sur les autorisations et la sécurité du système SAP	Des tableaux de bord et indicateurs sur les risques SoD facilitant l'analyse	Possibilité de réaliser des analyses Did-Do pour identifier les risques avérés	Possibilité d'utiliser la matrice SoD proposée par KPMG ou une matrice tierce



Expertise

Développé en utilisant des outils maîtrisés par les équipes KPMG certifiées GRC et expertes sur les autorisations

alteryx Power BI

39% des sondés déclarent avoir un tableau de bord et des indicateurs SOD

98% des sondés utilisent Excel pour gérer ces indicateurs

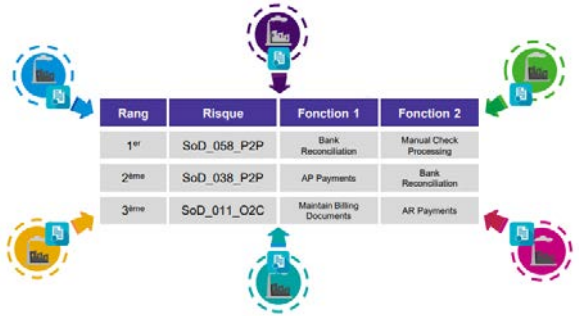
KPMG France

Zoom sur le benchmark SOD

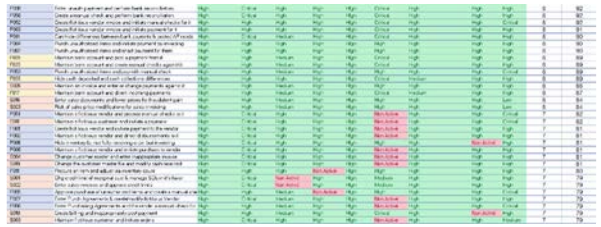
L'analyse peut être basée sur la matrice SOD du client ou à partir de la matrice SOD de KPMG créé sur la base des bonnes pratiques du marché.

Benchmark des risques SoD

Fort de son expertise fonctionnelle et sectorielle, KPMG France a construit un **benchmark des risques SoD les plus récurrents dans les organisations**, basé sur la fréquence d'activation des risques pondérés par leur criticité.

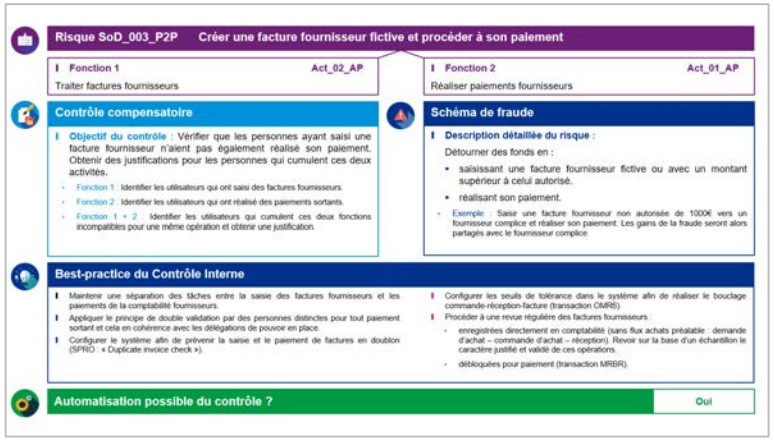


Rang	Risque	Fonction 1	Fonction 2
1er	SoD_058_P2P	Bank Reconciliation	Manual Check Processing
2ème	SoD_038_P2P	AP Payments	Bank Reconciliation
3ème	SoD_011_O2C	Maintain Billing Documents	AR Payments



Fiche risque SoD

Chaque risque fait l'objet d'une fiche expliquant le **schéma de fraude**, la bonne pratique de contrôle interne et le **contrôle compensatoire** potentiel associé. Ce référentiel, organisé par processus métier, pourra constituer la base d'une **approche itérative** de remédiation plus performante.



Risque SoD_003_P2P Créer une facture fournisseur fictive et procéder à son paiement

Fonction 1	Act_02_AP	Fonction 2	Act_01_AP
Traiter factures fournisseurs		Réaliser paiements fournisseurs	

Contrôle compensatoire

Objectif du contrôle : Vérifier que les personnes ayant saisi une facture fournisseur n'aient pas également réalisé son paiement. Obtenir des justifications pour les personnes qui cumulent ces deux activités.

