



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



39%

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

98%

des sondés utilisent Excel pour gérer ces indicateurs

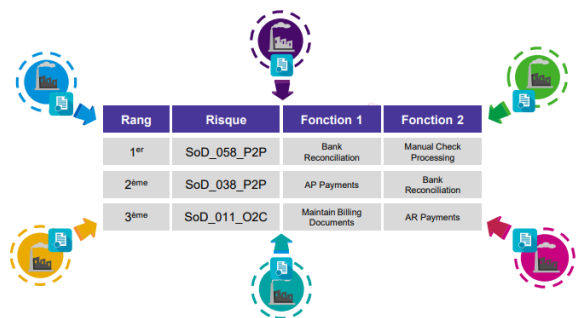
KPMG France

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.



Risque	Impact	Fréquence	Criticité	SoD	Processus	Contrôle	Prévalence	Score
1000	Créer un paiement et le valider sans autorisation	High	Critical	High	High	Critical	High	92
1001	Créer un paiement et le valider sans autorisation	High	Critical	High	High	Critical	High	90
1002	Créer un paiement et le valider sans autorisation	High	Critical	High	High	Critical	High	89
1003	Créer un paiement et le valider sans autorisation	High	Critical	High	High	Critical	High	88
1004	Créer un paiement et le valider sans autorisation	High	Critical	High	High	Critical	High	87
1005	Créer un paiement et le valider sans autorisation	High	Critical	High	High	Critical	High	86
1006	Créer un paiement et le valider sans autorisation	High	Critical	High	High	Critical	High	85
1007	Créer un paiement et le valider sans autorisation	High	Critical	High	High	Critical	High	84
1008	Créer un paiement et le valider sans autorisation	High	Critical	High	High	Critical	High	83
1009	Créer un paiement et le valider sans autorisation	High	Critical	High	High	Critical	High	82
1010	Créer un paiement et le valider sans autorisation	High	Critical	High	High	Critical	High	81
1011	Créer un paiement et le valider sans autorisation	High	Critical	High	High	Critical	High	80
1012	Créer un paiement et le valider sans autorisation	High	Critical	High	High	Critical	High	79
1013	Créer un paiement et le valider sans autorisation	High	Critical	High	High	Critical	High	78
1014	Créer un paiement et le valider sans autorisation	High	Critical	High	High	Critical	High	77
1015	Créer un paiement et le valider sans autorisation	High	Critical	High	High	Critical	High	76
1016	Créer un paiement et le valider sans autorisation	High	Critical	High	High	Critical	High	75
1017	Créer un paiement et le valider sans autorisation	High	Critical	High	High	Critical	High	74
1018	Créer un paiement et le valider sans autorisation	High	Critical	High	High	Critical	High	73
1019	Créer un paiement et le valider sans autorisation	High	Critical	High	High	Critical	High	72
1020	Créer un paiement et le valider sans autorisation	High	Critical	High	High	Critical	High	71
1021	Créer un paiement et le valider sans autorisation	High	Critical	High	High	Critical	High	70
1022	Créer un paiement et le valider sans autorisation	High	Critical	High	High	Critical	High	69
1023	Créer un paiement et le valider sans autorisation	High	Critical	High	High	Critical	High	68
1024	Créer un paiement et le valider sans autorisation	High	Critical	High	High	Critical	High	67
1025	Créer un paiement et le valider sans autorisation	High	Critical	High	High	Critical	High	66
1026	Créer un paiement et le valider sans autorisation	High	Critical	High	High	Critical	High	65
1027	Créer un paiement et le valider sans autorisation	High	Critical	High	High	Critical	High	64
1028	Créer un paiement et le valider sans autorisation	High	Critical	High	High	Critical	High	63
1029	Créer un paiement et le valider sans autorisation	High	Critical	High	High	Critical	High	62
1030	Créer un paiement et le valider sans autorisation	High	Critical	High	High	Critical	High	61
1031	Créer un paiement et le valider sans autorisation	High	Critical	High	High	Critical	High	60
1032	Créer un paiement et le valider sans autorisation	High	Critical	High	High	Critical	High	59
1033	Créer un paiement et le valider sans autorisation	High	Critical	High	High	Critical	High	58
1034	Créer un paiement et le valider sans autorisation	High	Critical	High	High	Critical	High	57
1035	Créer un paiement et le valider sans autorisation	High	Critical	High	High	Critical	High	56
1036	Créer un paiement et le valider sans autorisation	High	Critical	High	High	Critical	High	55
1037	Créer un paiement et le valider sans autorisation	High	Critical	High	High	Critical	High	54
1038	Créer un paiement et le valider sans autorisation	High	Critical	High	High	Critical	High	53
1039	Créer un paiement et le valider sans autorisation	High	Critical	High	High	Critical	High	52
1040	Créer un paiement et le valider sans autorisation	High	Critical	High	High	Critical	High	51
1041	Créer un paiement et le valider sans autorisation	High	Critical	High	High	Critical	High	50
1042	Créer un paiement et le valider sans autorisation	High	Critical	High	High	Critical	High	49
1043	Créer un paiement et le valider sans autorisation	High	Critical	High	High	Critical	High	48
