AFAI
Pour des systèmes d'information de confiance et créateurs de valeur

ifaci
institut français de l'audit et du contrôle internes

USF

ÉCHANGES ET PARTAGES

LIVRE BLANC

GUIDE D'ÉVALUATION D'UN SYSTÈME SAP POUR L'AUDIT INTERNE

À l'usage des auditeurs internes et managers du SI

Février 2015

Préface

Que l'on soit utilisateur ou non, il n'est plus utile de présenter l'ERP SAP. SAP, comme tous les ERPs, est plus qu'un simple système informatique : il formalise, structure les processus et comporte de nombreuses fonctionnalités métiers. Ainsi, les données les plus stratégiques y sont stockées. Ce système d'information est devenu si omniprésent au sein des organisations privées comme publiques que son nom entre dans le vocabulaire courant de leurs collaborateurs. Qui n'a pas entendu dire « c'est dans SAP » ou « c'est un processus SAP » ?

Toutefois, par son étendue dans l'organisation, par sa richesse et sa complexité, la mise en œuvre et l'emploi de ce type d'outil engendrent des risques spécifiques et tout dysfonctionnement du logiciel ou incident de sécurité peut avoir des impacts considérables sur l'image et plus encore sur l'activité de l'organisation qui l'utilise et donc directement sur son chiffre d'affaires.

C'est tout à fait naturellement que l'Institut Français des Auditeurs et Contrôleurs Internes (IFACI), l'Association Française de l'Audit et du conseil Informatiques (AFAI) et l'association des Utilisateurs SAP Francophones (USF) ont collaboré pendant plus d'un an pour rédiger ce guide d'évaluation d'un système SAP.

Destiné à un public large, il aidera à révéler les failles du contrôle interne liées à l'exploitation de SAP et à alerter l'organisation.

Nous tenons à souligner plus particulièrement la collaboration exemplaire, l'implication et la complémentarité des membres des trois associations qui ont élaboré cet ouvrage.

Pascal Antonini	**Farid Aractingi**	**Claude Molly-Mitton**
Président AFAI	Président IFACI	Président USF

Avertissement et droits d'auteur

Le présent Livre Blanc est le résultat de travaux menés par des membres de l'AFAI, de l'IFACI et de l'USF, dans le cadre d'un Groupe de Travail commun.

Les positions et opinions exprimées dans ce Livre Blanc représentent la compréhension de l'AFAI, de l'IFACI et de l'USF, au regard des informations à leur disposition à la date de rédaction du document. Toutes les marques, noms commerciaux, noms de domaines et autres signes distinctifs cités dans ce document sont utilisés à des fins d'identification et restent la propriété de leurs titulaires respectifs.

Remerciements

Comité de pilotage :

- Pascal Antonini, Président de l'AFAI.
- Patrick Geai, Vice-Président de l'USF.
- Vincent Manière, Vice-Président de l'AFAI.
- Philippe Mocquard, Délégué Général de l'IFACI.
- Claude Molly-Mitton, Président de l'USF.
- Yohann Vermeren, Membre de l'IFACI.

Contributeurs / Experts :

- Stéphanie Benzaquine, MAZARS.
- Bénédicte Ferrand, SHISHEIDO.
- Karen Moutardier, ERNST & YOUNG.
- Véronique Vias, BOUYGUES CONSTRUCTION.
- Eric Blanc, ASSISTANCE PUBLIQUE - HÔPITAUX DE PARIS.
- Frédéric Hemmer, EDF.
- Jean-Yves Kemplaire, CHR HANSEN.
- Jérome Lamotte, ARCELOR - MITTAL.
- Thibault Mathieux, LA POSTE.
- David Métivier, SODEXO.
- Simon Redondie, Direction Générale - GENDARMERIE NATIONALE.
- Gunnar Ribbert, SANOFI.

Ce Livre Blanc a été rédigé par Patrick Geai (LA POSTE), Vincent Manière (VMA CONSEILS) et Yohann Vermeren (KPMG).

Guide d'évaluation d'un système SAP pour l'audit interne : À l'usage des auditeurs internes et managers du SI

Sommaire

Objectif de ce guide

L'ERP SAP est un des progiciels qui soutiennent généralement des processus majeurs d'une entreprise ou d'une administration publique. Du fait de son caractère global et transverse, des données sensibles (Brevets industriels, données commerciales, financières, RH, etc) se retrouvent souvent dans les bases de données SAP. De plus, ses fonctionnalités sont vitales pour la mise en œuvre et le contrôle de processus majeurs.

Cela peut avoir, en cas de défaillance significative du système SAP, des impacts importants. Les principaux risques identifiés sont d'ordre financier, social, juridique et d'image. Le risque particulier lié à un système SAP concerne sa complexité, liée à sa richesse, qu'il convient de maitriser tant au niveau de l'installation que de la maintenance.

Dans ce contexte, l'Association Française de l'Audit et du conseil Informatique (AFAI), l'Institut Français de l'Audit et du Contrôle Internes (IFACI) et les Utilisateurs SAP Francophones (USF) ont souhaité s'associer pour réaliser un guide d'évaluation d'un système SAP. Les principaux objectifs recherchés ont été :

Pour les auditeurs et contrôleurs internes :

- Disposer d'un guide utilisable par des auditeurs n'ayant pas de compétence forte en informatique ni sur le progiciel SAP,
- Permettre d'établir un premier diagnostic sur la performance, la résilience et le niveau de sécurité du système SAP de l'organisation,
- Disposer des éléments d'alerte permettant d'identifier le besoin de lancer l'audit approfondi d'un ou plusieurs aspects d'un système SAP.

Pour les DSI et centres de compétences SAP :

- Disposer d'un référentiel clairement défini et reconnu sur les risques et bonnes pratiques SAP,
- Pouvoir auto-évaluer le niveau de maîtrise d'un système SAP,
- Anticiper autant que possible les incidents,
- Rendre les opérations du centre de compétences plus transparentes,
- Démystifier et communiquer, vis-à-vis de l'ensemble des directions de l'organisation, sur le niveau de maîtrise du système SAP dans l'organisation.

Objectif commun :

- Parler le même langage.

Certains éléments de guide peuvent être utilisés dans un contexte ERP hors SAP, les travaux proposés étant parfois applicables aux autres ERP.

Comme indiqué précédemment, ce guide d'évaluation d'un système SAP se veut avant tout pragmatique.

L'ambition de ce guide est donc de donner au lecteur un outil permettant d'acquérir une « assurance raisonnable » de la qualité et du niveau de sécurité d'un système SAP. Dans un second temps et en fonction du résultat obtenu, cette évaluation permettra d'identifier les risques et défaillances potentielles afin, si cela est nécessaire, de lancer un audit plus approfondi.

10 questions avant de se lancer dans l'évaluation

Avant de se lancer dans l'évaluation de SAP, il convient de comprendre les particularités du système SAP et de son périmètre. Effectivement, la criticité, la complexité ou par exemple la couverture fonctionnelle est différente d'un environnement SAP à un autre. Plusieurs questions simples permettront de mieux appréhender le contexte de la mission et pourront aider l'auditeur dans son jugement professionnel en cas de faiblesses identifiées.

- Quelle est la version du produit SAP audité (certaines versions anciennes de SAP ne sont plus maintenues par l'éditeur, certaines fonctionnalités ne sont disponibles que dans les versions récentes) ?
- Quelle est la couverture fonctionnelle (c'est-à-dire gestion des achats, des ventes, de la production etc) ?
- Quels sont les modules implémentés (par exemples : FI, MM, SD, CO, WM) ?
- Combien d'utilisateurs ont accès à SAP ?
- Combien existe-t-il de core models, de mandants et d'instances de production ?
- Quels sont les principaux sous-traitants pour l'exploitation, la maintenance évolutive, l'hébergement... ?
- Quelle est la criticité des processus ?
- Quels sont les projets et évolutions majeures (métiers et SI) en cours et prévus (relatifs à SAP) ?
- Quelles sont les interfaces critiques avec les autres applications du SI ?
- Comment est organisée la gestion de la connaissance SAP dans l'entreprise (Key Users, Centre de Compétence...) ?

Périmètre

De par son niveau stratégique (étant souvent support des processus métiers et financiers critiques) et sa grande couverture fonctionnelle, le périmètre d'investigation de SAP peut être très vaste. En effet, nous avons dénombré huit thèmes à explorer :

- Dimension stratégique de SAP dans l'organisation,
- Positionnement du Centre de compétence SAP,
- Gestion de la sous-traitance,
- Gestion des relations commerciales avec SAP,
- Modules fonctionnels tels que la finance ou la gestion de stocks,
- **Sécurité SAP**,
- **Continuité d'activité**,
- Maîtrise des risques liés à un projet SAP.

Dans le cadre de ce premier ouvrage, nous nous sommes limités aux aspects de sécurité et de continuité des activités. Sur ces deux thèmes, nous avons identifié sept domaines d'évaluation :

D1 • Organisation et Gouvernance de la Sécurité

D2 • Sécurité des données

D3 • Sécurité des accès et habilitations

D4 • Séparation des fonctions

D5 • Sécurité des flux entrants et sortants

D6 • Continuité de service
Plan de Reprise d'Activité (PRA)

D7 • Sécurité des changements

Sécurité d'un système SAP

Limites du guide d'évaluation

En se regroupant, les trois associations (AFAI, IFACI, USF) ont souhaité élaborer un guide ne nécessitant pas de compétence forte en Système d'Information sur le progiciel SAP, la principale cible étant de réaliser un outil pour les auditeurs internes généralistes des organisations.

Compte tenu de ce choix, ce document n'a pas pour vocation d'évaluer de façon exhaustive les aspects de sécurité liés à un système SAP. Il permet simplement d'évaluer le niveau de sécurité d'un système SAP et d'en identifier les points de vigilance. L'identification de ces derniers permettra à l'auditeur généraliste de demander un audit approfondi SAP sur tout ou partie du périmètre. Cet audit approfondi devra être mené par un expert du sujet SAP. Ce document n'a pas la vocation de servir de référentiel pour mener des audits approfondis par des experts du système SAP.

De plus, ce document comporte les limitations suivantes :

- Les contrôles applicatifs (par exemples : contrôle de cohérence des factures avec les commandes) et la sécurité associée ne font pas partie de ce guide d'évaluation.
- L'utilisation de ce guide et les résultats obtenus sont sous la responsabilité de l'auditeur.

Pour ces raisons, l'AFAI, l'IFACI et l'USF ont décidé de nommer ce document « Guide d'évaluation d'un système SAP pour l'Auditeur Interne ».

Méthodologie

Le Groupe de Travail s'est réparti en huit sous-groupes en fonction des différents domaines cités (cf. Périmètre, page 10). En moyenne, chaque personne a participé à deux sous-groupes. Pour chacun d'eux, un leader a été désigné pour assurer les aspects d'organisation (convocations, logistique, comptes-rendus...).

Chaque sous-groupe avait pour tâche :

- de préparer la rédaction d'un domaine suivant un format prédéfini,
- de présenter ses travaux en réunion plénière pour discussion,
- de mettre à jour son domaine en fonction des remarques faites en plénière.

Une trentaine de réunions en sous-groupe et une douzaine de réunions plénières ont été organisées avant d'aboutir à la constitution de ce guide d'évaluation rédigé par les trois copilotes de ces travaux.

Enfin, une relecture globale a été organisée avec tous les contributeurs et certains auditeurs généralistes.

Pour fixer les grands objectifs, superviser les travaux et arbitrer en cas de besoin, un comité de pilotage s'est réuni cinq fois. Cette instance était composée du Délégué Général de l'IFACI, des Présidents de l'AFAI et de l'USF et des trois copilotes des travaux.

Structuration du guide d'évaluation

Ce guide d'évaluation a été structuré selon les huit « **Domaines** » présentés au paragraphe « Périmètre » de cet ouvrage.

Pour chacun de ces domaines, il a été identifié de trois à sept « **Objectifs de Contrôle** » représentant des sous-chapitres à évaluer.

Exemple d'un objectif de contrôle : « L'organisation a défini une matrice de séparation unique des fonctions **validée par le management** » (cf. Domaine « Séparation des fonctions »).

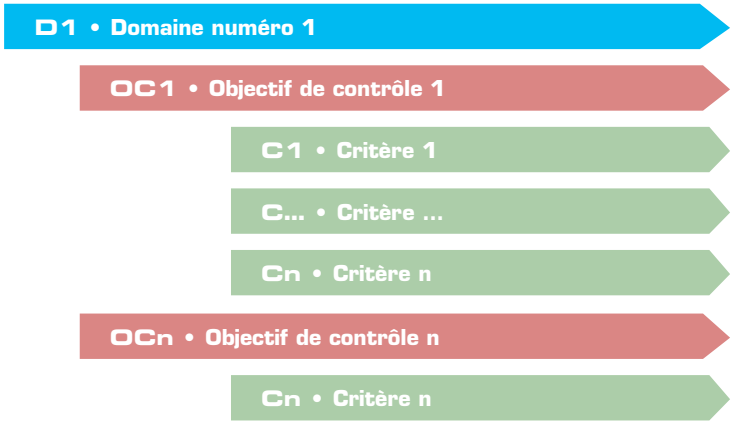
Ces critères ne sont pas tous spécifiques à SAP.

Pour chaque objectif de contrôle, il a été défini au minimum trois « **critères d'évaluation** ».

Exemple d'un critère d'évaluation : « La matrice unique de séparation des fonctions a été adaptée aux spécificités Métier de l'entité et a été validée par le management » pour l'objectif de contrôle ci-dessus.

Une méthode d'évaluation ainsi que des conseils pour utiliser ce guide sont également fournis.

Structure du guide d'évaluation



Comment utiliser ce guide d'évaluation ?

Modalités d'évaluation

Lors de la préparation de son programme d'évaluation et d'auto-évaluation, l'auditeur pourra sélectionner le ou les domaines correspondant au périmètre de sa mission. Il est donc tout à fait possible de réaliser une évaluation ciblée sur un ou plusieurs domaines. Bien entendu, en fonction du périmètre de la mission, il peut être pertinent de sélectionner plusieurs domaines qui seraient complémentaires.

Une fois le ou les domaines choisis, en fonction des objectifs et du périmètre de l'évaluation que l'on souhaite pratiquer (sur la base d'une analyse des risques préalable lorsqu'il s'agit d'un audit interne), il s'agit de passer en revue l'ensemble des objectifs de contrôle à évaluer. Pour chacun de ces objectifs de contrôle, il faut évaluer le niveau de maîtrise de chacun des critères correspondants.

Les critères d'un même objectif de contrôle expriment parfois une progressivité dans le niveau de maîtrise. Il n'y a cependant pas de pondération à appliquer et chaque critère peut s'évaluer indépendamment des autres critères.

Pour évaluer un objectif de contrôle, il convient donc d'examiner l'ensemble des critères de l'objectif de contrôle concerné. Le cas échéant, il conviendra de spécifier si un critère est « non applicable » au contexte du système SAP évalué.

Ci-dessous, Structure de fiche de test type :

OBJECTIF DE CONTRÔLE N°n

• PRÉSENTE LES ACTIVITÉS, MÉTHODES ET MESURES ORDONNÉES PAR LE MANAGEMENT AFIN DE GARANTIR LE DÉROULEMENT CONFORME D'UNE OPÉRATION.

CRITÈRE 1 • Les critères permettent d'évaluer si l'ensemble des conditions sont réunies pour répondre à l'objectif du contrôle.

Commentaires • Critère 1

Des informations complémentaires sont présentées dans la rubrique « commentaires » afin de faciliter la compréhension des travaux attendus.

Risques • Critère 1

Cette rubrique présente les risques génériques couverts par le contrôle.

Critère spécifique à SAP • Critère 1

Certains critères peuvent être évalués sans une connaissance particulière SAP.

Preuves à demander

- Documentation demandée permettant de justifier les travaux réalisés afin de comprendre le fonctionnement du contrôle et permettant de conclure.

Pour chacun de ces critères, le Groupe de Travail a retenu le code couleur suivant pour chaque niveau de maîtrise :

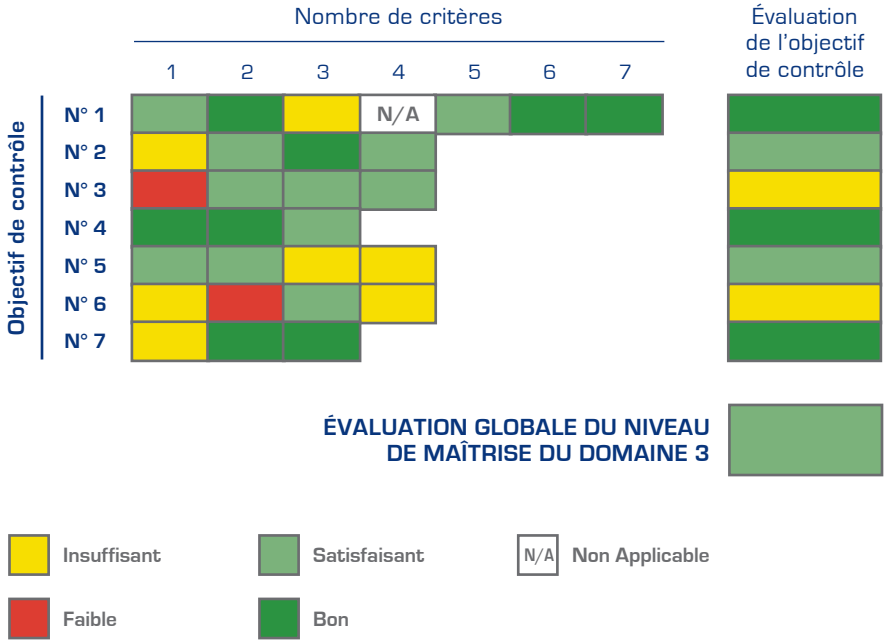
- Rouge : faible,
- Jaune : insuffisant,
- Vert clair : satisfaisant,
- Vert foncé : bon,
- Couleur blanche + N / A : Critère « Non Applicable » au contexte du système SAP évalué.

Il est bien sûr nécessaire de recueillir des preuves (documentation, tableaux de bord, comptes-rendus d'entretiens, indicateurs, mails, etc) permettant de conforter l'évaluation du niveau de maîtrise constaté. L'examen de la conformité du système SAP évalué au regard des bonnes pratiques attendues est aussi un moyen d'évaluer le niveau de maîtrise.

Modalités de restitution

Une fois l'ensemble des critères évalués, pour toutes les bonnes pratiques du domaine examiné, il est possible de positionner les résultats sous la forme d'un « mur de couleurs ».

Exemple d'évaluation : Domaine 3 / Gestion des accès et habilitations



Modalités d'appréciation

Sur la base de la restitution ci-dessus, c'est à l'utilisateur de porter un jugement sur le résultat de l'évaluation de l'objectif de contrôle en lui attribuant la couleur correspondante (colonne « Évaluation de l'objectif de contrôle »). Bien entendu, ce jugement tiendra compte de l'importance relative accordée aux différents critères d'évaluation en fonction du contexte de la mission et donc des risques à couvrir.

À la suite de cette opération, l'auditeur peut ainsi donner son appréciation sur l'ensemble du domaine.