- Fonction 1 : Identifier les utilisateurs qui ont saisi des factures fournisseurs.
- Fonction 2 : Identifier les utilisateurs qui ont réalisé des paiements sortants.
- Fonction 1 + 2 : Identifier les utilisateurs qui cumulent ces deux fonctions incompatibles pour une même opération et obtenir une justification.

Schéma de fraude

Description détaillée du risque :

Détourner des fonds en :

- saisissant une facture fournisseur fictive ou avec un montant supérieur à celui autorisé.
- réalisant son paiement.

Exemple : Saisir une facture fournisseur non autorisée de 1000€ vers un fournisseur complice et réaliser son paiement. Les gains de la fraude seront alors partagés avec le fournisseur complice

Best-practice du Contrôle Interne

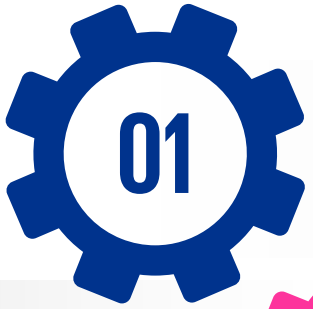
- Maintenir une séparation des tâches entre la saisie des factures fournisseurs et les paiements de la comptabilité fournisseurs.
- Appliquer le principe de double validation par des personnes distinctes pour tout paiement sortant et cela en cohérence avec les délégations de pouvoir en place.
- Configurer le système afin de prévenir la saisie et le paiement de factures en doublon (SPRO : « Duplicate invoice check »).
- Configurer les seuils de tolérance dans le système afin de réaliser le bouclage commande-réception-facture (transaction OMRS).
- Procéder à une revue régulière des factures fournisseurs :
  - enregistrées directement en comptabilité (sans flux achats préalable : demande d'achat – commande d'achat – réception). Revoir sur la base d'un échantillon le caractère justifié et validé de ces opérations.
  - débloquées pour paiement (transaction MRBR).

Automatisation possible du contrôle ? Oui

IRISc – Quelles sont les priorités des parties prenantes?

63% Des sondés identifient comme priorité l'outillage du Contrôle Interne pour améliorer la collaboration entre les trois lignes de défense

KPMG France Study 2021

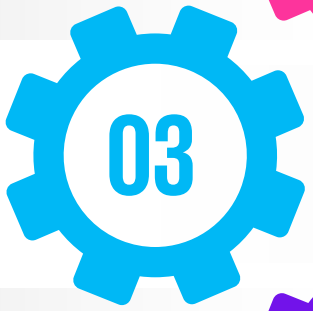


Directions Métier

- Des tableaux de bord **intelligibles et vulgarisés** qui permettent d'identifier les anomalies de séparation des fonctions sur les processus
- Des **contrôles compensatoires** pour remédier les risques sur les processus
- Des leviers **d'automatisation** des contrôles compensatoires

Direction Contrôle Interne

- La **maîtrise des risques** générés par les modifications des accès utilisateurs au quotidien
- La **garantie de la séparation des fonctions** au sein des processus critiques



Direction Audit Interne

- L'identification des zones de risque critiques et adresser en priorité
- L'**intégrité du dispositif de contrôles** en cas de réorganisation, d'acquisition de sociétés ou programme de transformation majeur

Direction des SI

- Un **outil agile et performant** facile à maintenir
- Des **tableaux de bord** et des **indicateurs** qui permettent d'identifier des déficiences dans la gestion des autorisations
- Un **état des lieux pragmatique** des propriétés des rôles et utilisateurs du système

IRISc – Les bénéfices

Robustesse & Ergonomie

- Construction de scripts d'analyse sur les objets les plus fins de l'ERP
- Des tableaux de bord interactifs et intelligibles pour tous les acteurs