1044	Créer un paiement et le valider sans autorisation	High	Critical	High	High	Critical	High	47
1045	Créer un paiement et le valider sans autorisation	High	Critical	High	High	Critical	High	46
1046	Créer un paiement et le valider sans autorisation	High	Critical	High	High	Critical	High	45
1047	Créer un paiement et le valider sans autorisation	High	Critical	High	High	Critical	High	44
1048	Créer un paiement et le valider sans autorisation	High	Critical	High	High	Critical	High	43
1049	Créer un paiement et le valider sans autorisation	High	Critical	High	High	Critical	High	42
1050	Créer un paiement et le valider sans autorisation	High	Critical	High	High	Critical	High	41
1051	Créer un paiement et le valider sans autorisation	High	Critical	High	High	Critical	High	40
1052	Créer un paiement et le valider sans autorisation	High	Critical	High	High	Critical	High	39
1053	Créer un paiement et le valider sans autorisation	High	Critical	High	High	Critical	High	38
1054	Créer un paiement et le valider sans autorisation	High	Critical	High	High	Critical	High	37
1055	Créer un paiement et le valider sans autorisation	High	Critical	High	High	Critical	High	36
1056	Créer un paiement et le valider sans autorisation	High	Critical	High	High	Critical	High	35
1057	Créer un paiement et le valider sans autorisation	High	Critical	High	High	Critical	High	34
1058	Créer un paiement et le valider sans autorisation	High	Critical	High	High	Critical	High	33
1059	Créer un paiement et le valider sans autorisation	High	Critical	High	High	Critical	High	32
1060	Créer un paiement et le valider sans autorisation	High	Critical	High	High	Critical	High	31
1061	Créer un paiement et le valider sans autorisation	High	Critical	High	High	Critical	High	30
1062	Créer un paiement et le valider sans autorisation	High	Critical	High	High	Critical	High	29
1063	Créer un paiement et le valider sans autorisation	High	Critical	High	High	Critical	High	28
1064	Créer un paiement et le valider sans autorisation	High	Critical	High	High	Critical	High	27
1065	Créer un paiement et le valider sans autorisation	High	Critical	High	High	Critical	High	26
1066	Créer un paiement et le valider sans autorisation	High	Critical	High	High	Critical	High	25
1067	Créer un paiement et le valider sans autorisation	High	Critical	High	High	Critical	High	24
1068	Créer un paiement et le valider sans autorisation	High	Critical	High	High	Critical	High	23
1069	Créer un paiement et le valider sans autorisation	High	Critical	High	High	Critical	High	22
1070	Créer un paiement et le valider sans autorisation	High	Critical	High	High	Critical	High	21
1071	Créer un paiement et le valider sans autorisation	High	Critical	High	High	Critical	High	20
1072	Créer un paiement et le valider sans autorisation	High	Critical	High	High	Critical	High	19
1073	Créer un paiement et le valider sans autorisation	High	Critical	High	High	Critical	High	18
1074	Créer un paiement et le valider sans autorisation	High	Critical	High	High	Critical	High	17
1075	Créer un paiement et le valider sans autorisation	High	Critical	High	High	Critical	High	16
1076	Créer un paiement et le valider sans autorisation	High	Critical	High	High	Critical	High	15
1077	Créer un paiement et le valider sans autorisation	High	Critical	High	High	Critical	High	14
1078	Créer un paiement et le valider sans autorisation	High	Critical	High	High	Critical	High	13
1079	Créer un paiement et le valider sans autorisation	High	Critical	High	High	Critical	High	12
1080	Créer un paiement et le valider sans autorisation	High	Critical	High	High	Critical	High	11
1081	Créer un paiement et le valider sans autorisation	High	Critical	High	High	Critical	High	10
1082	Créer un paiement et le valider sans autorisation	High	Critical	High	High	Critical	High	9
1083	Créer un paiement et le valider sans autorisation	High	Critical	High	High	Critical	High	8
1084	Créer un paiement et le valider sans autorisation	High	Critical	High	High	Critical	High	7
1085	Créer un paiement et le valider sans autorisation	High	Critical	High	High	Critical	High	6
1086	Créer un paiement et le valider sans autorisation	High	Critical	High	High	Critical	High	5
1087	Créer un paiement et le valider sans autorisation	High	Critical	High	High	Critical	High	4
1088	Créer un paiement et le valider sans autorisation	High	Critical	High	High	Critical	High	3
1089	Créer un paiement et le valider sans autorisation	High	Critical	High	High	Critical	High	2
1090	Créer un paiement et le valider sans autorisation	High	Critical	High	High	Critical	High	1