L'auditeur veillera dans son évaluation finale à identifier des points de vigilance et proposera éventuellement un audit approfondi.

domaine 1. Organisation et gouvernance de la Sécurité SAP

DÉFINITION ET PÉRIMÈTRE DU DOMAINE

- Ce domaine traite de l'organisation et des principes liés à la sécurité du système d'information relatifs à SAP. Les critères présentés dans ce domaine permettent d'évaluer le cadre des contrôles mis en place par l'entreprise couvrant dès lors les autres domaines traités dans ce guide.
- En termes de contenu, ce domaine a pour objectifs de s'assurer :
  - qu'une gestion des risques relatifs à SAP soit mise en place,
  - que des politiques et directives définissent les règles sur les aspects sécurité du système d'information et prennent en compte les particularités d'un système SAP,
  - et que les moyens de contrôle sont mis en place au sein de l'entreprise.
- Il convient aussi d'obtenir une compréhension précise des rôles et responsabilités des acteurs pour chacun des objectifs de contrôle de ce domaine.
- Un objectif de contrôle spécifique relatif à la gestion des sous-traitants a été défini compte tenu de l'ampleur du recours à la sous-traitance dans l'environnement informatique et particulièrement dans l'écosystème SAP.

RISQUES ASSOCIÉS

- Un dispositif de gestion des risques informatiques inadapté aux enjeux métiers ne permet pas de prendre en compte les risques majeurs de l'entreprise. Des risques informatiques peuvent être non couverts ou avec un dispositif de contrôle insuffisant. La non maîtrise des risques peut avoir des impacts importants sur l'activité de l'entreprise, notamment en termes d'intégrité (cohérence, fiabilité et pertinence) et de confidentialité des informations financières et opérationnelles.
- Une absence de démarche par les risques peut conduire à sous ou sur estimer les dispositifs de mise sous contrôle des applications majeures, des infrastructures clés et des données critiques.

OBJECTIF DE CONTRÔLE N°1

• LA GESTION DES RISQUES DU SYSTÈME SAP PREND EN COMPTE LES ENJEUX MÉTIERS

CRITÈRE 1 • Un processus d'évaluation des risques SI est décliné pour le système SAP et est mis à jour

Commentaires • Critère 1

Le processus d'évaluation des risques consiste à identifier et analyser les facteurs susceptibles d'affecter l'atteinte des objectifs métiers et financiers de l'organisation.

Ce processus vise à fixer les actions destinées à couvrir ces facteurs de risque.

Une condition préalable à l'évaluation des risques est l'établissement d'objectifs, cohérents et liés entre eux à différents niveaux.

Ci-dessous quelques exemples de risques liés au système d'information :

- Dépendance, disponibilité et fiabilité des traitements informatiques,
- Gestion des changements et des évolutions,
- Gestion des ressources et compétences SI,
- Sécurité de l'information.

Risques • Critère 1

- Arrêt non planifié de l'exploitation.
- Niveau de service insuffisant.
- Non-respect des exigences réglementaires ou légales.
- Accès non autorisé ou frauduleux.
- Vol, perte ou altération des données.

Critère spécifique à SAP • Critère 1

Critère spécifique à SAP : NON

Preuves à demander

- Obtenir le Plan de maîtrise des risques (PMR) ou son équivalent.
- Cartographie des risques SI et / ou métier : S'assurer que les risques liés au système SAP ont bien été pris en compte.

Bonnes pratiques

- Le management a mis en place une politique et une organisation de gestion des risques couvrant l'ensemble des processus critiques de l'entreprise intégrée au sein des métiers et de la fonction informatique.
- L'organisation dispose d'un processus d'évaluation continu (formel) qui identifie les risques relatifs aux processus métiers supportés par SAP, leur importance, leur probabilité de survenance et la manière de les gérer, et évalue également de manière appropriée l'impact d'un changement de circonstances pour l'entité.
- Ce dispositif d'analyse des risques implique les instances de gouvernance et leur communique les résultats.

CRITÈRE 2 • La gestion des risques telle que définie sur le système SAP est alignée avec les enjeux et les impacts métier

Commentaires • Critère 2

L'organisation dispose d'un processus d'évaluation (formel) qui identifie les risques relatifs aux processus métiers supportés par SAP, leur importance, leur probabilité de survenance et la manière de les gérer, et évalue également de manière appropriée l'impact d'un changement de circonstances pour l'entité.

Risques • Critère 2

- Arrêt non planifié de l'exploitation.
- Niveau de service insuffisant.
- Non-respect réglementaire ou légal.
- Accès non autorisé ou frauduleux.
- Vol, perte ou altération des données.

Critère spécifique à SAP • Critère 2

Critère spécifique à SAP : NON

Preuves à demander

- Processus d'évaluation et de mise à jour des risques.
- Indicateurs permettant d'alerter, de mesurer l'impact, la tendance haussière ou baissière.

Bonnes pratiques

- Les ressources informatiques supportant les processus « métiers » identifiés critiques sont inventoriées.
- L'évaluation de la fréquence et des impacts des risques SI s'appuie sur une méthode harmonisée au sein de l'entreprise et partagée avec les acteurs SI et « métiers ».
- Exemples d'indicateurs de risque (Guide d'Audit de Gouvernance des Systèmes d'Information) :
  - Risque de conformité : Non-respect des procédures de validation des livrables, de mise en production, Absence de publication des livrables...
  - Risque lié à la Sécurité : Taux d'indisponibilité des serveurs, Nombre d'incidents majeurs par application / infra, Nombre d'actes de malveillance externe (virus, hacking...), Nombre de mots de passe faibles, Nombre de tests de restauration effectués dans l'année, Nombre d'audits externes, Nombre de comptes génériques, Nombre de comptes cumulant des fonctions incompatibles...
  - Risque lié au Contrôle Interne : Niveau de satisfaction des utilisateurs, Nombre de mises en production non liées à une demande d'intervention, Nombre de changements urgents et non standards (modification des données en production)...

CRITÈRE 3 • La gestion des risques relatifs au système SAP prend en compte les incidents informatiques

Commentaires • Critère 3

Une procédure de gestion des incidents est définie et formalisée. Cette procédure définit les moyens de suivi (acteurs, outils), les indicateurs de criticité, les dispositifs d'escalade. La gestion des risques doit prendre en compte les principaux incidents informatiques afin d'évaluer la survenance d'incidents impactant un processus métier critique.

Risques • Critère 3

- Arrêt non planifié de l'exploitation.
- Niveau de service insuffisant.
- Non-respect réglementaire ou légal.
- Accès non autorisé ou frauduleux.
- Vol, perte ou altération des données.

Critère spécifique à SAP • Critère 3

Critère spécifique à SAP : NON

Preuves à demander

- La personne en charge de la gestion des risques est informée des incidents (incidents majeurs a minima) liés à SAP (arrêts non planifiés de plus de 4 heures sur un module critique). Documentations liées à la rupture de communication de l'ERP, à un incendie du centre de traitement, une panne serveur.

Bonnes pratiques

- Des bases d'incidents sont mises en place qui permettent de tracer et d'archiver les incidents majeurs.
- Un dispositif de veille est en place afin d'anticiper les risques émergents (veille sécurité internet, risques métiers ...).

CRITÈRE 4 • La gestion des risques relatifs au système SAP prend en compte les risques réglementaires, environnementaux et sociaux

Commentaires • Critère 4

Il convient ici de s'assurer que les textes légaux et réglementaires en vigueur n'ont pas été enfreints et sont bien pris en compte au sein même du système d'information SAP. Ce signifie notamment que l'organisation a la capacité à mettre en œuvre les projets de conformité dans les délais requis. Les réglementations s'appliquant peuvent être Bâle III, Solvency 3, le Contrôle Fiscal des Comptabilités Informatiques, les exigences de la CNIL[1]. Les risques sociaux s'appliquant à SAP RH sont les risques sociaux inhérents à tout SI RH.

Risques • Critère 4

- Non-respect réglementaire ou légal.

Critère spécifique à SAP • Critère 4

Critère spécifique à SAP : NON

Preuves à demander

- La personne en charge des risques est informée des évolutions réglementaires et sociales.
- Résultats de l'évaluation de la conformité réglementaire, légale et fiscale du système SAP.
- Obtenir un exemple de mise à jour de contraintes réglementaires au sein de SAP (exemples : évolution du taux de TVA, Fichier des Ecritures Comptables, déclaration à la CNIL ou autres).

Bonnes pratiques

- Les départements compétents sur les sujets réglementaires, légaux et fiscaux doivent être impliqués dans les travaux d'analyses de conformité et les actions d'alignement du SI avec les différentes contraintes réglementaires.

[1] Sans oublier les textes de base : loi de finance, code du commerce, règles comptables...

OBJECTIF DE CONTRÔLE N°2

• L'ORGANISATION A DÉFINI UNE POLITIQUE DE SÉCURITÉ PRENANT EN COMPTE LE SYSTÈME SAP

CRITÈRE 1 • Un ou plusieurs document(s) d'application de la politique de sécurité SI spécifique à SAP (« Directives de sécurité ») ont été définis

Commentaires • Critère 1

La société a défini une politique de sécurité permettant d'énoncer les principes devant être respectés. En fonction des entreprises, la politique de sécurité peut être complétée par soucis de précision autour de directives dédiées.

La politique de sécurité aborde les thèmes tels que :

- L'importance de la sécurité dans l'organisation ;
- Sa communication, son acceptation et son déploiement ;
- L'accès physique aux ressources informatiques ;
- Les responsabilités du collaborateur et du prestataire ;
- La gestion des accès (attribution, revue et révocation) à SAP ;
- L'accès aux applications, bases de données, systèmes d'exploitation ;
- La gestion des mots de passe ;
- Le monitoring du réseau ;
- L'accès à distance ;
- La protection anti-virus ;
- La revue des événements liés à la sécurité.

Risques • Critère 1

- Accès non autorisé ou frauduleux.
- Vol, perte ou altération des données.

Critère spécifique à SAP • Critère 1

Critère spécifique à SAP : NON

Preuves à demander

- Il existe une politique de sécurité du système d'information.
- Cette politique est validée de façon formelle par les instances de direction (DSI, RSSI...).
- Cette politique fait l'objet d'une revue périodique et les mises à jour sont approuvées par le management.
- Les documents d'application de la politique (référentiel de sécurité, directives de sécurité, etc) existent et sont maintenus.
- Les documents d'application de la politique de sécurité du SI traitent du système SAP.

Bonnes pratiques

- La politique de sécurité du SI doit être mise à jour régulièrement.

CRITÈRE 2 • Les directives de sécurité spécifiques au système SAP sont connues des directions concernées

Commentaires • Critère 2

Les directions concernées peuvent être la Direction des Systèmes d'Information, les directions utilisatrices de SAP (direction financière, direction logistique, direction des ressources humaines...) ainsi que leurs sous-traitants.

Risques • Critère 2

- Accès non autorisé ou frauduleux.
- Vol, perte ou altération des données.

Critère spécifique à SAP • Critère 2

Critère spécifique à SAP : NON

Preuves à demander

- Obtenir la preuve de communication des directives de sécurité inhérentes à SAP aux directions concernées (signature formelle, communication par e-mail ou diffusion sur l'Intranet ...).

Bonnes pratiques

- Le document présente l'ensemble des acteurs du document (rédacteurs, relecteurs et approbateurs), ainsi que la liste de diffusion.

CRITÈRE 3 • Des actions de sensibilisation sont régulièrement réalisées afin de diffuser les directives de sécurité SAP

Commentaires • Critère 3

Les utilisateurs SAP bénéficient de formations ou de supports de formation en vue de les informer sur les règles de sécurité applicables à SAP.

Risques • Critère 3

- Accès non autorisé ou frauduleux.
- Vol, perte ou altération des données.

Critère spécifique à SAP • Critère 3

Critère spécifique à SAP : NON

Preuves à demander

- Supports de formation en matière de sécurité du système d'information.
- Liste des participants aux formations de sécurité.
- Exemples d'email de sensibilisation ou autres dépliants montrant l'animation autour du sujet.

Bonnes pratiques

- Des communications régulières autour des bonnes pratiques en termes de sécurité informatique et d'utilisation de SAP sont faites auprès des utilisateurs du SI autour d'actions à la fois ludiques et pédagogiques (questionnaires, quizz, news...).

CRITÈRE 4 • La politique de sécurité et les « directives » associées sont régulièrement revues et mises à jour

Commentaires • Critère 4

Identifier les personnes en charge de la mise à jour de la politique de sécurité du SI et s'assurer que les nouveaux risques sont pris en compte.

Risques • Critère 4

- Accès non autorisé ou frauduleux.
- Vol, perte ou altération des données.
- Arrêt non planifié de l'exploitation.
- Niveau de service insuffisant.

Critère spécifique à SAP • Critère 4

Critère spécifique à SAP : NON

Preuves à demander

- La politique de sécurité du Système d'Information est mise à jour et validée par les instances de Direction.
- Validation formelle de la Politique de sécurité du Systèmes d'Information par les instances de Direction.

Bonnes pratiques

- Ces documents sont disponibles sur l'intranet de l'organisation.

OBJECTIF DE CONTRÔLE N°3

• L'ORGANISATION A DÉFINI ET FORMALISÉ DES DOCUMENTS DÉTAILLANT L'APPLICATION DE LA POLITIQUE DE SÉCURITÉ SI SPÉCIFIQUES À SAP (« DIRECTIVES DE SÉCURITÉ »)

CRITÈRE 1 • Une directive relative à la gestion des mots de passe a été définie

Commentaires • Critère 1

La gestion des mots de passe correspond aux règles de structuration des mots de passe (complexité, historique, durée de validité...).

Risques • Critère 1

- Accès non autorisé ou frauduleux.
- Vol, perte ou altération des données.
- Arrêt non planifié de l'exploitation.
- Niveau de service insuffisant.

Critère spécifique à SAP • Critère 1

Critère spécifique à SAP : NON

Preuves à demander

- Document décrivant la procédure de gestion des mots de passe, validée par les instances de Direction.

Bonnes pratiques

- Les directives en matière de sécurité des mots de passe doivent définir les règles suivantes :
  - Changement de mot de passe lors de la première connexion.
  - Modification régulière du mot de passe : durée de vie maximale définie.
  - Longueur minimale des mots de passe.

- Obligation de recourir à des caractères de type différents (alphanumériques et / ou caractère spéciaux).
- Historisation des derniers mots de passe.
- Blocage du compte après un nombre de tentatives de connexion infructueuses.

CRITÈRE 2 • Une directive relative à l'attribution, la revue et la révocation des accès a été définie

Commentaires • Critère 2

Le processus de gestion des rôles doit être défini en tenant compte de la séparation des fonctions.

Risques • Critère 2

- Accès non autorisé ou frauduleux.
- Vol, perte ou altération des données.

Critère spécifique à SAP • Critère 2

Critère spécifique à SAP : NON

Preuves à demander

- Procédure de gestion de l'attribution, de la revue et de la révocation des accès et exemples de mise en œuvre.

Bonnes pratiques

- Un processus intégré de suivi des utilisateurs est déployé au sein des organisations et pour l'ensemble des applications informatiques : de l'arrivée (par l'affectation des droits d'accès) jusqu'au départ (la révocation des droits), en passant par la gestion de sa mobilité (changement de périmètre).

CRITÈRE 3 • Une directive relative à la gestion des habilitations a été définie

Commentaires • Critère 3

La gestion des habilitations est formalisée au travers d'un processus d'habilitation d'un utilisateur (gestion des autorisations) par les administrateurs.

Risques • Critère 3

- Accès non autorisé ou frauduleux.
- Vol, perte ou altération des données.

Critère spécifique à SAP • Critère 3

Critère spécifique à SAP : NON

Preuves à demander

- Procédure de gestion des habilitations et exemples de mise en œuvre.

Bonnes pratiques

- Cf. objectif spécifique dédié à la gestion des habilitations (Domaine 3).

CRITÈRE 4 • Une directive liée à la gestion des utilisateurs externes (sous-traitants, auditeurs externes et autres) a été définie

Commentaires • Critère 4

La gestion des utilisateurs externes doit traiter des règles particulières (durée de validité des droits d'accès, convention de nommage pour les comptes utilisateurs...).

Risques • Critère 4

- Accès non autorisé ou frauduleux.
- Vol, perte ou altération des données.

Critère spécifique à SAP • Critère 4

Critère spécifique à SAP : NON

Preuves à demander

- Directive relative à la gestion des utilisateurs externes et exemples de mise en œuvre.

Bonnes pratiques

- Les utilisateurs externes doivent être encadrés par une directive dédiée propre présentant les règles communes aux utilisateurs externes et internes, ainsi que les règles particulières. Par exemple, Les utilisateurs externes sont clairement identifiables par une convention de nommage spécifique et ont des dates de fin de validité en adéquation avec leur contrat.

CRITÈRE 5 • Des directives relatives aux bonnes pratiques en matière de sécurité ont été définies

Commentaires • Critère 5

Différentes directives sont émises, relatives à la sécurité des données, à la séparation des fonctions, à la sécurité des flux entrants et sortants de SAP, au maintien en condition opérationnelle et la sécurité des changements, au plan de reprise d'activité et la continuité de SAP, aux copies de données de production dans des environnements non productifs ainsi qu'à l'archivage des données.

Risques • Critère 5

- Accès non autorisé ou frauduleux.
- Vol, perte ou altération des données.

Critère spécifique à SAP • Critère 5

Critère spécifique à SAP : NON

Preuves à demander

• Des directives liées :

- À la sécurité des données,
- À la séparation des fonctions,
- À la sécurité des flux entrants et sortants de SAP,
- À la sécurité des changements,
- Au plan de reprise d'activité et la continuité de SAP,
- À la sécurité des accès aux systèmes non productifs (qui reçoivent souvent des données réelles issues de la production),
- À l'archivage des données.

Bonnes pratiques

• Cf. objectif spécifique dédié.

OBJECTIF DE CONTRÔLE N°4

• L'ORGANISATION A DÉFINI ET FORMALISÉ DES EXIGENCES EN MATIÈRE DE SÉCURITÉ VIS-À-VIS DES SOUS-TRAITANTS INFORMATIQUES DU CENTRE DE COMPÉTENCES SAP

CRITÈRE 1 • Une clause spécifique (contrat ou annexes) est définie pour indiquer les droits, les accès et modalités de contrôles des sous-traitants informatiques du domaine SAP

Commentaires • Critère 1

Les utilisateurs externes peuvent être des sous-traitants, intérimaires, prestataires, stagiaires ou auditeurs externes par exemple.

Le contrôle des accès des utilisateurs externes doit respecter les règles de complexité des mots de passe, la séparation des fonctions entre systèmes, les principes d'accès au système de production (existence d'environnements de développement, de pré-production, de production).

Les modalités de surveillance des accès des sous-traitants doivent être encadrées.

Risques • Critère 1

- Accès non autorisé, frauduleux ou inapproprié des prestataires au système et aux programmes.
- Usurpation d'identité via un compte utilisateur.
- Vol, perte ou altération des données de l'organisation.
- Existence de conflit de séparation des tâches.

Critère spécifique à SAP • Critère 1

Critère spécifique à SAP : NON

Preuves à demander

- Un exemple de contrat en cours entre l'organisation et un sous-traitant et le modèle de contrat dédié (le nombre de preuve à contrôler peut varier selon le périmètre, les risques...).

- La preuve que les utilisateurs externes font l'objet d'une identification claire dans les systèmes, ont des droits d'accès avec des périodes définies et qu'ils sont régulièrement contrôlés.