83%

De réduction des risques en moyenne sur quelques semaines

Fiabilité & Rapidité

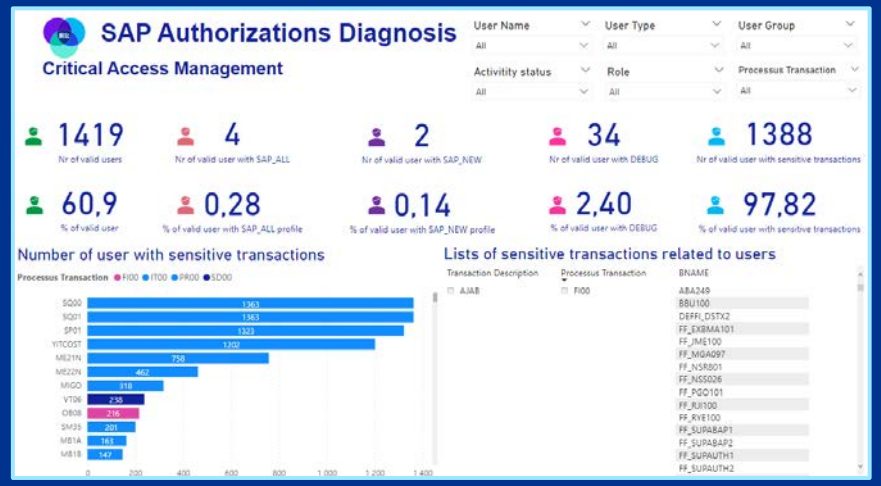
- Des indicateurs construits sur la base de multiples expériences clients
- Un diagnostic efficace basé sur les données standards du système

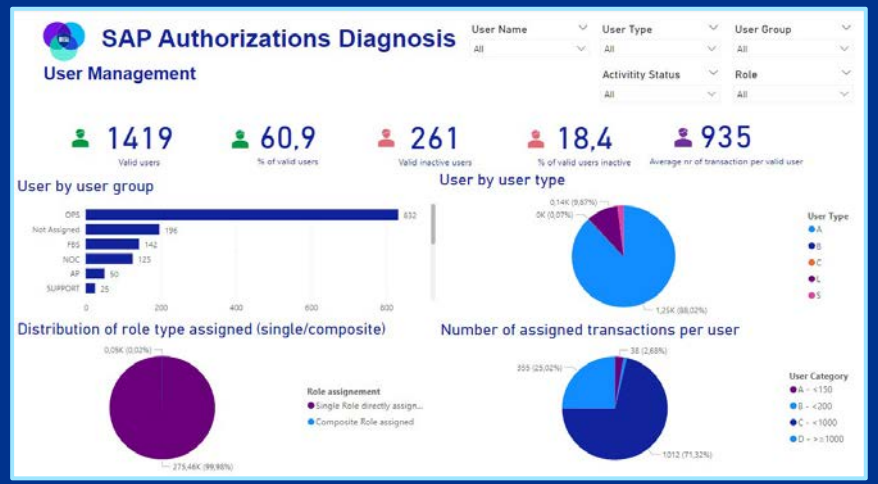
Flexibilité & Performance

- Des indicateurs standards ou sur mesure quelle que soit la version de l'ERP
- La possibilité de traiter des volumes de données significatifs
- Possibilité d'utiliser un matrice SOD KPMG basé sur les bonnes pratiques du marché, ainsi qu'un ensemble de règles spécifiques à l'entreprise

IRISc – Aperçu des tableaux de bord

Les fichiers de détail des analyses de risques peuvent être téléchargés pour investiguer les éventuelles anomalies et construire le plan d'action





Les matrices SOD de KPMG couvrent les processus suivants :

SAP	Microsoft D365
Basis, Finance, HR and Payroll, MM, O2C, P2P	A2R, Q2C, R2R, S2P

IRISc – Notre offre d'accompagnement

Revue de matrice SOD	Revue de la matrice SOD et des contrôles compensatoires Analyse critique des risques du référentiel au regard des processus métiers et des bonnes pratiques du marché
Aide au choix d'outillage	Benchmark des différentes solutions du marché au regard de vos besoins métier, de votre contexte IT & organisationnel
Revue de gouvernance	Revue critique des procédures, du RACI et des KPIs de gouvernance GRC
Déploiement de solutions GRC	Définition & mise en place de la stratégie GRC dans les programmes de transformation Conception et intégration des solutions GRC
Data Management	Identification des conflits SoD et aide au choix des actions de remédiation ou d'atténuation les plus appropriées Assistance à la reconstruction des rôles dans le système afin d'obtenir un modèle d'autorisation sans conflit SoD
Automatisation des contrôles	Identification des leviers d'automatisation sur la base des référentiels de contrôles existants & cibles. Automatisation des contrôles et mise en place des workflows

Contacts

Pauline Eckert
peckert@kpmg.fr

Mathieu Chastre
mchastre@kpmg.fr

kpmg.fr