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

<p>Fonction 1 Act_02_AP Traiter factures fournisseurs</p> <p>Contrôle compensatoire</p> <p>Objectif du contrôle : Vérifier que les personnes ayant saisi une facture fournisseur n'ont pas également réalisé son paiement. Obtenir des justifications pour les personnes qui cumulent ces deux activités.</p> <ul style="list-style-type: none"> 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. <p>Best-practice du Contrôle Interne</p> <ul style="list-style-type: none"> 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 coherente avec les délégations de pouvoir en place. Configurer le système afin de prévenir la saisie et le paiement de factures en double (SPRO « Duplicate invoice check »). 	<p>Fonction 2 Act_01_AP Réaliser paiements fournisseurs</p> <p>Schéma de fraude</p> <p>Description détaillée du risque :</p> <p>Détourner des fonds en :</p> <ul style="list-style-type: none"> saissant une facture fournisseur fictive ou avec un montant supérieur à celui autorisé. réalisant son paiement. <p>Exemple : Saisir une facture fournisseur non autorisée de 1000€ vers un fournisseur complexe et réaliser son paiement. Les gains de la fraude seront alors partagés avec le fournisseur complexe.</p> <p>Configurer les seuils de tolérance dans le système afin de réaliser le bouclage commande-réception-facture (transaction OMR8).</p> <p>Procéder à une revue régulière des factures fournisseurs :</p> <ul style="list-style-type: none"> enregistrées directement en comptabilité (sans flux achats préalable : demande d'achat - commande d'achat - réception). Revenir sur la base d'un échantillon le caractère justifié et valide de ces opérations. débloquées pour paiement (transaction MRBR).
--	---

Automatisation possible du contrôle ? Oui



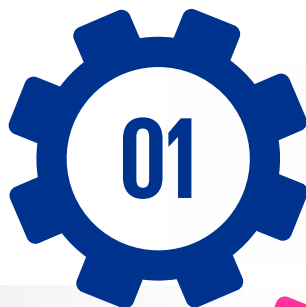
IRISc – Quelles sont les priorités des parties prenantes?