Bonnes pratiques

- Une clause décrivant les modalités détaillées de clôture du service et de réversibilité a été définie dans le contrat.
- Il y a une revue périodique (au moins annuelle) du contrat avec toutes les parties prenantes.
- La contractualisation d'un Plan d'Assurance Sécurité (PAS) reprend l'ensemble des points liés à la Sécurité des SI et les modalités de pilotage et de contrôles de l'application du PAS.

CRITÈRE 2 • Une clause spécifique (contrat ou annexes) est définie pour indiquer les règles de confidentialité, les moyens de protection des données et les modalités de contrôles des accès sous-traitants informatiques du domaine SAP

Commentaires • Critère 2

Les utilisateurs externes doivent respecter les règles de confidentialité et de protection des données de l'organisation.

Risques • Critère 2

- Accès non autorisé ou frauduleux.
- Vol, perte ou altération des données.

Critère spécifique à SAP • Critère 2

Critère spécifique à SAP : NON

Preuves à demander

- La clause définissant l'ensemble de ces principes liés à la sécurité des données et à la confidentialité.

Bonnes pratiques

- N / A.

CRITÈRE 3 • Des niveaux de qualité et de service sont demandés aux sous-traitants

Commentaires • Critère 3

Les exigences de qualité et de service peuvent être matérialisées par un PAQ (Plan Assurance Qualité), les règles de bonnes pratiques internes à la mise en œuvre d'un projet (SI), et un SLA (Service Level Agreement) décrivant le niveau de service attendu devant être défini et suivi.

Risques • Critère 3

- Arrêt non planifié de l'exploitation.
- Niveau de service insuffisant.

Critère spécifique à SAP • Critère 3

Critère spécifique à SAP : NON

Preuves à demander

- Plan d'Assurance Qualité.
- Service Level Agreement ou contrat de service.

Bonnes pratiques

- Un suivi régulier est réalisé par un responsable en charge du pilotage du sous-traitant. Des indicateurs sont calculés et des plans d'action sont mis en place et suivis lorsque nécessaire.
- Des points de gestion du service externalisé sont faits régulièrement avec le prestataire. Il y a des comptes-rendus systématiques après chaque point de gestion du service.

OBJECTIF DE CONTRÔLE N°5

• L'ORGANISATION A DÉFINI DES MODALITÉS DE CONTRÔLES DE LA GOUVERNANCE DU SYSTÈME SAP

CRITÈRE 1 • Des contrôles sont réalisés afin d'assurer une gestion adéquate des risques liés à SAP

Commentaires • Critère 1

Un processus de contrôle est en place permettant de s'assurer que les risques sont mis à jour régulièrement et que des actions appropriées sont déployées.

Risques • Critère 1

- Arrêt non planifié de l'exploitation.
- Interdépendance des processus qui sont gérés dans le même outil.
- Niveau de service insuffisant.
- Non-respect réglementaire ou légal.
- Accès non autorisé ou frauduleux.
- Vol, perte ou altération des données.

Critère spécifique à SAP • Critère 1

Critère spécifique à SAP : NON

Preuves à demander

- Référentiel de contrôle interne informatique et métier lié à SAP et répondant aux risques identifiés.

Bonnes pratiques

- Les contrôles informatiques suivent les mêmes règles que les contrôles métiers en termes de documentation, d'évaluation et de reporting.
- Un outil informatique de gestion de la gouvernance, des risques et de la conformité permet de documenter le référentiel de contrôle, les campagnes d'évaluation et les actions correctives à mettre en place. Des reportings sont réalisés et communiqués.

CRITÈRE 2 • Des contrôles sont réalisés concernant l'application des directives de la Politique Sécurité du SI (SAP)

Commentaires • Critère 2

À titre d'exemple, il peut s'agir de tests périodiques de non intrusion, tests d'entrées et sorties.

Risques • Critère 2

- Arrêt non planifié de l'exploitation,
- Niveau de service insuffisant.
- Non-respect réglementaire ou légal.
- Accès non autorisé ou frauduleux.
- Vol, perte ou altération des données.

Critère spécifique à SAP • Critère 2

Critère spécifique à SAP : NON

Preuves à demander

- Preuve des contrôles réalisés sur chacun des domaines énoncés.

Bonnes pratiques

- Les contrôles et leurs tests sont documentés au sein d'une application dédiée.

CRITÈRE 3 • Des contrôles sont réalisés afin de s'assurer de l'application des principes en matière de sécurité SAP concernant les sous-traitants informatiques du domaine SAP en particulier

Commentaires • Critère 3

RAS.

Risques • Critère 3

- Arrêt non planifié de l'exploitation,
- Niveau de service insuffisant.
- Non-respect réglementaire ou légal.
- Accès non autorisé ou frauduleux.
- Vol, perte ou altération des données.

Critère spécifique à SAP • Critère 3

Critère spécifique à SAP : NON

Preuves à demander

- Preuve de la réalisation des contrôles.

Bonnes pratiques

- Les contrôles et leurs tests sont documentés au sein d'une application dédiée.

CRITÈRE 4 • Les contrôles en termes de respect des engagements de qualité et de services permettent la mise en œuvre d'un processus d'amélioration continue en matière de sécurité

Commentaires • Critère 4

Le processus d'évaluation des contrôles réalisés et des moyens mis en place doit faire partie d'un processus d'amélioration continue.

Les risques liés au SI étant en permanente évolution, ce processus est donc fondamental pour conserver une couverture optimale des risques informatiques.

Risques • Critère 4

- Arrêt non planifié de l'exploitation.
- Niveau de service insuffisant.
- Non-respect réglementaire ou légal.
- Accès non autorisé ou frauduleux.
- Vol, perte ou altération des données.

Critère spécifique à SAP • Critère 4

Critère spécifique à SAP : NON

Preuves à demander

- Preuve du processus d'amélioration continue et de la prise en compte des risques informatiques et du suivi de la mise en œuvre et de l'efficacité des contrôles clés.

Bonnes pratiques

- L'évaluation des risques résiduels s'appuie sur les tests d'efficacité des contrôles clés au sein des processus majeurs de la fonction SI tels que la gestion de la sécurité logique et physique, gestion de l'exploitation, la gestion des développements, la gestion des changements.

domaine 2. Sécurité des données

DÉFINITION ET PÉRIMÈTRE DU DOMAINE

Ce domaine traite des aspects de protection des données gérées par le système SAP, tant sur les problématiques de confidentialité que d'intégrité.

En effet, par nature et en raison du périmètre fonctionnel couvert et du nombre d'utilisateurs, le système SAP comporte des données sensibles et / ou des données personnelles.

En termes de structure, le domaine est découpé selon les grandes étapes suivantes :

- La définition des besoins métiers en matière de sécurité des données.
- La protection de l'accès aux données.
- Les dispositifs de gestion de la confidentialité des données.
- Les dispositifs de gestion de l'intégrité des données.

Enfin, un point spécifique concerne le respect des obligations règlementaires incombant à l'organisation quand elle doit gérer des données à caractère personnel.

RISQUES ASSOCIÉS

Les principaux risques identifiés sur ce domaine sont :

- L'infraction à la loi.
- L'accès non autorisé au système et aux données qu'il gère.
- La copie non autorisée de données.
- La perte ou l'altération de données.
- La mauvaise identification des besoins métier en matière de protection des données.
- La mise en place de mesures de protection ne permettant pas d'atteindre les besoins métiers exprimés.

OBJECTIF DE CONTRÔLE N°1

• LA CRITICITÉ ET LA SENSIBILITÉ DES DONNÉES SONT RÉGULIÈREMENT ÉVALUÉES

CRITÈRE 1 • Un référentiel de classification des données existe

Commentaires • Critère 1

Le référentiel intègre les objectifs en matière de Disponibilité, d'Intégrité, de Confidentialité et de Traçabilité (DICT).

Ce référentiel inclut notamment l'identification des contraintes réglementaires pesant sur l'organisation et ses données.

De même, les données à caractère personnel sont identifiées.

Risques • Critère 1

- Accès non autorisé ou frauduleux.
- Non-respect réglementaire ou légal.
- Perte de données.
- Perte de traçabilité.
- Vol de données.
- Altération ou perte d'intégrité des données.

Critère spécifique à SAP • Critère 1

Critère spécifique à SAP : NON

Preuves à demander

- Le référentiel de classification et preuve de son utilisation.

Bonnes pratiques

- Le référentiel doit être simple à comprendre, non interprétable, et contenir un nombre réduit de niveaux de classification.

CRITÈRE 2 • Des propriétaires de données sont identifiés

Commentaires • Critère 2

Le propriétaire de données est le représentant du métier qui est responsable de la donnée (vis-à-vis des tiers et des collaborateurs...).

Risques • Critère 2

- Accès non autorisé ou frauduleux.
- Non-respect réglementaire ou légal.
- Perte de données.
- Perte de traçabilité.
- Vol de données.
- Altération ou perte d'intégrité des données.

Critère spécifique à SAP • Critère 2

Critère spécifique à SAP : NON

Preuves à demander

- Lien documenté entre le propriétaire et la donnée (via le dictionnaire des données ou le processus métier considéré).

Bonnes pratiques

- La liste des propriétaires par donnée est publiée et partagée.

CRITÈRE 3 • Les données sont classifiées par les propriétaires sur la base du référentiel

Commentaires • Critère 3

La classification des données est réalisée en application du référentiel et formalisée pour chaque donnée ou groupe de données dans le respect des catégories et criticités des données.

Risques • Critère 3

- Accès non autorisé ou frauduleux.
- Non-respect réglementaire ou légal.
- Perte de données.
- Perte de traçabilité.
- Vol de données.
- Altération ou perte d'intégrité des données.

Critère spécifique à SAP • Critère 3

Critère spécifique à SAP : NON

Preuves à demander

- Classification par criticité des données.

Bonnes pratiques

- La classification des données est validée formellement par le propriétaire. Elle fait l'objet d'une mise à jour régulière.
- Dans SAP, on pourra définir des criticités pour les différentes tables de données.

CRITÈRE 4 • Les données nécessitant un chiffrement sont identifiées

Commentaires • Critère 4

Suite à la classification des données du système SAP, une étape distincte de décision quant au chiffrement éventuel des données peut être conduite.

Risques • Critère 4

- Accès non autorisé ou frauduleux.
- Non-respect réglementaire ou légal.
- Perte de données.
- Perte de traçabilité.
- Vol de données.
- Altération ou perte d'intégrité des données.

Critère spécifique à SAP • Critère 4

Critère spécifique à SAP : NON

Preuves à demander

- Relevé de décision de chiffrer ou non certaines données.

Bonnes pratiques

- La décision de chiffrer ou de ne pas chiffrer est documentée.

OBJECTIF DE CONTRÔLE N°2

• L'ORGANISATION A MIS EN PLACE LES DISPOSITIFS DE PROTECTION DE L'ACCÈS AUX DONNÉES, EN FONCTION DES BESOINS

CRITÈRE 1 • Dans le cas d'accès à SAP via Internet, des pare-feux sont mis en œuvre pour protéger les accès

Commentaires • Critère 1

Des pare-feux ont été installés au niveau de chaque connexion Internet et entre toute zone démilitarisée (DMZ) et la zone de réseau interne.

Risques • Critère 1

- Accès non autorisé ou frauduleux.
- Perte de données.
- Perte de traçabilité.
- Vol de données.
- Altération ou perte d'intégrité des données.

Critère spécifique à SAP • Critère 1

Critère spécifique à SAP : NON

Preuves à demander

- Obtenir la documentation définissant les règles de pare-feu, et vérifier que ces règles sont appliquées.

Bonnes pratiques

- Il est réalisé une évaluation régulière des risques avec mise à jour et maintien au niveau des pratiques diffusées sur les réseaux.

CRITÈRE 2 • La mise en place de SAP Router est effective et sécurisée

Commentaires • Critère 2

Le SAP Router est un dispositif apportant une sécurité supplémentaire pour filtrer les flux atteignant le système SAP.

Risques • Critère 2

- Accès non autorisé ou frauduleux.
- Perte de données.
- Perte de traçabilité.
- Vol de données.
- Altération ou perte d'intégrité des données.

Critère spécifique à SAP • Critère 2

Critère spécifique à SAP : NON

Preuves à demander

- Obtenir et examiner la documentation pour vérifier que les règles de paramétrage du SAP Router sont définies et mises à jour régulièrement.
- Examiner la liste des personnes ayant un accès effectif au SAP Router.

Bonnes pratiques

- SAP Router doit être mis en œuvre dès qu'un accès distant est implémenté.

CRITÈRE 3 • Des dispositifs de détection des intrusions sont associés au filtrage réseau sur les zones permettant l'accès à Internet

Commentaires • Critère 3

En complément des pare-feux, des dispositifs de détection d'intrusion (ou IDS pour Intrusion Detection System) permettent l'identification des cas où la sécurité est contournée et offrent la faculté de protection appropriée en fonction de l'intrusion.

Risques • Critère 3

- Accès non autorisé ou frauduleux.
- Perte de données.
- Perte de traçabilité.
- Vol de données.
- Altération ou perte d'intégrité des données.

Critère spécifique à SAP • Critère 3

Critère spécifique à SAP : NON

Preuves à demander

- Obtenir la preuve des alertes et de leur traitement.

Bonnes pratiques

- RAS.

CRITÈRE 4 • L'accès physique aux données et aux systèmes d'hébergement est restreint de façon appropriée

Commentaires • Critère 4

L'accès aux salles blanches, mais également aux locaux, est restreint aux personnes autorisées.

Risques • Critère 4

- Accès non autorisé ou frauduleux.
- Perte de données.
- Perte de traçabilité.
- Vol de données.
- Altération ou perte d'intégrité des données.

Critère spécifique à SAP • Critère 4

Critère spécifique à SAP : NON

Preuves à demander

- Procédures d'accès et règles d'attribution, notamment pour les salles hébergeant les données, y compris chez les prestataires.
- Journal d'accès à la salle blanche hébergeant les serveurs.

Bonnes pratiques

- RAS.

CRITÈRE 5 • Les interventions en requête des utilisateurs dans les bases de données de production sont interdites. Les interventions des applications externes en interrogation sont autorisées et contrôlées

Commentaires • Critère 5

Les requêtes dans les tables sont parfois laissées libres en production pour compenser les fonctionnalités manquantes.

Dans le cas où les requêtes sont réalisées sous forme de service à la demande au Centre de Compétences, il est nécessaire de demander la procédure qui encadre ce service incluant la vérification que les demandeurs sont bien habilités à réaliser les requêtes.

Risques • Critère 5

- Accès non autorisé ou frauduleux.
- Perte de données.
- Perte de traçabilité.
- Vol de données.
- Altération ou perte d'intégrité des données.

Critère spécifique à SAP • Critère 5

Critère spécifique à SAP : OUI

Preuves à demander

- Justification de l'inactivation des transactions de requêtage (S_TCODE à la valeur SQVI ou à la valeur SQ01).
- Preuve de l'impossibilité de lancer les programmes concernés, car les objets d'autorisations liés (S_QUERY à la valeur 2, 23, 67) ne sont pas attribués.

Bonnes pratiques

- Des requêtes ad hoc sont développées en fonction des besoins exprimés et formalisées, en suivant le processus de gestion des changements.

CRITÈRE 6 • Les interventions en administration des bases de données sont encadrées, tracées et contrôlées

Commentaires • Critère 6

Les utilisateurs techniques ont souvent un rôle critique, avec la possibilité d'interventions sur les bases, et la faculté de s'attribuer des droits.

Risques • Critère 6

- Accès non autorisé ou frauduleux.
- Perte de données.
- Perte de traçabilité.
- Vol de données.
- Altération ou perte d'intégrité des données.

Critère spécifique à SAP • Critère 6

Critère spécifique à SAP : NON

Preuves à demander

- Tables d'accès au Système de gestion de bases de données - SGBD - (journaux).
- Procédures de gestion des bases de données (existence, application et mise à jour).
- Procédures de gestion des logs des bases de données pour les accès par les administrateurs.

Bonnes pratiques

- Avec l'utilisation de SAP, le recours à des Administrateurs de la base de données est exceptionnel, la couche applicative permettant l'ensemble des fonctionnalités de gestion des bases de données. Les cas d'exceptions (création d'index bitmap, réorganisation de tables, modification de paramètre de configuration) doivent être tracés.

CRITÈRE 7 • Les interventions de maintenance sont encadrées, tracées et contrôlées

Commentaires • Critère 7

Pour des raisons de maintenance ou des besoins relatifs au projet, les équipes (clients, intégrateurs, SAP) peuvent être amenées à accéder au système productif (diagnostic d'anomalies en production, opérations sur les données comme dans les fusions de sociétés...). Une procédure doit donc permettre de tracer et de contrôler l'action des intervenants (accès nominatifs, utilisation de SAP GRC Access Control Firefighter / SAP GRC Access Control Emergency Access Management qui tracent toutes les actions réalisées, signature d'engagement de confidentialité...). Les intervenants pouvant être localisés un peu partout sur la planète, cela augmente le risque.

Risques • Critère 7

- Accès non autorisé ou frauduleux.
- Perte de données.
- Perte de traçabilité.
- Vol de données.
- Altération ou perte d'intégrité des données.

Critère spécifique à SAP • Critère 7

Critère spécifique à SAP : NON

Preuves à demander

- Procédures relatives à la maintenance.
- Calendrier des actions programmées.
- Journal des traces.

Bonnes pratiques

- RAS.

OBJECTIF DE CONTRÔLE N°3

• L'ORGANISATION A MIS EN PLACE LES DISPOSITIFS DE PROTECTION DE LA CONFIDENTIALITÉ DES DONNÉES, EN FONCTION DES BESOINS

CRITÈRE 1 • Des dispositifs de gestion des niveaux de confidentialité en accord avec la classification ont été mis en œuvre

Commentaires • Critère 1

On observe généralement différents niveaux en matière de traitement de la confidentialité : de la consultation libre au chiffrement.

Risques • Critère 1

- Accès non autorisé ou frauduleux.
- Vol de données.

Critère spécifique à SAP • Critère 1

Critère spécifique à SAP : NON

Preuves à demander

- Journaux traçant l'utilisation des données jugées les plus sensibles et preuve de l'exploitation de ces journaux.
- Preuves de la mise en place des dispositifs de chiffrement.
- Preuves de l'existence de règles et procédures mises en place.
- Contrôler la correcte définition et la mise en œuvre de règles de gestion des niveaux de confidentialité en fonction des besoins exprimés.

Bonnes pratiques

- RAS.

CRITÈRE 2 • Les dispositifs sont mis à jour périodiquement pour prendre en compte l'évolution des risques et des besoins de confidentialité

Commentaires • Critère 2

Les évolutions des risques et les changements en matière de besoins de sécurité sont à évaluer périodiquement.

Risques • Critère 2

- Accès non autorisé ou frauduleux.
- Vol de données.

Critère spécifique à SAP • Critère 2

Critère spécifique à SAP : NON

Preuves à demander

- Documentation de l'évolution du dispositif.

Bonnes pratiques

- Une mise à jour annuelle est un minimum.

CRITÈRE 3 • La mise en œuvre des dispositifs et leur efficacité sont contrôlées régulièrement

Commentaires • Critère 3

Ces contrôles sont effectués par les équipes métier et leur management, et les actions de correction nécessaires sont entreprises.

Risques • Critère 3

- Accès non autorisé ou frauduleux.
- Vol de données.

Critère spécifique à SAP • Critère 3

Critère spécifique à SAP : NON

Preuves à demander

- Justificatifs de l'organisation et de la réalisation de ces contrôles, ainsi que des éventuels plans d'actions.

Bonnes pratiques

- La périodicité des contrôles est établie en fonction des niveaux de criticité.
- Quel que soit le niveau, une évaluation annuelle peut être considérée comme une bonne pratique.

CRITÈRE 4 • Des actions régulières de sensibilisation sont menées auprès des personnes ayant accès aux données confidentielles

Commentaires • Critère 4

L'objectif est de responsabiliser les acteurs sur les comportements qui pourraient affecter la sécurité des données confidentielles.

Risques • Critère 4

- Accès non autorisé ou frauduleux.
- Vol de données.

Critère spécifique à SAP • Critère 4

Critère spécifique à SAP : NON

Preuves à demander

- Preuve des actions de sensibilisation (formation, mails, courriers d'engagement...).

Bonnes pratiques

- Une charte existe et est diffusée.
- Un engagement formel à la respecter est consigné.

CRITÈRE 5 • L'interdiction de l'utilisation des données de production confidentielles dans d'autres environnements est mise en place

Commentaires • Critère 5

Les environnements non productifs n'offrent généralement pas le même niveau de sécurité des données.

Risques • Critère 5

- Accès non autorisé ou frauduleux.
- Vol de données.

Critère spécifique à SAP • Critère 5

Critère spécifique à SAP : NON

Preuves à demander

- Procédures de mise à disposition des données sur les environnements non productifs ou évaluation des niveaux de sécurité des environnements non productifs.

Bonnes pratiques

- Des outils d'anonymisation des données sont utilisés pour alimenter les environnements non productifs à partir des données de production.

CRITÈRE 6 • Un processus de destruction sécurisé des données obsolètes existe et est déployé

Commentaires • Critère 6

Cela est particulièrement sensible sur les supports externes de stockage (cartouches, CD / DVD, disques externes...).

Risques • Critère 6

- Accès non autorisé ou frauduleux.
- Vol de données.

Critère spécifique à SAP • Critère 6

Critère spécifique à SAP : NON

Preuves à demander

- Procédures de destruction des données et compte rendu de la dernière destruction des données.
- Le cas échéant, preuve du processus d'aliénation des matériels ou consommables ayant servi au stockage des données.

Bonnes pratiques

- RAS.

OBJECTIF DE CONTRÔLE N°4

• L'ORGANISATION A MIS EN PLACE LES DISPOSITIFS DE PROTECTION DE L'INTÉGRITÉ DES DONNÉES, EN FONCTION DES BESOINS

CRITÈRE 1 • Des dispositifs de conservation de l'intégrité des données ont été mis en œuvre en correspondance avec les besoins d'intégrité définis

Commentaires • Critère 1

Les accès en modification et en suppression sont attribués aux seules personnes habilitées. Par ailleurs, des journaux tracent toute modification / suppression de données, selon un paramétrage propre à SAP.

Ces journaux sont exploités régulièrement et les corrections nécessaires effectuées.

Risques • Critère 1

- Accès non autorisé ou frauduleux.
- Perte de traçabilité.
- Altération ou perte d'intégrité des données.

Critère spécifique à SAP • Critère 1

Critère spécifique à SAP : OUI

Preuves à demander

- Matrice des droits d'accès aux données et transactions.
- Existence de la mise en œuvre de journaux sur les tables (programme RDDPRCHK et paramètre REC / Client pour les tables mandant-dépendantes) et preuve de leur exploitation.

Bonnes pratiques

- Le paramétrage des journaux proposés par SAP est adapté au besoin de l'organisation et ne se limite pas au paramétrage standard.

CRITÈRE 2 • Les dispositifs sont mis à jour périodiquement pour prendre en compte l'évolution des risques et des besoins d'intégrité

Commentaires • Critère 2

Les évolutions des risques et les changements en matière de besoins de sécurité sont à évaluer périodiquement.

Risques • Critère 2

- Accès non autorisé ou frauduleux.
- Perte de traçabilité.
- Altération ou perte d'intégrité des données.

Critère spécifique à SAP • Critère 2

Critère spécifique à SAP : NON

Preuves à demander

- Documentation de l'évolution du dispositif.

Bonnes pratiques

- Une mise à jour annuelle est un minimum.

CRITÈRE 3 • La mise en œuvre des dispositifs et leur efficacité sont contrôlées régulièrement

Commentaires • Critère 3

Ces contrôles sont effectués par les équipes opérationnelles et leur management, et les actions de correction nécessaires sont entreprises.

Risques • Critère 3

- Accès non autorisé ou frauduleux.
- Perte de traçabilité.
- Altération ou perte d'intégrité des données.

Critère spécifique à SAP • Critère 3

Critère spécifique à SAP : NON

Preuves à demander

- Justificatifs de l'organisation et de la réalisation de ces contrôles, ainsi que des éventuels plans d'actions.

Bonnes pratiques

- La périodicité des contrôles est établie en fonction des niveaux de criticité.
- Quel que soit le niveau, une évaluation annuelle peut être considérée comme une bonne pratique.

CRITÈRE 4 • L'intégrité des journaux de modification de données est assurée

Commentaires • Critère 4

Les actions exécutées par tout utilisateur avec des droits étendus (SAP ALL ou administrateur) sont consignées.

Risques • Critère 4

- Accès non autorisé ou frauduleux.
- Perte de traçabilité.
- Altération ou perte d'intégrité des données.

Critère spécifique à SAP • Critère 4

Critère spécifique à SAP : NON

Preuves à demander

- Vérification de l'existence d'un dispositif de sécurisation des journaux.

Bonnes pratiques

- Un enregistrement des journaux sur un serveur distinct sécurisé est réalisé pour éviter la possibilité de modification par un utilisateur ayant des droits étendus sur le serveur d'origine.

OBJECTIF DE CONTRÔLE N°5

• L'ORGANISATION A MIS EN PLACE LES DISPOSITIFS POUR RESPECTER LA RÉGLEMENTATION EN MATIÈRE DE DONNÉES PERSONNELLES

CRITÈRE 1 • La réglementation en matière de protection des données personnelles hébergées sur SAP est connue

Commentaires • Critère 1

Les obligations touchent notamment à la déclaration, l'acceptation, la mise à disposition, la conservation (...) en ce qui concerne les données et aux différentes procédures associées à mettre en œuvre (déclaration d'incidents, évaluation des dispositifs...).

NB : La règlementation européenne s'appliquerait à partir de 2014 pour l'ensemble de la population européenne, quel que soit le lieu d'hébergement des données. Pour les autres populations, des règlementations locales peuvent s'appliquer.

Risques • Critère 1

- Non-respect des exigences réglementaires ou légales.

Critère spécifique à SAP • Critère 1

Critère spécifique à SAP : NON

Preuves à demander

- Une organisation est en place pour suivre les évolutions de la réglementation en matière de données personnelles.

Bonnes pratiques

- Il existe dans l'organisation un correspondant informatique et liberté ou un Délégué à la protection des données personnelles.

CRITÈRE 2 • La réglementation en matière de protection des données à caractère personnel hébergées sur SAP est appliquée.

Commentaires • Critère 2

Les différentes obligations touchent notamment à la Déclaration, l'Acceptation, la Mise à disposition, la Conservation... en ce qui concerne les données et aux différentes procédures associées à mettre en œuvre (déclaration d'incidents, évaluation des dispositifs...).

NB : La règlementation européenne s'appliquerait à partir de 2014 pour l'ensemble de la population européenne, quel que soit le lieu d'hébergement des données. Pour les autres populations, des règlementations locales peuvent s'appliquer.

Risques • Critère 2

- Non-respect règlementaire ou légal.

Critère spécifique à SAP • Critère 2

Critère spécifique à SAP : NON

Preuves à demander

- Déclaration de fichiers et de traitements.
- Procédures de gestion documentées y compris les modalités d'information des personnes faisant l'objet de traitement de données à caractère personnel et les dispositions mise en œuvre pour leur permettre d'exercer leur droit (opposition, rectification...).

Bonnes pratiques

- RAS.

CRITÈRE 3 • Le respect de la règlementation en matière de protection des données personnelles hébergées sur SAP est vérifié.

Commentaires • Critère 3

Ces contrôles sont effectués par des équipes internes pour s'assurer de la mise en œuvre des dispositifs permettant le respect de la règlementation. Les actions de correction nécessaires sont entreprises.

Risques • Critère 3

- Non-respect réglementaire ou légal.

Critère spécifique à SAP • Critère 3

Critère spécifique à SAP : NON

Preuves à demander

- Justificatifs de l'organisation, de la réalisation de ces contrôles et des éventuels plans d'actions.

Bonnes pratiques

- Les traitements de données à caractère personnel sont listés de manière exhaustive et de manière informatisée.

domaine 3. Gestion des accès et habilitations

DÉFINITION ET PÉRIMÈTRE DU DOMAINE

Ce domaine concerne quatre aspects relatifs à l'accès, la gestion et l'affectation des rôles aux différents types utilisateurs du système SAP :

- La gestion globale des mots de passe (politique, structuration, sécurité, etc).
- La gestion des comptes utilisateurs en définissant les règles associées (nommage, création, compte d'utilisateurs externes à l'entreprise, comptes spécifiques et techniques avec des droits étendus).
- La gestion des rôles utilisateurs et leur processus d'affectation aux utilisateurs. On peut également parler de gestion des habilitations des utilisateurs.
- Les aspects liés à la sécurité des accès et rôles utilisateurs (surveillance et pilotage).

RISQUES ASSOCIÉS

Les principaux risques identifiés sur ce domaine sont :

- Une robustesse insuffisante de la protection par mot de passe.
- L'accès non autorisé à des informations protégées, et les modifications inappropriées de valeurs de données.
- L'utilisation frauduleuse de fonctionnalités.
- L'usurpation d'identités.
- La perte de traçabilité des opérations rendant impossible l'identification de l'auteur des actions réalisées dans le système SAP (destruction de preuves).
- La déresponsabilisation des utilisateurs.
- Des dépenses non justifiées.

OBJECTIF DE CONTRÔLE N°1

• L'ORGANISATION A DÉFINI DES MOYENS AFIN DE SÉCURISER LES ACCÈS AU SYSTÈME (ENVIRONNEMENT DE PRODUCTION)

CRITÈRE 1 • Les paramètres généraux de sécurité sont définis dans les directives de la Politique de Sécurité des Systèmes d'Information (PSSI) du groupe

Commentaires • Critère 1

S'il n'y a pas de directive Sécurité dédiée à SAP, il s'agit de mettre en œuvre les recommandations générales de l'entreprise sur le sujet.

Risques • Critère 1

- Accès non autorisé ou frauduleux.
- Usurpation d'identité.
- Vol de données.
- Perte d'image.

Critère spécifique à SAP • Critère 1

Critère spécifique à SAP : NON

Preuves à demander

- Politique Sécurité SI du groupe et les directives associées.

CRITÈRE 2 • Des critères de complexité des mots de passe (y compris la longueur) ont été mis en place et sont conformes à la PSSI

Commentaires • Critère 2

- Nombre minimal de caractères dans un mot de passe = X (X conforme à la PSSI).
- Nombre minimum de chiffres constituant le mot de passe = Y (Y conforme à la PSSI).

- Nombre minimum de lettres constituant le mot de passe = Z (Z conforme à la PSSI).
- Une liste des mots de passe interdits a été paramétrée.

Risques • Critère 2

- Accès non autorisé ou frauduleux.
- Usurpation d'identité.
- Vol de données.
- Perte d'image.

Critère spécifique à SAP • Critère 2

Critère spécifique à SAP : OUI

Preuves à demander

- Demander aux audités d'extraire de la table RSPARAM (nom technique de la table SAP) et y vérifier les lignes suivantes en fonction de la politique sécurité du système d'information (PSSI) :
  - login / min_password_lng = X (Nombre minimal de caractères).
  - login / min_password_digits = Y (Nombre minimal de chiffres).
  - login / min_password_letters = Z (Nombre minimal de lettres).

CRITÈRE 3 • La fréquence de changement du mot de passe a été définie et est contrôlée

Commentaires • Critère 3

Délai de validité des mots de passe (en jours) = X (X conforme à la PSSI).

Risques • Critère 3

- Accès non autorisé ou frauduleux.
- Usurpation d'identité.
- Vol de données.
- Perte d'image.

Critère spécifique à SAP • Critère 3

Critère spécifique à SAP : OUI

Preuves à demander

- Demander aux audités d'extraire de la table RSPARAM (nom technique de la table SAP) et vérifier les lignes suivantes :
  - login / disable_multi_gui_login = 1 (multi login non autorisé).
  - login / multi_login_users = Users (liste des comptes autorisés à un login multiple).
  - login / failed_user_auto_unlock = 0 (nombre de connexion avant blocage du compte).
  - login / no_automatic_user_sapstar = 1 (re-création automatique du compte SAP*).

CRITÈRE 4 • La réutilisation du mot de passe a été définie et est appliquée

Commentaires • Critère 4

Nombre de mots de passe à enregistrer dans l'historique = X (X conforme à la PSSI).

Risques • Critère 4

- Accès non autorisé ou frauduleux.
- Usurpation d'identité.
- Vol de données.
- Perte d'image.

Critère spécifique à SAP • Critère 4

Critère spécifique à SAP : OUI

Preuves à demander

- Demander aux audités d'extraire de la table RSPARAM (nom technique de la table SAP) et y vérifier la ligne suivante : login / password_history_size = X.

CRITÈRE 5 • Les règles de blocages / déblocages des comptes ont été définies et sont conformes à la PPSI Groupe

Commentaires • Critère 5

- Les paramètres SAP à vérifier sont les suivants :
  - Nombre de tentatives de connexion avant fermeture de session = X (X conforme à la PSSI).
  - Nombre de tentatives avant verrouillage de l'utilisateur = Y (Y conforme à la PSSI).
  - Déverrouillage automatique à minuit d'un utilisateur verrouillé = 0.
  - Délai d'inactivité avant déconnexion (en sec.) = Z (Z conforme à la PSSI).
- Règles de déblocage : bien identifier l'utilisateur à débloquer et vérifier que ce n'est pas toujours le même utilisateur.

Risques • Critère 5

- Accès non autorisé ou frauduleux.
- Usurpation d'identité.
- Vol de données.
- Perte d'image.

Critère spécifique à SAP • Critère 5

Critère spécifique à SAP : OUI

Preuves à demander

- Demander aux audités d'extraire de la table RSPARAM (nom technique de la table SAP) et y vérifier les lignes suivantes :
  - login / fails_to_session_end = X (tentatives de connexion avant fermeture de session).
  - login / fails_to_user_lock = Y (tentatives de connexion avant verrouillage de l'utilisateur).
  - login / failed_user_auto_unlock = 0 (Déverrouillage automatique à minuit d'un utilisateur verrouillé).
  - rdisp / gui_auto_logout = Z (Délai d'inactivité avant déconnexion).
- Procédure de déblocage des comptes.

CRITÈRE 6 • Les conditions de communication des mots de passe (initiaux et renouvelés) sont sécurisées

Commentaires • Critère 6

Communication restreinte à l'utilisateur.

Risques • Critère 6

- Accès non autorisé ou frauduleux.
- Usurpation d'identité.
- Vol de données.
- Perte d'image.

Critère spécifique à SAP • Critère 6

Critère spécifique à SAP : NON

Preuves à demander

- Procédure de gestion des mots de passe.
- Preuve que la communication à l'utilisateur, de son identifiant et de son mot de passe, se fait par des canaux différents.

CRITÈRE 7 • Les autres paramètres généraux de sécurité SAP sont conformes aux directives de sécurité de la PSSI du groupe et sont appliqués

Commentaires • Critère 7

- Interdiction de connexions multiples avec le même compte.
- Liste des comptes utilisateur autorisés aux connections multiples avec le même compte = Users XX.
- Désactivation du contrôle des droits d'accès = 0.
- Recréation automatique du compte SAP* = 1.

Risques • Critère 7

- Accès non autorisé ou frauduleux.
- Usurpation d'identité.
- Vol de données.
- Perte de traçabilité.
- Perte d'image.

Critère spécifique à SAP • Critère 7

Critère spécifique à SAP : OUI

Preuves à demander

- Demander aux audités d'extraire de la table RSPARAM (nom technique de la table SAP) et y vérifier les lignes suivantes :
  - login / disable_multi_gui_login = 1
    (Interdiction de connexions multiples).
  - login / multi_login_users = Users
    (Liste des comptes utilisateur autorisés aux connexions multiples).
  - login / failed_user_auto_unlock = 0
    (Désactivation du contrôle des droits d'accès).
  - login / no_automatic_user_sapstar = 1
    (Recréation automatique du compte SAP*).

OBJECTIF DE CONTRÔLE N°2

• LA GESTION DES ACCÈS UTILISATEURS A ÉTÉ FORMELLEMENT DÉFINIE

CRITÈRE 1 • Un processus de gestion (création, modification, suppression) des comptes utilisateurs métier est défini

Commentaires • Critère 1

Vérifier que le processus comprend la validation formelle avant la création. Seuls les utilisateurs habilités peuvent valider la création d'un compte utilisateur.

Risques • Critère 1

- Accès non autorisé ou frauduleux.
- Usurpation d'identité.
- Perte d'image.

Critère spécifique à SAP • Critère 1

Critère spécifique à SAP : NON

Preuves à demander

- Procédure de gestion des comptes utilisateurs.
- Liste des personnes habilitées à valider la création / modification d'un utilisateur.
- Sur un échantillon de création, modification, suppression, vérifier que la procédure a bien été appliquée (notamment obtenir la preuve de la validation).
- Comprendre les procédures de dérogations si elles sont admises. Les preuves de la correcte application de ces procédures sont également à demander.

Bonnes pratiques

- La procédure de gestion des utilisateurs est formalisée et appliquée, ce processus est interconnecté avec un processus RH.

CRITÈRE 2 • Les comptes utilisateurs sont nominatifs et uniques. Il existe des règles de nommage des utilisateurs

Commentaires • Critère 2

Vérifier la conformité entre la règle en vigueur et les utilisateurs existants dans le système. Vérifier qu'on identifie et supprime les doublons. S'il y a des exceptions, des dérogations doivent être formalisées.

Risques • Critère 2

- Accès non autorisé ou frauduleux.
- Usurpation d'identité.
- Vol de données.

Critère spécifique à SAP • Critère 2

Critère spécifique à SAP : NON

Preuves à demander

- Extraction de la table des utilisateurs.

Bonnes pratiques

- Le nommage des comptes des prestataires (et autres personnels extérieurs) est spécifique (exemple : Nom-ext).

CRITÈRE 3 • Il existe des règles de séparation des fonctions au sein du processus de gestion de création / modification des comptes et d'affectation des droits

Commentaires • Critère 3

Le demandeur doit être différent de l'approbateur, différent du créateur du compte et différent de la personne qui affecte les droits.

Risques • Critère 3

- Accès non autorisé ou frauduleux.
- Vol de données.
- Perte de données.

Critère spécifique à SAP • Critère 3

Critère spécifique à SAP : NON

Preuves à demander

- Sur un échantillon de création, modification et suppression, vérifier que le demandeur est différent de l'approbateur, différent du créateur du compte et différent de la personne qui affecte les droits.

Bonnes pratiques

- La procédure de gestion des utilisateurs est formalisée et appliquée.

CRITÈRE 4 • Une attention particulière est portée à la gestion des comptes des prestataires, intérimaires ou toute personne non collaborateur

Commentaires • Critère 4

Ce critère est également présent dans le domaine Gouvernance : Objectif de contrôle n°4.