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

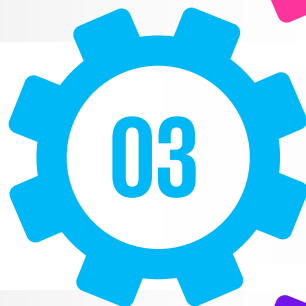
Directions Métier



- 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

- 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 Audit Interne



- 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

- 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 Contrôle Interne



Direction des SI



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

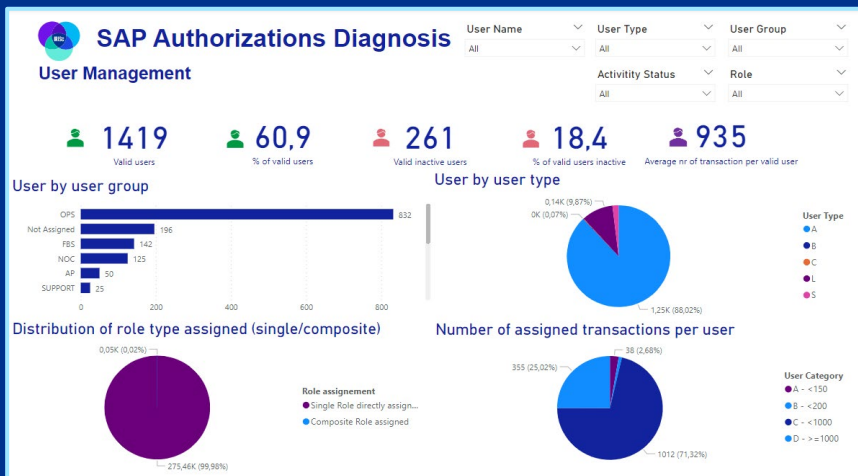
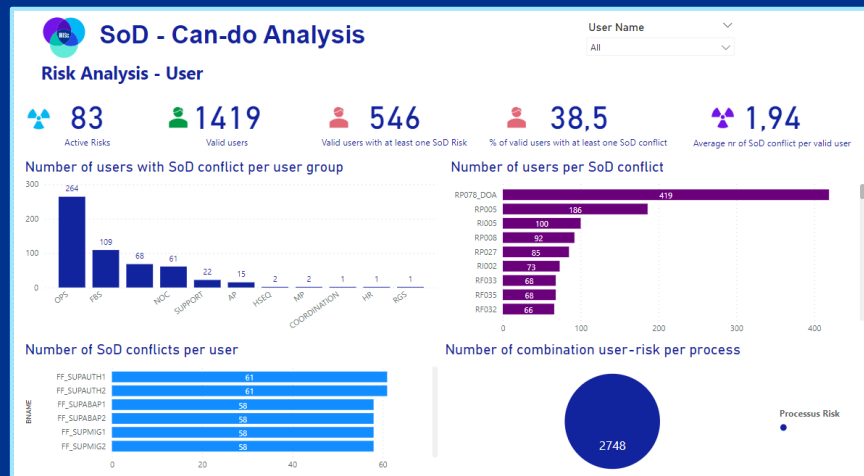
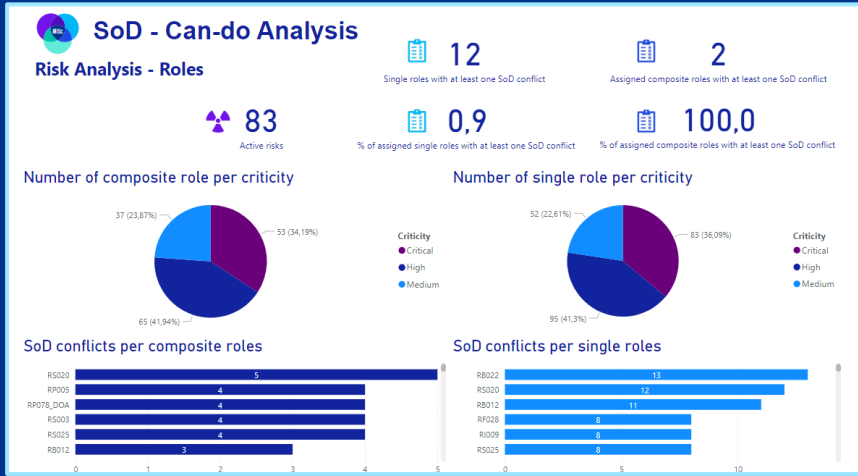
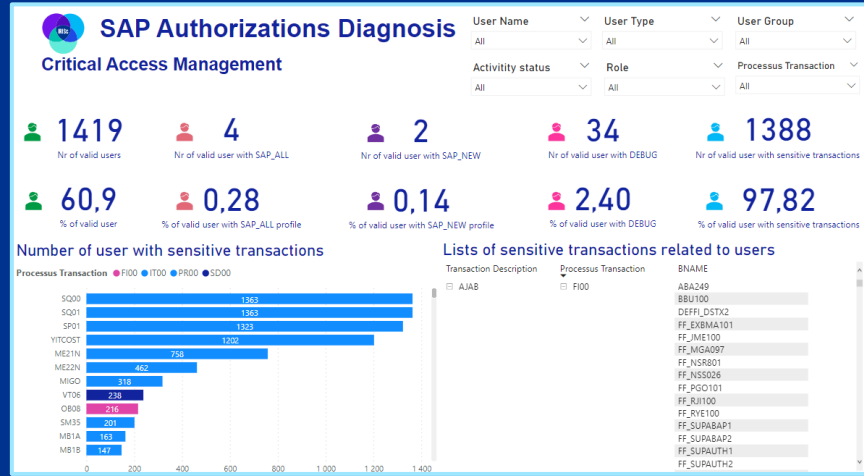