Risques • Critère 4

- Accès non autorisé ou frauduleux.
- Usurpation d'identité.
- Vol de données.
- Perte de données.
- Perte d'image.

Critère spécifique à SAP • Critère 4

Critère spécifique à SAP : NON

Preuves à demander

- La procédure de gestion des utilisateurs (en particulier le passage concernant les personnes externes).

Bonnes pratiques

- La procédure de gestion des utilisateurs comprend la gestion des comptes des personnes externes et notamment une revue spécifique des droits qui leurs sont attribués.
- Les comptes des personnes externes ont une date de fin de contrat définie (ou date de fin de validité des accès).

OBJECTIF DE CONTRÔLE N°3

• UNE SURVEILLANCE ET UN PILOTAGE DE LA SÉCURITÉ DES ACCÈS SONT EN PLACE

CRITÈRE 1 • Il existe des revues des utilisateurs actifs

Commentaires • Critère 1

Régulièrement, des contrôles sont effectués pour vérifier que tous les accès identifiés sont bien actifs.

Risques • Critère 1

- Accès non autorisé ou frauduleux.
- Usurpation d'identité.

Critère spécifique à SAP • Critère 1

Critère spécifique à SAP : NON

Preuves à demander

- Comparaison avec les listes RH pour vérifier que les utilisateurs (collaborateurs de l'entreprise) sont toujours salariés.
- Pour les utilisateurs externes, le contrat de prestation pourra être demandé.

Bonnes pratiques

- Des contrôles périodiques sont réalisés une interface entre le SIRH et SAP permet d'automatiser ces revues pour les utilisateurs internes a minima.

CRITÈRE 2 • Une revue des utilisateurs inactifs est réalisée

Commentaires • Critère 2

Optimisation des licences.

Risques • Critère 2

- Non maîtrise des dépenses.

Critère spécifique à SAP • Critère 2

Critère spécifique à SAP : OUI

Preuves à demander

- Liste des utilisateurs SAP ne s'étant pas connectés depuis plus de 3 mois.

Bonnes pratiques

- Après examen de l'opportunité, il est effectué une redistribution de la licence à un autre utilisateur pour optimiser le parc de licences SAP.
- Il existe des procédures de licences managements et de Software Asset Management.

CRITÈRE 3 • Un contrôle des utilisateurs ayant plusieurs comptes est réalisé

Commentaires • Critère 3

Il s'agit de la gestion des doublons d'utilisateurs.

Risques • Critère 3

- Accès non autorisé ou frauduleux.
- Usurpation d'identité.
- Vol de données.
- Non maîtrise des dépenses.

Critère spécifique à SAP • Critère 3

Critère spécifique à SAP : OUI

Preuves à demander

- Extraction des utilisateurs et identification des éventuels doublons.

Bonnes pratiques

- Il est réalisé des contrôles périodiques des utilisateurs qui auraient plusieurs accès à SAP.

CRITÈRE 4 • Les outils d'extractions de traces (permettant d'identifier les pistes d'audits) des modifications de comptes existent et sont utilisés

Commentaires • Critère 4

Il existe des revues de traces (ou log) pour vérifier que le processus a bien été mis en œuvre (séparation des fonctions, dates de modification, ajouts de profils puis suppressions, suppressions de comptes).

Risques • Critère 4

- Accès non autorisé ou frauduleux.
- Usurpation d'identité.

Critère spécifique à SAP • Critère 4

Critère spécifique à SAP : OUI

Preuves à demander

- Conclusions de la revue.

Bonnes pratiques

- Il est réalisé une sélection automatisée des utilisateurs ayant fait l'objet de modifications de comptes.

OBJECTIF DE CONTRÔLE N°4

• L'ORGANISATION A MIS EN PLACE UNE GESTION DES TYPOLOGIES DES COMPTES (SYSTÈME, SERVICE, DIALOGUE)

CRITÈRE 1 • La cartographie des comptes utilisateurs Système et Service existe et est maintenue

Commentaires • Critère 1

Liste des utilisateurs avec leur typologie ainsi que les différents cas et modalités d'utilisation.

Risques • Critère 1

- Accès non autorisé ou frauduleux.
- Usurpation d'identité.

Critère spécifique à SAP • Critère 1

Critère spécifique à SAP : OUI

Preuves à demander

- Cartographie à jour (avec extraction des comptes de types Services et Systèmes pour comparaison) avec le lien usage et rôles attribués.

Bonnes pratiques

- Le blocage des comptes inutilisés est effectué régulièrement.
- Il existe des règles de nommage par typologie et usage (interface, Remote Function Call...).
- Une attention particulière est portée aux comptes de type Service (double accès par dialogue et usage technique).

CRITÈRE 2 • Les mots de passe des comptes de Service ont un niveau de sécurité élevé (mise sous séquestre et avec un mot de passe spécifique)

Commentaires • Critère 2

Comptes Services avec SAP_ALL (comptes à droits étendus) nécessaire aux activités techniques.

Risques • Critère 2

- Accès non autorisé ou frauduleux.
- Perte de traçabilité.

Critère spécifique à SAP • Critère 2

Critère spécifique à SAP : OUI

Preuves à demander

- Procédure de gestion et de séquestre des mots de passes des comptes Services.

Bonnes pratiques

- Il existe un processus de gestion des mots de passe avec une utilisation unique, qui sont conservés dans un coffre-fort et que seules certaines personnes sont habilitées à récupérer.
- Les administrateurs sécurité du système sont responsables de ces comptes.

CRITÈRE 3 • Des revues des comptes utilisateurs de type Service ou Système sont réalisées

Commentaires • Critère 3

Vérifier que tous les comptes utilisateurs Systèmes et Services sont bien exploités conformément à la cartographie définie.

Risques • Critère 3

- Accès non autorisé ou frauduleux.
- Usurpation d'identité.
- Vol de données.

Critère spécifique à SAP • Critère 3

Critère spécifique à SAP : OUI

Preuves à demander

- Procédure de revue et trace des revues effectuées.

Bonnes pratiques

- Des revues trimestrielles sont réalisées.
- Les administrateurs sécurité du système sont responsables de ces comptes.

OBJECTIF DE CONTRÔLE N°5

• L'ORGANISATION A MIS EN PLACE DES MODALITÉS DE GESTION DES COMPTES SI

CRITÈRE 1 • Il existe une procédure pour sécuriser les comptes Editeurs SAP (comptes créés en standard lors de l'installation et nécessaires en cas d'intervention de SAP)

Commentaires • Critère 1

Vérifier qu'il existe une procédure pour sécuriser la gestion de ces comptes.

Risques • Critère 1

• Perte de traçabilité.

Critère spécifique à SAP • Critère 1

Critère spécifique à SAP : OUI

Preuves à demander

• Procédure de gestion des comptes SI dédiés à l'accès par l'éditeur.

Bonnes pratiques

• Les mots de passe initiaux de ces comptes sont modifiés.

CRITÈRE 2 • Les comptes utilisateurs à droits étendus (SAP_ALL & SAP_NEW) ne sont utilisés qu'en cas de crise (un seul compte avec un mot de passe secret)

Commentaires • Critère 2

Vérifier qu'il y a une définition des cas de crise.

Risques • Critère 2

- Accès non autorisé ou frauduleux.
- Usurpation d'identité.
- Vol de données.

Critère spécifique à SAP • Critère 2

Critère spécifique à SAP : OUI

Preuves à demander

- Demander l'extraction des logs des connexions pour vérifier qu'on est bien dans les cas de crise (comparaison entre les crises et la fréquence d'utilisation réelle de ces comptes).

Bonnes pratiques

- L'usages de ces comptes à droits étendus sont limités aux situations de crise et la trace des utilisations est conservée.

CRITÈRE 3 • Les RACIs par population et par environnement technique sont pris en compte dans la mise en œuvre des autorisations

Commentaires • Critère 3

À titre d'exemple, les développeurs ne doivent pas avoir accès à la plate-forme de production.

Risques • Critère 3

- Accès non autorisé ou frauduleux.
- Vol de données.

Critère spécifique à SAP • Critère 3

Critère spécifique à SAP : NON

Preuves à demander

- Matrice RACI.

Bonnes pratiques

- Les développeurs ne sont pas autorisés à accéder à l'environnement de production.
- L'assistance aux utilisateurs ne doit pas avoir accès aux données utilisateurs en modification, idem pour les prestataires.

CRITÈRE 4 • Une revue périodique des populations techniques (utilisateurs du service informatique et équivalents) est réalisée

Commentaires • Critère 4

Suivi des utilisateurs techniques à risque.

Risques • Critère 4

- Accès non autorisé ou frauduleux.
- Vol de données.

Critère spécifique à SAP • Critère 4

Critère spécifique à SAP : NON

Preuves à demander

- Conclusions de la revue des comptes techniques pour s'assurer que les traitements réalisés sont conformes et justifiés.

Bonnes pratiques

- Des contrôles périodiques sont réalisés en tenant compte des populations internes et externes.

OBJECTIF DE CONTRÔLE N°6

• LE PROCESSUS DE GESTION DES RÔLES EST SOUS CONTRÔLE

CRITÈRE 1 • Un processus de gestion (création, modification, suppression) des rôles est défini

Commentaires • Critère 1

La gestion des rôles (ensemble de transactions affectées à une fonction dans l'organisation) doit suivre un processus documenté.

Risques • Critère 1

- Accès non autorisé ou frauduleux.

Critère spécifique à SAP • Critère 1

Critère spécifique à SAP : NON

Preuves à demander

- Procédure de gestion des rôles et preuve de la mise en œuvre opérationnelle.

Bonnes pratiques

- Dans cette procédure, il est indiqué que la modification des rôles doit suivre le processus de gestion des changements (notamment, les rôles ne doivent pas être modifiés en environnement de production) et doivent respecter la matrice de séparation des tâches définie.
- Une revue régulière des rôles est prévue et réalisée.
- Une convention de nommage des rôles permet d'identifier de façon claire les rôles techniques, métiers, et les différents niveaux de rôles.

CRITÈRE 2 • Il existe un référentiel des rôles avec des axes organisationnels. Ce référentiel est mis à jour régulièrement

Commentaires • Critère 2

Exemple : Faire une utilisation appropriée des variantes de rôles (simples / composites / dérivés) et faire le lien avec la séparation des fonctions.

La notion de structure organisationnelle permet de restreindre les rôles sur des périmètres de management définis en fonction de l'organisation.

Risques • Critère 2

- Accès non autorisé, insuffisamment limité en terme de périmètre, ou frauduleux.

Critère spécifique à SAP • Critère 2

Critère spécifique à SAP : OUI

Preuves à demander

- Le Référentiel des rôles avec les axes d'organisationnels et preuve de la mise à jour.

Bonnes pratiques

- Le référentiel est mis à jour régulièrement, en fonction des changements d'organisation.
- Une revue régulière des rôles est prévue et réalisée.
- Une convention de nommage des rôles permet d'identifier de façon claire les rôles techniques, métiers, et les différents niveaux de rôles.

CRITÈRE 3 • Les passe-droits possibles dans le standard SAP sont connus et correctement gérés

Commentaires • Critère 3

Vérifier que l'utilisation de « SAP edit », du mode « debug » est bien sécurisé qui permettent de réaliser des opérations directement au sein des programmes et des tables.

Risques • Critère 3

- Accès non autorisé ou frauduleux.
- Perte de données.
- Vol de données.

Critère spécifique à SAP • Critère 3

Critère spécifique à SAP : OUI

Preuves à demander

- Preuve que « SAP edit » est désactivé (demander à un utilisateur ayant des accès privilégiés de taper sap_edit ou / h pour vérifier qu'il n'y a pas d'accès).

Bonnes pratiques

- En production, il est utile de vérifier que ces passes droits sont désactivés.

CRITÈRE 4 • La traçabilité de la gestion des rôles est assurée

Commentaires • Critère 4

La traçabilité des actions effectuées sur les rôles est assurée (ajout / suppression d'une transaction).

Risques • Critère 4

- Accès non autorisé ou frauduleux.
- Perte de traçabilité.

Critère spécifique à SAP • Critère 4

Critère spécifique à SAP : OUI

Preuves à demander

- Historique des logs : revues des ajouts et suppressions de transactions au sein des rôles.

Bonnes pratiques

- Il est effectué une revue régulière des logs de gestion des rôles.

OBJECTIF DE CONTRÔLE N°7

• L'AFFECTATION DES RÔLES EST MAITRISÉE

CRITÈRE 1 • Le processus d'affectation des rôles respecte les règles de séparation des tâches

Commentaires • Critère 1

La personne qui gère les rôles en création / modification / suppression est différente de la personne qui affecte ces droits aux utilisateurs.

Risques • Critère 1

• Accès non autorisé ou frauduleux.

Critère spécifique à SAP • Critère 1

Critère spécifique à SAP : NON

Preuves à demander

• Demander la procédure d'affectation des rôles.

Bonnes pratiques

• RAS.

CRITÈRE 2 • La traçabilité des actions liées à l'affectation des rôles est assurée et les logs sont revus

Commentaires • Critère 2

La vérification des logs par les opérationnels ne peut généralement pas être exhaustive en raison des volumes liés.

Risques • Critère 2

• Accès non autorisé ou frauduleux.

• Perte de traçabilité.

Critère spécifique à SAP • Critère 2

Critère spécifique à SAP : OUI

Preuves à demander

- Résultats du contrôle des logs.

Bonnes pratiques

- Il est effectué une revue régulière des logs.

CRITÈRE 3 • Les actions effectuées par les administrateurs des droits sont contrôlées via une revue régulière

Commentaires • Critère 3

Par exemple, revue des actions effectuées par la(es) personnes(s) en charge de l'affectation des droits afin de s'assurer qu'elles ne se sont pas auto-affectées des droits.

Risques • Critère 3

- Accès non autorisé ou frauduleux.
- Perte de données.
- Vol de données.

Critère spécifique à SAP • Critère 3

Critère spécifique à SAP : OUI

Preuves à demander

- Preuve de la revue des logs par échantillon.

Bonnes pratiques

- Il est effectué une revue régulière des logs par échantillon.

---

domaine 4. Séparation des fonctions

DÉFINITION ET PÉRIMÈTRE DU DOMAINE

L'un des principes du contrôle interne est la mise en place de règles de séparation des fonctions.

Ce principe a notamment pour objectif d'éviter qu'un même agent cumule des tâches qui lui permettraient de réaliser un processus de bout en bout sans intervention et contrôle d'un tiers.

Il s'agit d'éviter les erreurs, les négligences, les fraudes et leur dissimulation.

De fait, il convient de déployer ce principe de séparation des fonctions au sein des processus métiers et notamment ceux supportés par SAP. Néanmoins, il est à noter que la séparation des fonctions au sein de SAP est un sujet techniquement complexe pour les raisons suivantes :

- Il existe plusieurs milliers de transactions SAP, qui couvrent l'ensemble des processus métiers de l'entreprise ;
- À cela, il faut ajouter les transactions spécifiquement développées par l'entreprise ;
- Plusieurs filiales ou entités d'un même groupe peuvent être hébergées sur le même serveur générant des risques d'étanchéité organisationnelle ;
- Le paramétrage de la sécurité dans SAP est très fin et par conséquent très difficile à maintenir.

RISQUES ASSOCIÉS

- Cumul de tâches incompatibles conduisant aux des risques d'erreurs, de négligences, de fraudes.
- Accès non autorisé ou frauduleux aux systèmes et programmes.

OBJECTIF DE CONTRÔLE N°1

• L'ORGANISATION A DÉFINI UNE MATRICE DE SÉPARATION DES FONCTIONS VALIDÉE PAR LE MANAGEMENT

CRITÈRE 1 • La matrice de séparation des fonctions a été validée par le management et a été adaptée aux spécificités métier de l'entité

Une matrice de séparation des fonctions est un référentiel des transactions sensibles par utilisateurs afin de mettre en avant les problématique de transactions incompatibles au regard des métiers.

Commentaires • Critère 1

Tous les principaux référentiels de contrôle interne (COSO, COCO, Turnbull, CDR, AMF, etc) mentionnent l'importance de la « séparation des fonctions » au sein des processus opérationnels et financiers.

Ils accordent une attention particulière aux activités de contrôle dédiées aux systèmes d'information.

Risques • Critère 1

- Accès non autorisé ou frauduleux.

Critère spécifique à SAP • Critère 1

Critère spécifique à SAP : NON

Preuves à demander

- Obtenir la matrice et sa description.
- Obtenir la preuve de la validation de cette matrice par le management (directions utilisatrices).
- Demander la procédure de revue de la matrice, vérifier son approbation, sa mise à jour, son application et sa périodicité.
- Obtenir la preuve de la communication de la matrice de séparation des fonctions au niveau de la mise en œuvre entre les métiers (chef de service) et les responsables de la séparation des fonctions.

Bonnes pratiques

- Les matrices sont être mises à jour de manière régulière.
- Les directions métiers doivent être toutes impliquées dans ce processus d'approbation.

CRITÈRE 2 • La matrice de séparation des fonctions a été adaptée à l'environnement SAP

Commentaires • Critère 2

Chaque fonction de la matrice doit regrouper les transactions correspondantes (ex. création d'une facture, modification d'une facture).

Un conflit peut correspondre par exemple à :

- la capacité de créer un fournisseur, d'enregistrer une facture et de payer cette facture,
- la modification de la rémunération et la validation de cette rémunération.

Risques • Critère 2

- Accès non autorisé ou frauduleux.

Critère spécifique à SAP • Critère 2

Critère spécifique à SAP : OUI

Preuves à demander

- Obtenir la matrice de séparation des fonctions SAP et vérifier la pertinence des fonctions au regard des transactions autorisées. du lien entre fonctions et transactions.
- La matrice adaptée SAP doit bien contenir les transactions incompatibles entre elles (avec objets d'autorisations associés).

Bonnes pratiques

- Les transactions spécifiques (développées par l'entité) sont incluses dans cette matrice.
- Les transactions sensibles sont identifiées. Les transactions ouvrant droit à la même opération mais dont la désignation diffère en fonction du module sont identifiées.
- Chaque fonction et chaque transaction doivent avoir un libellé suffisamment explicite pour permettre un contrôle par rapprochement.
- Une attention est prêtée aux conventions de nommage des transactions spécifiques (commençant par Y ou Z ou autre).

CRITÈRE 3 • Les processus métiers de la matrice intègrent l'exhaustivité des modules fonctionnels actifs de SAP (y compris ceux en cours de déploiement)

Commentaires • Critère 3

Vérifier que la matrice couvre l'ensemble des processus fonctionnels de l'entité (Achats, Stocks, Ventes, RH, Finance, production, etc).

Identifier les processus non pris en compte par l'entité. Une matrice peut présenter des fonctions sans transaction SAP dans le cas où l'organisation ne l'a pas déployée sur l'ensemble des processus métiers.

Risques • Critère 3

- Accès non autorisé ou frauduleux.

Critère spécifique à SAP • Critère 3

Critère spécifique à SAP : OUI

Preuves à demander

- Vérifier la cohérence entre les modules fonctionnels actifs de SAP et les processus analysés dans la matrice.

Bonnes pratiques

- Analyser les systèmes couvrant les processus non gérés dans SAP (revue de processus de bout en bout). Par exemple, une commande pourrait être créée dans SAP et réceptionnée dans un système dédié par la même personne. Il n' y aurait pas de conflit au niveau de SAP mais conflit fonctionnel.

CRITÈRE 4 • Les conflits et les risques associés sont documentés. La matrice de séparation des fonctions est diffusée aux utilisateurs

Commentaires • Critère 4

- Chaque conflit génère un risque qui doit être formalisé et associé à une priorité.
- Les risques doivent avoir été identifiés selon leur niveau de criticité (critique, élevé, moyen, bas).
- Chaque niveau de criticité doit faire l'objet d'une définition.

Risques • Critère 4

- Accès non autorisé ou frauduleux.

Critère spécifique à SAP • Critère 4

Critère spécifique à SAP : NON

Preuves à demander

- Récupérer la preuve de la documentation des conflits de séparation des fonctions.
- Obtenir la preuve de la diffusion de ce document.
- S'assurer de la compréhension des conflits et risques associés.

Bonnes pratiques

La description des risques liés aux conflits doit être explicite et ne doit pas se limiter à une simple indication de fonctions incompatibles ; par exemple :

- Une formulation du type : « Création de commande et réception de marchandises incompatibles » serait insuffisante car elle n'expliciterait pas le risque qui pourrait être libellé comme suit : « Risque de créer une commande non autorisée et de faire la réception à usage personnel ».

OBJECTIF DE CONTRÔLE N°2

• LES RÔLES SAP NE CONTIENNENT PAS DE CONFLIT INTRINSÈQUE DE SÉPARATION DES FONCTIONS

CRITÈRE 1 • L'entité dispose d'un moyen d'identification, de gestion et de suivi des conflits de séparation des tâches dans SAP

Commentaires • Critère 1

Les rôles sont « conformes », ils ne cumulent pas de transactions incompatibles permettant d'éviter d'attribuer des transactions en conflit.

Risques • Critère 1

- Accès non autorisé ou frauduleux.

Critère spécifique à SAP • Critère 1

Critère spécifique à SAP : OUI

Preuves à demander

- Entretien avec les équipes en charge du processus de gestion des rôles et des équipes de gestion des habilitations.
- Obtenir la preuve que la matrice des rôles incompatibles existe.
- Obtenir la liste des exceptions « rôles non conformes » acceptés.

Bonnes pratiques

- Une étude est régulièrement menée pour s'assurer que les rôles ne présentent pas de conflits intrinsèques.

CRITÈRE 2 • La matrice de séparation des fonctions est connue et mise en œuvre par les équipes en charge de l'attribution des rôles aux utilisateurs

Commentaires • Critère 2

L'attribution à un utilisateur de plusieurs rôles est conforme à la séparation des fonctions, les conflits générés par l'accumulation de rôles ont été pris en compte.

Risques • Critère 2

- Accès non autorisé ou frauduleux.

Critère spécifique à SAP • Critère 2

Critère spécifique à SAP : OUI

Preuves à demander

- Obtenir la preuve du contrôle de conformité de la séparation des fonctions lors de l'attribution d'un nouveau rôle.

Bonnes pratiques

- Un outil de vérification de conformité à la matrice existe.

CRITÈRE 3 • Un processus formalisé de gestion des conflits volontairement attribués aux utilisateurs existe

Commentaires • Critère 3

- La validation légitime et indépendante d'une attribution des conflits existe.
- L'évaluation et l'acceptation de l'attribution de conflits font l'objet d'une traçabilité.
- Une liste des personnes autorisées à valider un conflit est maintenue.

Risques • Critère 3

- Accès non autorisé ou frauduleux.

Critère spécifique à SAP • Critère 3

Critère spécifique à SAP : NON

Preuves à demander

- Preuve de la validation formelle.
- Évaluation de la traçabilité du processus.

Bonnes pratiques

- Les attributions de rôles générant des conflits à risques très élevés (fraude) sont prises en compte et interdites.

OBJECTIF DE CONTRÔLE N°3

• UNE GESTION APPROPRIÉE DES CONFLITS EST MISE EN ŒUVRE

CRITÈRE 1 • L'entité dispose d'un moyen d'identification, de gestion et de suivi des conflits de séparation des tâches dans SAP

Commentaires • Critère 1

Soit les Conflits sont « justifiés » et des contrôles compensatoires existent, Soit les conflits sont « injustifiés » et font l'objet d'un plan d'action approprié.

SAP GRC Access Control ou d'autres outils spécifiques (manuels et / ou automatisés) peuvent être utilisés. Mais ces outils, même s'ils facilitent le pilotage des conflits, présentent une complexité et impliquent un temps et des compétences pour analyser et compenser les conflits.

Risques • Critère 1

- Accès non autorisé ou frauduleux.

Critère spécifique à SAP • Critère 1

Critère spécifique à SAP : OUI

Preuves à demander

- Observer le fonctionnement et l'utilisation réelle de l'outil déployé, identifier les conflits paramétrés dans l'outil, visualiser les conflits existants.

CRITÈRE 2 • Chaque conflit résiduel fait l'objet d'une documentation et a minima d'un contrôle compensatoire ou d'un plan d'actions

Commentaires • Critère 2

Dans la grande majorité des systèmes SAP, il reste des rôles affectés à des utilisateurs générant des conflits. Ces derniers doivent systématiquement faire l'objet d'un contrôle compensatoire adapté au risque et au conflit.

Risques • Critère 2

- Accès non autorisé ou frauduleux.

Critère spécifique à SAP • Critère 2

Critère spécifique à SAP : OUI

Preuves à demander

- Obtenir la liste des conflits existants et analyser la pertinence des contrôles compensatoires définis.
- Vérifier que l'ensemble des conflits identifiés fait l'objet d'un contrôle compensatoire ou d'un plan d'actions. Analyser la pertinence du contrôle compensatoire.

Bonnes pratiques

- Un responsable métier est en charge de piloter les conflits et les contrôles compensatoires déployés. Un suivi est réalisé et animé de manière régulière.
- Les conflits liés à la fraude n'existent pas car ils ne sont pas tolérés par l'entreprise.

CRITÈRE 3 • Les contrôles compensatoires sont définis et validés par le management. Les contrôles compensatoires sont utilisés en dernier recours

Commentaires • Critère 3

Les contrôles compensatoires doivent être utilisés en dernier recours :

- Soit le conflit n'est pas justifié. Auquel cas, il faut corriger le conflit dans le système (modification des droits d'accès).

- Soit le conflit est justifié mais peut être évité en modifiant l'actuelle répartition des tâches entre utilisateurs. Auquel cas, l'organisation doit être ajustée et les droits d'accès corrigés en adéquation avec les nouveaux rôles et responsabilités.
- Soit le conflit est justifié et ne peut être évité. Auquel cas, un contrôle compensatoire doit être défini et validé afin de réduire le risque afférent.

Risques • Critère 3

- Accès non autorisé ou frauduleux.

Critère spécifique à SAP • Critère 3

Critère spécifique à SAP : NON

Preuves à demander

- Obtenir la preuve de l'avancement des plans d'actions.
- Faire un échantillonnage.

Bonnes pratiques

- Les contrôles compensatoires sont régulièrement repensés afin de s'assurer de leur pertinence, ainsi que de leur utilité.

CRITÈRE 4 • Les contrôles compensatoires sont appliqués par le métier et un processus de mise à jour régulière est en place

Commentaires • Critère 4

Les contrôles compensatoires doivent être appliqués et documentés. Ces contrôles sont réalisés par un tiers indépendant du détenteur de la transaction en conflit.

La liste des contrôles compensatoires est revue de manière régulière par un tiers indépendant.

Risques • Critère 4

- Accès non autorisé ou frauduleux.

Critère spécifique à SAP • Critère 4

Critère spécifique à SAP : NON

Preuves à demander

- Obtenir une documentation du contrôle et de sa revue.
- Faire un échantillonnage.
- Preuve que les tiers contrôleurs sont indépendants.

Bonnes pratiques

- Les contrôles sont documentés au sein d'un système dédié permettant d'avoir une traçabilité sur l'ensemble des contrôles qui ne seraient pas réalisés.

Synthèse d'une revue de la séparation des fonctions et proposition d'approche

- Obtenir la matrice de séparation des fonctions.
- Constater que la matrice a été adaptée à SAP et est connue des équipes « habilitations » et « rôles et autorisations » (dans le cadre de la création des rôles et aussi des affectations) :
  - S'assurer que la matrice couvre tout le périmètre fonctionnel géré dans SAP (achats, RH, finance etc) et le « périmètre » informatique.
  - S'assurer que la matrice est appliquée à tous les utilisateurs.
- Obtenir une description des rôles, responsabilités et processus de revue de la séparation des fonctions et de sa mise à jour.
- Obtenir la liste des conflits potentiels dans SAP.
- Obtenir la liste des utilisateurs ayant des conflits de séparation des fonctions.
- Faire une sélection de conflits (notamment concernant la fraude) existants.
- Demander si ces conflits sont connus et justifiés.
- Évaluer la conception du contrôle compensatoire.
- Obtenir la preuve de ce contrôle.

domaine 5. Sécurisation des flux entrants et sortants

DÉFINITION ET PÉRIMÈTRE DU DOMAINE

Ce domaine traite des problématiques d'entrées et de sorties automatisées de données.

Ces mouvements peuvent avoir pour origine des interfaces avec d'autres applications ou d'autres systèmes SAP.

En complément, le périmètre de ce domaine inclus également les fonctionnalités à déclenchement manuel d'import et d'export en masse de données.

Les préoccupations liées à ce domaine concernent à la fois la connaissance, la documentation et la mise en œuvre maîtrisée de ces dispositifs d'échange entre applications, ainsi que le pilotage du bon achèvement de ces traitements automatisés du point de vue métier.

En termes de sécurité, les interfaces et les mécanismes d'échange sur lesquels elles s'appuient constituent autant de portes ouvertes sur le système SAP dont il est nécessaire d'assurer la maîtrise.

Les attentes concernent donc principalement :

- La cartographie des flux inter applicatifs mis en œuvre.
- La vérification du bon achèvement métiers des flux.
- La prévention contre les flux non autorisés.
- La maîtrise des dispositifs d'import / export en masse.

RISQUES ASSOCIÉS

Les principaux risques identifiés sur ce domaine sont :

- Les atteintes à la confidentialité des données.
- La perte d'intégrité ou le vol de données.
- La falsification ou la suppression des fichiers d'échange.
- La compromission des données importées et / ou exportées.
- L'exécution de programme non autorisés via des passerelles ouvertes.
- L'usurpation d'identité d'une application.

OBJECTIF DE CONTRÔLE N°1

• L'ORGANISATION A MIS EN ŒUVRE DES MOYENS DESTINÉS À ASSURER LA MAÎTRISE DES FLUX INTER APPLICATIFS

CRITÈRE 1 • La cartographie des flux applicatifs existe, est tenue à jour et est conforme à l'existant en production

Commentaires • Critère 1

Cette cartographie est exhaustive et recense toutes les interfaces, quel que soit leur type : RFC, IDOCs, BATCH INPUT, BATCH...

NB :

- Un message IDOC est un conteneur de données SAP assurant l'échange structuré d'information entre deux systèmes applicatifs.
- RFC « Remote Function Call » est un protocole permettant la communication entre deux systèmes SAP.
- Traiter le transfert d'un lot de données contenu dans un fichier amont.
- BATCH est un type de transfert de données provenant d'une application.

Risques • Critère 1

- Accès non autorisé ou frauduleux.
- Perte de données.
- Perte de traçabilité.
- Usurpation d'identité.
- Altération ou perte d'intégrité des données.

Critère spécifique à SAP • Critère 1

Critère spécifique à SAP : OUI pour certains types d'interfaces.

Preuves à demander

- Inventaire des flux applicatifs, entrants et sortants.

- Liste des destinations RFC, obtenue en utilisant la transaction SM59.
- Date de dernière mise à jour de la cartographie.

Bonnes pratiques

- La cartographie précise les applications partenaires, les données métiers véhiculées, la fréquence et le sens des échanges, l'événement déclencheur.

CRITÈRE 2 • Toute liaison applicative est clairement documentée

Commentaires • Critère 2

La connaissance détaillée des caractéristiques de chacune de ces liaisons est un préalable indispensable à sa maîtrise.

Risques • Critère 2

- Accès non autorisé ou frauduleux.
- Perte de données.
- Perte de traçabilité.
- Usurpation d'identité.
- Altération ou perte d'intégrité des données.

Critère spécifique à SAP • Critère 2

Critère spécifique à SAP : NON

Preuves à demander

- Les spécifications fonctionnelles générales et détaillées disposent pour chaque liaison des informations transférées.

Bonnes pratiques

- La description précise l'application partenaire et l'objet de l'interface, les informations sur les données transférées, le responsable de l'application / interface, la méthode d'authentification et d'identification de l'utilisateur, les autorisations relatives à la connexion de l'utilisateur.

CRITÈRE 3 • Les flux contenant des informations de nature confidentielle sont cryptés

Commentaires • Critère 3

En accord avec la politique de sécurité et les décisions prises en matière de protection des données (voir également le domaine 2 Sécurité des données) en tenant compte des besoins exprimés par les métiers, des dispositifs spécifiques de cryptage peuvent être nécessaires.

Risques • Critère 3

- Accès non autorisé ou frauduleux.
- Perte de données.
- Usurpation d'identité.
- Vol de données.

Critère spécifique à SAP • Critère 3

Critère spécifique à SAP : NON

Preuves à demander

- Exigences métiers en termes de confidentialité et d'intégrité des données échangées, formalisées.
- Spécifications fonctionnelles générales et détaillées qui décrivent la nature des informations et les modalités de cryptage mises en œuvre.

Bonnes pratiques

- L'échange s'appuie sur les protocoles de communication sécurisée HTTPS (HTTP) ou SNC (RFC).

CRITÈRE 4 • Les éventuels flux entre l'environnement de production et les autres environnements (pré-production, recette, développement) sont maîtrisés

Commentaires • Critère 4

La protection de l'environnement de production et son isolement restent un objectif prioritaire. Or, dans le cadre d'un système SAP, la gestion des différents environnements pourrait conduire à des situations de porosité et d'échanges entre les différents environnements SAP.

Risques • Critère 4

- Accès non autorisé ou frauduleux.
- Perte de données.
- Usurpation d'identité.

Critère spécifique à SAP • Critère 4

Critère spécifique à SAP : OUI

Preuves à demander

- La cartographie du paysage système SAP et les flux entre les systèmes.

Bonnes pratiques

- Les seuls flux éventuels autorisés concernent les flux de transports (STMS) ou les flux sortants de production pour générer des données de test.
- C'est un sujet sensible qui peut justifier l'intervention d'un spécialiste.

CRITÈRE 5 • Les communications doivent être assurées de manière automatique. Les canaux de communication qui peuvent être utilisés par des utilisateurs physiques sont identifiés et surveillés, leur utilisation est restreinte

Commentaires • Critère 5

Les communications RFC de type DIALOGUE sont maitrisées. Elles sont à éviter et à surveiller. Leur utilisation est restreinte.

Risques • Critère 5

- Accès non autorisé ou frauduleux.
- Perte de données.
- Perte de traçabilité.
- Usurpation d'identité.
- Altération ou perte d'intégrité des données.

Critère spécifique à SAP • Critère 5

Critère spécifique à SAP : OUI

Preuves à demander

- Liste des destinations RFC de type DIALOGUE (NB : Le programme RFCCHECK est exécuté pour vérifier les destinations RFC s'appuyant sur l'utilisation d'un identifiant et d'un mot de passe).
- Procédure de gestion du compte utilisateur de la liaison.

Bonnes pratiques

- Les communications RFC de type Dialogue sont interdites.

OBJECTIF DE CONTRÔLE N°2

• DES DISPOSITIFS ASSURANT L'INTÉGRITÉ DES FLUX MÉTIERS ONT ÉTÉ DÉFINIS

CRITÈRE 1 • Il existe des contrôles pour assurer la cohérence technique et le bon format des flux

Commentaires • Critère 1

Il s'agit de vérifier auprès des équipes IT, la cohérence et le format de la donnée informatique et des tables émises et reçues via les flux.

Risques • Critère 1

- Accès non autorisé ou frauduleux.
- Perte de données.
- Perte de traçabilité.
- Usurpation d'identité.
- Altération ou perte d'intégrité des données.

Critère spécifique à SAP • Critère 1

Critère spécifique à SAP : NON

Preuves à demander

- Description ou procédure de contrôle de cohérence technique.
- Descriptif d'un éventuel outillage.
- Compte-rendu de bonne exécution.

Bonnes pratiques

- Les caractéristiques de chaque donnée et / ou table sont connues et contrôlées : format, nombre et nature de colonne, etc.
- Les contrôles portant sur les formats des fichiers et des données sont automatisés.

CRITÈRE 2 • Il existe des contrôles fonctionnels pour assurer la cohérence métier des données

Commentaires • Critère 2

Il s'agit de vérifier auprès des équipes métier, de manière quantitative et qualitative, les informations émises et reçues via les flux.

Risques • Critère 2

- Accès non autorisé ou frauduleux.
- Perte de données.
- Perte de traçabilité.
- Usurpation d'identité.
- Altération ou perte d'intégrité des données.

Critère spécifique à SAP • Critère 2

Critère spécifique à SAP : NON

Preuves à demander

- Description ou procédure de contrôle de cohérence métier.
- Descriptif d'un éventuel outillage.
- Compte-rendu de bonne exécution.

Bonnes pratiques

- Les caractéristiques de chaque information sont connues et contrôlées. Par exemple : nombre de commandes, valeur moyenne, totaux, etc.

CRITÈRE 3 • Le bon achèvement de l'acheminement des flux est supervisé

Commentaires • Critère 3

Ce point concerne la supervision technique des flux, généralement assurée par les équipes de production.

Risques • Critère 3

- Perte de traçabilité.
- Altération ou perte d'intégrité des données.

Critère spécifique à SAP • Critère 3

Critère spécifique à SAP : NON

Preuves à demander

- Politique de conservation des logs.
- Procédure de gestion des anomalies et des rejets, liste des XXXX (IDOCs) ou des fichiers d'interfaces non transférés (en erreur) le jour du contrôle.

Bonnes pratiques

- Le processus de gestion des anomalies d'interfaces fait partie intégrante du processus métier, notamment lors des périodes de clôture.

CRITÈRE 4 • Le traitement des anomalies et des rejets est tracé et assuré dans des délais appropriés

Commentaires • Critère 4

Le rejet par les mécanismes de contrôles permet d'identifier les flux dont l'intégrité n'est pas parfaite (en raison par exemple d'incohérences ou car incomplètes).

Toutefois, les flux représentant des opérations réelles doivent bien être intégrés dans le système, de façon valide et sécurisée, et sur la période de temps à laquelle ils appartiennent.

Risques • Critère 4

- Accès non autorisé ou frauduleux.
- Perte de données.
- Perte de traçabilité.
- Usurpation d'identité.
- Altération ou perte d'intégrité des données.

Critère spécifique à SAP • Critère 4

Critère spécifique à SAP : NON

Preuves à demander

- Procédure de gestion des anomalies et des rejets, liste des XXX (IDOCs) ou des fichiers d'interfaces en erreur le jour du contrôle.

- La procédure doit indiquer comment les données sont recyclées dans un délai approprié et par des personnes habilitées.
- Justification du recyclage des rejets et des erreurs sur un échantillon.

Bonnes pratiques

- Le processus de gestion des anomalies d'interfaces fait partie intégrante du processus métier, notamment lors des périodes de clôture.