Flexibilité & Performance

- 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

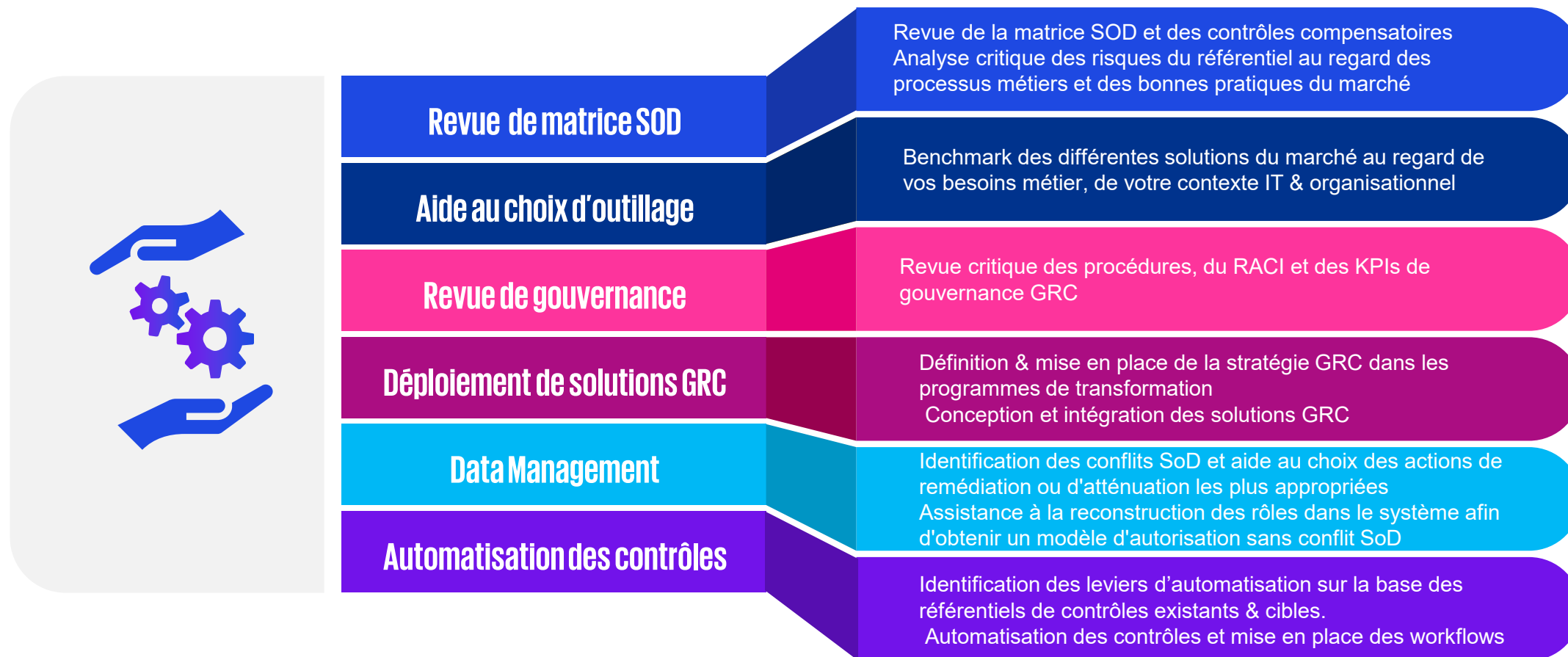


Les matrices SOD de KPMG couvrent les processus suivants :

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



IRISc – Notre offre d'accompagnement





Contacts

Pauline Eckert

peckert@kpmg.fr

Mathieu Chastre

mchastre@kpmg.fr

kpmg.fr



Les informations contenues dans ce document sont d'ordre général et ne sont pas destinées à traiter les particularités d'une personne ou d'une entité. Bien que nous fassions tout notre possible pour fournir des informations exactes et appropriées, nous ne pouvons garantir que ces informations seront toujours exactes à une date ultérieure. Elles ne peuvent ni ne doivent servir de support à des décisions sans validation par les professionnels ad hoc. KPMG S.A. est membre français de l'organisation mondiale KPMG constituée de cabinets indépendants affiliés à KPMG International Limited, une société de droit anglais (« private company limited by guarantee »). KPMG International et ses entités liées ne proposent pas de services aux clients. Aucun cabinet membre n'a le droit d'engager KPMG International ou les autres cabinets membres vis-à-vis des tiers. KPMG International n'a le droit d'engager aucun cabinet membre.

© 2023 KPMG S.A., société anonyme d'expertise comptable et de commissariat aux comptes, membre français de l'organisation mondiale KPMG constituée de cabinets indépendants affiliés à KPMG International Limited, une société de droit anglais (« private company limited by guarantee »). Tous droits réservés. Le nom et le logo KPMG sont des marques utilisées sous licence par les cabinets indépendants membres de l'organisation mondiale KPMG.