CRITÈRE 5 • Les droits de modification / suppression des fichiers de données de l'interface (y compris les IDOCs) sont connus, documentés et vérifiés

Commentaires • Critère 5

Il y a différentes façons d'échanger des données avec SAP : des fichiers d'interfaces ou des IDOCs. (Un IDOC étant un conteneur de données).

Chaque type donne lieu à des protections spécifiques dans SAP ou au niveau du système d'exploitation (Accès aux serveurs / répertoires de données).

Risques • Critère 5

- Accès non autorisé ou frauduleux.
- Perte de données.
- Perte de traçabilité.
- Usurpation d'identité.
- Altération ou perte d'intégrité des données.

Critère spécifique à SAP • Critère 5

Critère spécifique à SAP : NON

Preuves à demander

- Liste des personnes disposant éventuellement des droits pour modifier les fichiers d'interfaces (y compris les IDOCs), les supprimer, etc.

Bonnes pratiques

- Vérification régulière que personne ne dispose de droit permettant de modifier un fichier d'interface et / ou un IDOC ou de le supprimer.

OBJECTIF DE CONTRÔLE N°3

• UNE PRÉVENTION CONTRE LES FLUX NON AUTORISÉS EST EN PLACE

CRITÈRE 1 • La création / modification / suppression des liaisons RFC est encadrée et maitrisée

Commentaires • Critère 1

Le kit de développement RFC permet de créer / modifier / supprimer une interface de type RFC (Remote Function Call). Il est installé en standard par SAP.

La gestion des liaisons RFC est réservée à un groupe restreint d'administrateurs clairement identifiés. La liste est tenue à jour.

Risques • Critère 1

- Accès non autorisé ou frauduleux.
- Perte de données.
- Perte de traçabilité.
- Usurpation d'identité.
- Altération ou perte d'intégrité des données.

Critère spécifique à SAP • Critère 1

Critère spécifique à SAP : OUI

Preuves à demander

- Preuve de la suppression du kit de développement RFC (SDK « RFCSDK ») sur l'environnement de production.
- Liste de référence des administrateurs pouvant gérer les liaisons RFC.
- Procédure de gestion des interfaces.

Bonnes pratiques

- Une procédure prévoit explicitement la vérification de l'absence de ce SDK et sa suppression le cas échéant. Cet acte d'administration est tracé et certifié.

CRITÈRE 2 • L'usage du gateway SAP est sécurisé

Commentaires • Critère 2

Le gateway SAP permet d'exécuter des programmes au niveau du système d'exploitation et de sécuriser la communication avec d'autres applications.

Son paramétrage est défini dans deux fichiers SECINFO et REGINFO.

Risques • Critère 2

- Accès non autorisé ou frauduleux.
- Perte de données.
- Perte de traçabilité.
- Usurpation d'identité.
- Vol de données.
- Altération ou perte d'intégrité des données.

Critère spécifique à SAP • Critère 2

Critère spécifique à SAP : OUI

Preuves à demander

- Fichiers SECINFO et REGINFO : vérifier leur existence et obtenir leur contenu à l'aide de la transaction SMGW.
- Validation des règles paramétrées dans ces fichiers au regard des règles présentes dans les spécifications.

Bonnes pratiques

- Les règles sont définies de façon à limiter les accès au strict nécessaire.

CRITÈRE 3 • Le mécanisme « trusted system » (système fiable) n'est pas mis en œuvre. Dans le cas contraire, son utilisation fait l'objet d'une décision et les systèmes reliés possèdent tous un niveau de sécurité équivalent

Commentaires • Critère 3

Le mécanisme « trusted system » permet à un utilisateur SAP de ne pas devoir s'identifier / s'authentifier lors de la connexion à l'application tierce SAP.

Risques • Critère 3

- Accès non autorisé ou frauduleux.
- Perte de données.
- Perte de traçabilité.
- Usurpation d'identité.
- Vol de données.
- Altération ou perte d'intégrité des données.

Critère spécifique à SAP • Critère 3

Critère spécifique à SAP : OUI

Preuves à demander

- La liste des destinations RFC considérées comme « système fiable ».
- La transaction SM59 est une connexion sécurisée.

OBJECTIF DE CONTRÔLE N°4

• L'ORGANISATION A MIS EN PLACE UNE GESTION SÉCURISÉE DES FONCTIONNALITÉS D'IMPORT / EXPORT EN MASSE DE DONNÉES

CRITÈRE 1 • Les dispositifs d'Import / Export de données en masse dans SAP sont connus et documentés

Commentaires • Critère 1

SAP propose différentes méthodes d'Import / Export de données en masse : SAPGUI scripting, eCATT et CATT, LSMW, batch-input, transaction fonctionnelle standard (création d'articles en masse via le module MM).

Risques • Critère 1

- Accès non autorisé ou frauduleux.
- Perte de données.
- Perte de traçabilité.
- Usurpation d'identité.
- Vol de données.
- Altération ou perte d'intégrité des données.
- Risque réglementaire.

Critère spécifique à SAP • Critère 1

Critère spécifique à SAP : OUI

Preuves à demander

- Spécifications fonctionnelles générales et détaillées qui décrivent les processus d'Import / Export de données en masse.

Bonnes pratiques

Les paramètres du système SAP sont en adéquation avec les méthodes d'Import / Export utilisées :

- Paramètres SAP.
- Propriétés mandant via transaction SCC4 (interdiction des CATT et eCATT).

CRITÈRE 2 • La séparation des tâches entre la décision et l'exécution des opérations d'Import / Export est assurée

Commentaires • Critère 2

Les personnes en mesure de réaliser les opérations d'Import / Export sont distinctes des personnes ayant autorité pour décider ces opérations.

Risques • Critère 2

- Accès non autorisé ou frauduleux.
- Perte de données.
- Perte de traçabilité.
- Usurpation d'identité.
- Vol de données.
- Altération ou perte d'intégrité des données.

Critère spécifique à SAP • Critère 2

Critère spécifique à SAP : NON

Preuves à demander

- Procédure des opérations d'Import / Export.
- Vérification de l'approbation formelle sur un échantillon d'opérations.

Bonnes pratiques

- La personne ayant autorité est un responsable métier.

CRITÈRE 3 • La qualité et l'intégrité de l'information à importer ou exporter du système est garantie par les processus en place

Commentaires • Critère 3

La cohérence métiers et technique des données et des informations à importer ou à exporter est préalablement contrôlée et validée (ex. prix d'achat négatif interdit...).

Des processus de contrôle garantissent que les données importées et / ou exportées sont conformes à l'original.

Risques • Critère 3

- Accès non autorisé ou frauduleux.
- Perte de données.
- Perte de traçabilité.
- Usurpation d'identité.
- Vol de données.
- Altération ou perte d'intégrité des données.

Critère spécifique à SAP • Critère 3

Critère spécifique à SAP : NON

Preuves à demander

- Procédures de contrôles des données :
  - Avant l'Import / Export.
  - Après l'Import / Export.
- Spécifications fonctionnelles et détaillées qui décrivent les contrôles d'Import / Export de données en masse.

Bonnes pratiques

- La qualité des données importées / exportées sont contrôlées en amont et en aval.

CRITÈRE 4 • Les opérations d'Import / Export de données en masse dans SAP sont identifiées, surveillées, tracées et documentées

Commentaires • Critère 4

Des dispositifs de surveillance et de documentation assurent la connaissance de ces actions et leur traçabilité pour investigation postérieure, si nécessaire. Dans la mesure où des logs de traitement existent, une politique de conservation doit exister (en cas de contrôle fiscal, le contrôleur peut demander de remonter jusqu'au fait générateur et de justifier étape par étape toutes les transformations réalisées, la log peut aider dans ce cas précis).

Risques • Critère 4

- Accès non autorisé ou frauduleux.
- Perte de données.
- Perte de traçabilité.
- Usurpation d'identité.
- Vol de données.
- Altération ou perte d'intégrité des données.

Critère spécifique à SAP • Critère 4

Critère spécifique à SAP : NON

Preuves à demander

- Liste des opérations d'Import / Export.
- Existence de logs d'Import / Export, de leur analyse et de leur exploitation.

Bonnes pratiques

- Un archivage des logs est effectué.
- Les requêtes ad' hoc font l'objet d'une expression fonctionnelle des besoins et sont suivies.

CRITÈRE 5 • Les utilisateurs pouvant gérer les données d'Import / Export en masse sont en nombre restreint

Commentaires • Critère 5

Les fonctionnalités d'Import / Export, par le manque de contrôle qui les caractérisent, ne peuvent pas être laissées libres d'accès au plus grand nombre.

Risques • Critère 5

- Accès non autorisé ou frauduleux.
- Perte de données.
- Perte de traçabilité.
- Usurpation d'identité.
- Vol de données.
- Altération ou perte d'intégrité des données.

Critère spécifique à SAP • Critère 5

Critère spécifique à SAP : NON

Preuves à demander

- Seules les personnes dûment habilitées disposent des droits nécessaires et suffisants pour réaliser les opérations.

Bonnes pratiques

- Il faut vérifier régulièrement que les habilitations sont restreintes.

domaine 6. Continuité de service et Plan de Reprise d'Activité (PRA)

DÉFINITION ET PÉRIMÈTRE DU DOMAINE

La gestion de la continuité d'une application sensible est généralement formalisée dans un Plan de Continuité d'Activité (PCA) pour permettre à une organisation de fonctionner même en cas de problème critique, même si cela doit être en mode dégradé.

On distingue le PCA du Plan de Reprise d'Activité (PRA) qui permet d'assurer, en cas de crise majeure ou importante d'un centre informatique, la reconstruction de son infrastructure et la remise en route des applications supportant l'activité d'une organisation.

Les notions de PCA et de PRA sont valables pour tout système d'information et ne sont donc pas spécifiques à un système SAP.

Attention : Ce domaine ne permet pas d'auditer un PCA. Il s'agit ici d'évaluer la continuité d'activité du système SAP uniquement.

RISQUES ASSOCIÉS

Comme évoqué dans la première partie de cet ouvrage, un système SAP soutient des processus plus ou moins majeurs (stratégiques, opérationnels) d'une organisation.

En fonction du niveau de sensibilité des processus embarqués au sein du système SAP et des impacts forts en cas de panne du système SAP qui pourraient être engendrés, il doit être déterminé le niveau de criticité du système SAP y compris pour les risques qui en découlent.

Parmi les risques les plus fréquents en cas d'indisponibilité d'un système SAP, on peut identifier :

- Des problèmes de continuité d'activité.
- Le non-respect des obligations réglementaires et légales de l'organisation.
- La perte de données.
- Une altération ou perte d'intégrité des données.
- La non maîtrise des dépenses.
- Une baisse de la qualité des niveaux de service du système.
- Une perte d'image pour l'organisation.

OBJECTIF DE CONTRÔLE N°1

• LES RISQUES MÉTIERS DUS À UNE INTERRUPTION DE SERVICE ET / OU UNE PERTE DE DONNÉES SONT IDENTIFIÉS

CRITÈRE 1 • Les effets d'une interruption de service sur l'activité de l'organisation sont identifiés

Commentaires • Critère 1

Évaluer / quantifier les risques métier et financier. Cela est très dépendant du périmètre fonctionnel du système audité.

Risques • Critère 1

- Perte d'image.
- Perte financière.
- Arrêt non planifié de l'exploitation.

Critère spécifique à SAP • Critère 1

Critère spécifique à SAP : NON

Preuves à demander

- L'étude d'impact existe et est tenue à jour : Business Impact Analysis (BIA)...

Bonnes pratiques

- Il faut vérifier qu'il y a bien une réflexion régulière sur la perte de données tolérables par le métier.

CRITÈRE 2 • Les effets d'une perte de données sur l'activité de l'organisation sont identifiés

Commentaires • Critère 2

Évaluer / quantifier les risques notamment financiers. Cela est très dépendant du périmètre fonctionnel du système audité.

Risques • Critère 2

- Non maîtrise des dépenses.
- Non-respect réglementaire ou légal.

Critère spécifique à SAP • Critère 2

Critère spécifique à SAP : NON

Preuves à demander

- L'étude d'impact ou BIA (Business Impact Analysis) a été réalisée permettant l'étude de l'impact d'une perte de données et d'une indisponibilité prolongée d'un système sur le métier.
- L'historique de ses mises à jour.

Bonnes pratiques

- Il faut vérifier qu'il y a bien une réflexion régulière sur la perte de données tolérables par le métier.

CRITÈRE 3 • Les effets d'un dysfonctionnement des applications interfacées sont identifiés dans le cas où ils pourraient provoquer une interruption de service

Commentaires • Critère 3

Les applications liées au système SAP par interface ne risquent pas d'affecter le système SAP en cas de dysfonctionnement.

Risques • Critère 3

- Arrêt non planifié de l'exploitation.

Critère spécifique à SAP • Critère 3

Critère spécifique à SAP : NON

Preuves à demander

- La cartographie des applications critiques et la formalisation des risques associés.
- La cartographie des flux et interfaces.
- Prise en compte des dysfonctionnements SAP sur les autres applications.

Bonnes pratiques

- Il convient de s'assurer que la continuité technique est intégrée dans la continuité globale du processus.

OBJECTIF DE CONTRÔLE N°2

• LES EXIGENCES DE CONTINUITÉ DE SERVICES SONT FORMALISÉES (CONTRAT DE SERVICE)

CRITÈRE 1 • Les exigences de continuité de service sont formalisées dans un document

Commentaires • Critère 1

Il ne s'agit pas ici de PCA (incluant les processus et procédures manuelles) mais de continuité du service au quotidien de l'application SAP.

Risques • Critère 1

- Niveau de service insuffisant.

Critère spécifique à SAP • Critère 1

Critère spécifique à SAP : NON

Preuves à demander

- Le document décrivant les dispositifs de la gestion de la continuité d'un système SAP (contrat de service).

Bonnes pratiques

- Il faut vérifier que le contrat de service (SLA) existe et soit mis à jour en cas de changement majeur.

CRITÈRE 2 • La perte de données maximale admise est définie

Commentaires • Critère 2

Demander les objectifs en termes de Perte de Données Maximale Admissible (PDMA) ou Recovery Point Objective (RPO).

Risques • Critère 2

- Niveau de service insuffisant.

Critère spécifique à SAP • Critère 2

Critère spécifique à SAP : NON

Preuves à demander

- Vérifier que le PDMA est défini dans le contrat de service.

Bonnes pratiques

- Identifier le PDMA par domaine fonctionnel en fonction d'un calendrier des périodes critiques (clôture annuelle, paye, DADS...).

CRITÈRE 3 • La durée maximale d'interruption de service est définie

Commentaires • Critère 3

Demander les objectifs en termes de Durée Maximale d'Indisponibilité Admissible (DMIA) ou Recovery Time Objective (RTO).

Risques • Critère 3

- Niveau de service insuffisant.

Critère spécifique à SAP • Critère 3

Critère spécifique à SAP : NON

Niveau de service insuffisant.

Critère spécifique à SAP : NON

Preuves à demander

- Vérifier que la DMIA est définie dans le contrat de service.

Bonnes pratiques

- Des dispositifs existent au niveau des métiers en cas de dépassement du RTO.

CRITÈRE 4 • Le taux de disponibilité annuel garanti est défini

Commentaires • Critère 4

Ce taux est exprimé en pourcentage et la formule de calcul doit être clairement définie et validé par les Métiers.

Risques • Critère 4

- Niveau de service insuffisant.

Critère spécifique à SAP • Critère 4

Preuves à demander

- Vérifier que le taux de disponibilité et sa formule de calcul sont formalisés dans le contrat de service.

Bonnes pratiques

- Il existe un reporting et une analyse du taux d'indisponibilité.

CRITÈRE 5 • Les exigences de services sont validées par les métiers

Commentaires • Critère 5

RAS.

Risques • Critère 5

- Niveau de service insuffisant.

Critère spécifique à SAP • Critère 5

Critère spécifique à SAP : NON

Preuves à demander

- Vérifier que le contrat de services est signé par le propriétaire du processus et par le responsable DSI.

Bonnes pratiques

- RAS.

CRITÈRE 6 • Le « rapport de service » est transmis de manière régulière

Commentaires • Critère 6

Le rapport de service correspond au compte-rendu du niveau de service réalisé au regard du Contrat de Service. Il s'agit du rapport de suivi de l'application du contrat de service et des niveaux de SLA définis ».

Risques • Critère 6

- Niveau de service insuffisant.
- Continuité d'activité.

Critère spécifique à SAP • Critère 6

Critère spécifique à SAP : NON

Preuves à demander

- Dernier Rapport de Service.

Bonnes pratiques

- Ceci est réalisé à minima mensuellement.

OBJECTIF DE CONTRÔLE N°3

• L'ENSEMBLE DU DISPOSITIF SUPPORTANT SAP EST CONFORME AUX EXIGENCES DE CONTINUITÉ DE SERVICE DÉFINIES PAR LE MÉTIER

NB : Cet objectif de contrôle correspond au cas où le système SAP est hébergé en interne. Dans le cas d'un Cloud ou d'une externalisation, il convient de se reporter à l'objectif de contrôle correspondant (Objectif de Contrôle numéro 7).

CRITÈRE 1 • Le matériel (serveur, disques...), les télécommunications et réseaux et la disponibilité des bases de données sont conformes aux exigences de service attendues

Commentaires • Critère 1

Ce point pourra être vérifié au regard du Dossier d'Architecture Technique (DAT) si des exigences y sont formulées.

Risques • Critère 1

- Continuité d'activité.

Critère spécifique à SAP • Critère 1

Critère spécifique à SAP : NON

Preuves à demander

- Un dispositif de détection et d'alerte d'interruption de service de télécommunications & réseau a été défini comprenant :
  - Savoir si une analyse de risques a été menée pour identifier les mesures permettant de répondre s aux exigences de services métiers.
  - Vérifier si le DAT prend en compte ces mesures.
  - Vérifier si ces mesures ont été correctement mises en œuvre (dossier de mises en production, procès-verbal de recette avant mise en production.
- Le dispositif de réplication de la base de données est surveillé.
- Un responsable a été identifié.

Bonnes pratiques

- En cas de non-conformité, il convient de s'assurer que l'indisponibilité qui en découle et qui est assumée par le PRA est acceptable par rapport à l'exigence du service (cf. domaine 1).

CRITÈRE 2 • La disponibilité du système SAP est pilotée, par rapport aux exigences du service

Commentaires • Critère 2

Le monitoring SAP ou le suivi généralisé à toute l'infrastructure est réalisé. Un dispositif de contrôle technique de l'activité de l'application SAP existe.

Risques • Critère 2

- Arrêt non planifié de l'exploitation.

Critère spécifique à SAP • Critère 2

Critère spécifique à SAP : OUI

Preuves à demander

- Vérifier l'existence d'un dispositif qui s'assure que l'application répond bien (« test de vie » de l'application) et qu'un responsable est identifié.
- S'assurer qu'il existe un dispositif de test de charge du système.
- Il existe un historique d'alertes sur incidents.
- Une supervision des outils vitaux du système SAP est assurée.

Bonnes pratiques

- Des sondes sont utilisées.

CRITÈRE 3 • Une gestion des incidents est définie avec un système d'escalade

Commentaires • Critère 3

La gestion des incidents permet de moduler le niveau d'escalade (jusqu'au PRA et / ou à la gestion de crise).

Risques • Critère 3

- Arrêt non planifié de l'exploitation.
- Niveau de service insuffisant.

Critère spécifique à SAP • Critère 3

Critère spécifique à SAP : NON

Preuves à demander

- Le processus d'escalade est formalisé avec des critères définis et approuvés par le métier (priorité / criticité / étendue / date de résolution attendue).

Bonnes pratiques

- Le processus de gestion des incidents alimente le processus de gestion des problèmes.

OBJECTIF DE CONTRÔLE N°4

• LE SYSTÈME SAP EST COUVERT PAR UN PRA

CRITÈRE 1 • Le PRA est défini et conforme aux objectifs du métier

Commentaires • Critère 1

Le PRA du système SAP doit s'inscrire dans un PRA global du métier. Il intègre notamment une partie sur le retour à la normale.

Risques • Critère 1

- Perte de données.
- Non continuité d'activité.

Critère spécifique à SAP • Critère 1

Critère spécifique à SAP : NON

Preuves à demander

- Le PRA formalisé. Le PRA est à jour et validé par le Métier.

Bonnes pratiques

- RAS.

CRITÈRE 2 • Le PRA est testé sur une base régulière et maintenu pour garantir son efficacité

Commentaires • Critère 2

Le test du PRA porte notamment sur le matériel, le changement de site, les télécommunications, les bases de données, les procédures de redémarrage et de tests de bon fonctionnement de l'application SAP avec ses interfaces, etc.

Risques • Critère 2

- Perte de données.
- Arrêt non planifié de l'exploitation.

Critère spécifique à SAP • Critère 2

Critère spécifique à SAP : NON

Preuves à demander

- Les résultats du dernier test.

Bonnes pratiques

- Il est réalisé un test annuel.

CRITÈRE 3 • Les aspects RH (localisation des équipes informatiques, disponibilité / astreintes des techniciens) sont couverts par le PRA

Commentaires • Critère 3

RAS.

Risques • Critère 3

- Perte de données.
- Continuité d'activité.

Critère spécifique à SAP • Critère 3

Critère spécifique à SAP : NON

Preuves à demander

- Les tests de PRA inclus aussi la mise en situation et l'évaluation des aspects RH de la continuité de l'activité afin de permettre l'identification d'éventuelles faiblesses. Les tests inclus les accès VPN disponible, les équipements en ordinateurs portables.

Bonnes pratiques

- RAS.

CRITÈRE 4 • La priorité associée au redémarrage du système SAP, dans le cadre d'un PRA global, est définie et conforme aux objectifs du Métier

Commentaires • Critère 4

Le degré de priorité de reprise du système SAP, au sein du PRA global, est en adéquation avec son niveau de criticité.

Risques • Critère 4

- Arrêt non planifié de l'exploitation.

Critère spécifique à SAP • Critère 4

Critère spécifique à SAP : NON

Preuves à demander

- La définition des priorités de reprise du PRA.

Bonnes pratiques

- Existence d'un site de secours respectant une distance avec le site initial en fonction d'une étude adéquate (fonction des risques environnementaux).

CRITÈRE 5 • Lors du retour à la normale après un PRA, la mise en cohérence des échanges inter-applicatifs est assurée

Commentaires • Critère 5

L'ensemble des transactions ou opérations antérieures ou postérieures au PRA font l'objet d'un dispositif de vérification de leur exhaustivité et de l'absence de doublons.

Risques • Critère 5

- Perte de données.
- Altération ou perte d'intégrité des données.

Critère spécifique à SAP • Critère 5

Critère spécifique à SAP : NON

Preuves à demander

- La procédure de retour à la normale et les documents attestant de ces tests et leurs mises à jour.
- Vérifier qu'un point de cohérence entre les applications a été défini.

Bonnes pratiques

- RAS.

OBJECTIF DE CONTRÔLE N°5

• UN DISPOSITIF DE GESTION DE CRISE AUTOUR DE L'APPLICATION SAP EST ORGANISÉ

CRITÈRE 1 • La liste de personnes à mobiliser en cas de crise (appelée « Cellule de crise ») existe et est mise à jour régulièrement, un décideur dans la cellule de crise a été désigné

Commentaires • Critère 1

Cette liste peut faire partie du PCA.

Risques • Critère 1

- Arrêt non planifié de l'exploitation.

Critère spécifique à SAP • Critère 1

Critère spécifique à SAP : NON

Preuves à demander

- La liste des personnes avec le numéro de téléphone (y compris portable) à comparer avec l'annuaire téléphonique de l'entreprise.
- Contrôler que les membres de la cellule de crise ont connaissance de cette liste.

Bonnes pratiques

- Une cellule de crise est définie au préalable et inclut des personnes du Métier autant que des techniciens.
- La liste est régulièrement imprimée et accessible en cas de panne réseau généralisée.

CRITÈRE 2 • Les critères de déclenchement de la cellule de crise sont définis

Commentaires • Critère 2

Ces critères peuvent faire partie du PCA.

Risques • Critère 2

- Niveau de service insuffisant.
- Arrêt non planifié de l'exploitation.

Critère spécifique à SAP • Critère 2

Critère spécifique à SAP : NON

Preuves à demander

- Demander la liste des critères de déclenchement d'une crise.
- Comptes rendus, main courante et historique des dernières gestions de crises.

Bonnes pratiques

- RAS.

CRITÈRE 3 • Le dispositif de gestion de crise est testé

Commentaires • Critère 3

Ce test peut être réalisé à petite échelle, en simulant un scénario de crise afin de s'assurer que toutes les dispositions sont prises. Ce dispositif intègre également un retour à la normale.

Risques • Critère 3

- Niveau de service insuffisant.
- Arrêt non planifié de l'exploitation.

Critère spécifique à SAP • Critère 3

Critère spécifique à SAP : NON

Preuves à demander

- Le dernier rapport de test de crise.

Bonnes pratiques

- Il existe un planning prévisionnel de test.

CRITÈRE 4 • Le dispositif de communication de crise est défini

Commentaires • Critère 4

RAS.

Risques • Critère 4

- Arrêt non planifié de l'exploitation.
- Perte d'image.

Critère spécifique à SAP • Critère 4

Critère spécifique à SAP : NON

Preuves à demander

- La formalisation du dispositif de communication de crise (y compris la personne responsable de communication).

Bonnes pratiques

- RAS.

CRITÈRE 5 • Le retour d'expérience de crise est formalisé et sert à améliorer le service

Commentaires • Critère 5

Capitalisation sur une crise antérieure (si elle existe).

Risques • Critère 5

- Niveau de service dégradé.
- Arrêt non planifié de l'exploitation.

Critère spécifique à SAP • Critère 5

Critère spécifique à SAP : NON

Preuves à demander

- Rapport d'analyse à postériori de la crise et plan d'actions qui en a découlé.

Bonnes pratiques

- RAS.

OBJECTIF DE CONTRÔLE N°6

• LA SAUVEGARDE DU SYSTÈME SAP EST ASSURÉE

CRITÈRE 1 • Les modalités de sauvegarde sont définies et formalisées par rapport aux exigences du service

Commentaires • Critère 1

Les procédures doivent décrire la périodicité des sauvegardes, le détail des objets sauvegardés, le mode de suivi et les actions à mettre en œuvre en cas d'échec.

Risques • Critère 1

- Perte de données.
- Altération ou perte d'intégrité des données.

Critère spécifique à SAP • Critère 1

Critère spécifique à SAP : NON

Preuves à demander

- Procédure de sauvegarde formalisée.
- Preuve de la vérification de l'existence et de la lisibilité d'une sauvegarde annuelle.

Bonnes pratiques

- Les procédures de sauvegarde sont mises à jour régulièrement.

CRITÈRE 2 • Les données et l'application font l'objet de sauvegarde en accord avec les exigences et le bon achèvement est vérifié

Commentaires • Critère 2

Un suivi des sauvegardes existe et est formalisé.

Risques • Critère 2

- Perte de données.

Critère spécifique à SAP • Critère 2

Critère spécifique à SAP : NON

Preuves à demander

- Le compte rendu de bonne exécution des sauvegardes sur une période représentative (minimum deux mois).
- Le dispositif de suivi et d'archivage des sauvegardes.

Bonnes pratiques

- Il est réalisé une vérification quotidienne des sauvegardes.
- Il est mis en place d'un système d'alerte en cas d'échec de sauvegarde.

CRITÈRE 3 • Les sauvegardes et les restaurations réalisées font l'objet de tests réguliers

Commentaires • Critère 3

RAS.

Risques • Critère 3

- Perte de données.

Critère spécifique à SAP • Critère 3

Critère spécifique à SAP : NON

Preuves à demander

- Les comptes-rendus des derniers tests réalisés.

Bonnes pratiques

- Il est réalisé un test de restauration (annuel a minima) pour les applications critiques.

CRITÈRE 4 • Une conservation des sauvegardes est organisée dans un lieu distinct de celui du site d'exploitation

Commentaires • Critère 4

RAS.

Risques • Critère 4

- Perte de données.

Critère spécifique à SAP • Critère 4

Critère spécifique à SAP : NON

Preuves à demander

- La procédure d'archivage des sauvegardes sur un site externalisé.

Bonnes pratiques

- RAS.

OBJECTIF DE CONTRÔLE N°7

• SI LE SYSTÈME SAP EST EXTERNALISÉ, IL EST COUVERT PAR UN DISPOSITIF DE CONTINUITÉ DE SERVICE

NB : Cet objectif de contrôle correspond au cas où le système SAP est hébergé en externe ou dans le Cloud. Dans le cas où l'hébergement est interne, il convient de se reporter à l'objectif de contrôle correspondant (Objectif de Contrôle numéro 3).

Toutefois, les critères de l'objectif de contrôle numéro 3 (système SAP hébergé en interne) peuvent aider à vérifier la qualité de la continuité de service fournie par le prestataire conformément à la formalisation faite dans le contrat ou aider à le faire évoluer.

CRITÈRE 1 • Le contrat prévoit une offre de continuité de service répondant aux exigences de continuité de service du système SAP

Commentaires • Critère 1

Pour ceux qui utilisent le Cloud, s'assurer que l'offre de service associée est conforme aux exigences attendues en termes de protection des données, de continuité d'exploitation, de réversibilité...

Risques • Critère 1

- Perte de données.
- Arrêt non planifié de l'exploitation.

Critère spécifique à SAP • Critère 1

Critère spécifique à SAP : NON

Preuves à demander

- Contrat avec date et signature.

Bonnes pratiques

- Une certification du fournisseur (SSAE16 ou ISAE 3402) est obtenue, ainsi que le dernier rapport d'audit présentant les principales observations concernant le contrôle interne.

CRITÈRE 2 • Le contrôle du dispositif de continuité est prévu dans le contrat

Commentaires • Critère 2

Il existe une clause d'auditabilité dans le contrat. Une communication des derniers tests de PRA est effectuée.

Risques • Critère 2

- Perte de données.
- Arrêt non planifié de l'exploitation.

Critère spécifique à SAP • Critère 2

Critère spécifique à SAP : NON

Preuves à demander

- Contrat avec date et signature.
- Les comptes-rendus des derniers tests de PRA.

Bonnes pratiques

- La dernière attestation de certification est obtenue.

CRITÈRE 3 • Un rapport du niveau de service rendu en matière de continuité est transmis et examiné de manière régulière

Commentaires • Critère 3

Ceci est équivalent au SLA interne.

Risques • Critère 3

- Arrêt non planifié de l'exploitation.

Critère spécifique à SAP • Critère 3

Critère spécifique à SAP : NON

Preuves à demander

- Le dernier « niveau de service » en termes de continuité de service.

Bonnes pratiques

- Cela est réalisé a minima mensuellement.

CRITÈRE 4 • Une procédure de réversibilité existe et est testée régulièrement (au moins une fois tous les 2 ans)

Commentaires • Critère 4

Cela permet d'anticiper le changement de prestataire et / ou de logiciel. Ne pas oublier les dispositifs de récupération des données et la vérification de la capacité à les utiliser.

Risques • Critère 4

- Niveau de service insuffisant.
- Perte de données.
- Non maîtrise des dépenses.

Critère spécifique à SAP • Critère 4

Critère spécifique à SAP : NON

Preuves à demander

- Procédure de réversibilité.
- Résultats des tests de réversibilité et plans d'actions associés.
- Les critères de sélection d'un nouveau prestataire.

Bonnes pratiques

- RAS.

domaine 7. Sécurisation des changements

DÉFINITION ET PÉRIMÈTRE DU DOMAINE

Ce domaine traite des problématiques de la sécurisation des changements. Il s'agit de tout changement concernant le système SAP et ses interfaces.

Les préoccupations liées à ce domaine concernent à la fois le processus de gestion des changements, ses acteurs et leurs droits ainsi que les dispositifs de changements exceptionnels ou ceux qui ne peuvent pas suivre la procédure habituelle de gestion des changements.

En termes de sécurité, la gestion des mandants et la documentation associée, les acteurs et leurs droits, les développements spécifiques ainsi que le versionning constituent les éléments de sécurité minimum à évaluer.

Enfin, un focus particulier doit être fait sur la sécurisation de la plate-forme de production, son niveau de protection ainsi que le contrôle des utilisateurs qui y ont accès.

Les attentes concernent donc principalement :

- L'organisation des changements.
- Les dispositifs de sécurisation des changements.
- Les actions spécifiques liées à la sécurisation de la plate-forme de production.

RISQUES ASSOCIÉS

Les principaux risques identifiés sur ce domaine sont :

- Niveau de service insuffisant.
- Arrêt non planifié de l'exploitation.
- Perte de données.
- Altération ou perte d'intégrité des données.
- Accès non autorisé ou frauduleux.

OBJECTIF DE CONTRÔLE N°1

• ORGANISER UN CHANGEMENT

CRITÈRE 1 • Des étapes de décision des changements existent et sont formalisées et respectées

Commentaires • Critère 1

Le processus prend en compte les arbitrages entre les changements de projets et ceux issus du Maintien en conditions opérationnelles (exemple : réintégration d'une modification faites à chaud).

Risques • Critère 1

- Niveau de service insuffisant.
- Arrêt non planifié de l'exploitation.
- Perte de données.
- Altération ou perte d'intégrité des données.

Critère spécifique à SAP • Critère 1

Critère spécifique à SAP : NON

Preuves à demander

- Définition des acteurs.
- Demande de changement validée.

Bonnes pratiques

- Trois étapes minimum dans le processus : Le processus doit contenir une étape d'approbation du changement. Une étape de validation de la recette. Une étape d'approbation avant la livraison de l'ordre de transport en production (Change Advisory Board).

CRITÈRE 2 • Le processus de gestion des changements est formellement documenté

Commentaires • Critère 2

Un changement correspond à toute modification, installation, évolution ou correction de l'application.

Risques • Critère 2

- Niveau de service insuffisant.
- Arrêt non planifié de l'exploitation.
- Perte de données.
- Altération ou perte d'intégrité des données.

Critère spécifique à SAP • Critère 2

Critère spécifique à SAP : OUI

Preuves à demander

- Procédure de gestion des changements.
- Procédure de gestion des Ordres de Transport.
- Procès-verbal d'un changement.

Bonnes pratiques

- Le processus doit contenir au moins une étape de recette et une étape de mise en production.

CRITÈRE 3 • Les acteurs du changement respectent les principes de séparation des fonctions

Commentaires • Critère 3

RAS.

Risques • Critère 3

- Niveau de service insuffisant.
- Arrêt non planifié de l'exploitation.
- Perte de données.
- Altération ou perte d'intégrité des données.

Critère spécifique à SAP • Critère 3

Critère spécifique à SAP : NON

Preuves à demander

- Vérifier sur un échantillon représentatif des changements (ordres de transport ou autres) que la séparation des fonctions est respectée.

Bonnes pratiques

- Matrice de séparation des fonctions et incompatibilités entre elles.

CRITÈRE 4 • Les acteurs effectuant des changements sont clairement identifiés

Commentaires • Critère 4

Ce critère concerne de manière distincte : les développeurs, paramétreurs et l'administrateur des transports.

Risques • Critère 4

- Niveau de service insuffisant.
- Arrêt non planifié de l'exploitation.
- Perte de données.
- Altération ou perte d'intégrité des données.

Critère spécifique à SAP • Critère 4

Critère spécifique à SAP : NON

Preuves à demander

- Vérifier sur un échantillon représentatif des changements (ordres de transport ou autres) qui ont été effectués par des acteurs habilités.

Bonnes pratiques

- Vérifier régulièrement que seuls les acteurs concernés sont déclarés.

CRITÈRE 5 • Lorsqu'une modification ne peut pas être contenue dans un ordre de transport, une procédure doit clairement et formellement documenter le « geste de modification »

Commentaires • Critère 5

RAS.

Risques • Critère 5

- Niveau de service insuffisant.
- Arrêt non planifié de l'exploitation.
- Perte de données.
- Altération ou perte d'intégrité des données.

Critère spécifique à SAP • Critère 5

Critère spécifique à SAP : OUI

Preuves à demander

- Les changements réalisés manuellement et directement sur les différents environnements doivent être identifiés, tracés et formellement documentés.

Bonnes pratiques

- Trois étapes minimum dans le processus : Le processus doit contenir une étape d'approbation du changement. Une étape de validation de la recette. Une étape d'approbation avant la mise en œuvre du changement (Change Advisory Board).

CRITÈRE 6 • Toutes les activités du processus sont auditables

Commentaires • Critère 6

RAS.

Risques • Critère 6

- Perte de traçabilité.

Critère spécifique à SAP • Critère 6

Critère spécifique à SAP : OUI

Preuves à demander

- Vérifier sur un échantillon représentatif des changements (ordres de transport ou autres) que les mises en production sont tracées et correspondent aux demandes effectuées.

Bonnes pratiques

- Les activités du processus sont tracées et documentées.

OBJECTIF DE CONTRÔLE N°2

• SÉCURISER LES CHANGEMENTS

CRITÈRE 1 • La procédure pour la gestion des mandants est définie, documentée et communiquée à toutes les parties prenantes

Commentaires • Critère 1

Les options de modification du mandant doivent être décrites.

Risques • Critère 1

- Perte de traçabilité.
- Altération ou perte d'intégrité des données.

Critère spécifique à SAP • Critère 1

Critère spécifique à SAP : OUI

Preuves à demander

- Le document de configuration des mandants.

Bonnes pratiques

- Tenir à jour la liste des mandants et leurs paramétrages.

CRITÈRE 2 • La gestion des mandants d'une application SAP n'est autorisée que pour les utilisateurs définis

Commentaires • Critère 2

RAS.

Risques • Critère 2

- Perte de traçabilité.
- Altération ou perte d'intégrité des données.

Critère spécifique à SAP • Critère 2

Critère spécifique à SAP : OUI

Preuves à demander

- Définition des acteurs.
- Seules les personnes dûment habilitées disposent des droits nécessaires et suffisants pour modifier les mandants.

Bonnes pratiques

- Les autorisations nécessaires pour gérer le paramétrage inter-mandants (S_TABU_DIS) sont correctement attribuées.
- Les autorisations nécessaires pour gérer le paramétrage dépendant du mandant (S_TABU_CLI) sont correctement attribuées.

CRITÈRE 3 • Tout développement spécifique garantit le contrôle d'autorisation

Commentaires • Critère 3

Sans contrôle de sécurité dans les objets spécifiques (programmes, tables) la sécurité des informations n'est pas assurée.

Risques • Critère 3

- Accès non autorisé ou frauduleux.

Critère spécifique à SAP • Critère 3

Critère spécifique à SAP : OUI

Preuves à demander

- L'expression de besoin doit contenir un chapitre sur les contrôles d'autorisation.
- La recette comporte un test de contrôle des autorisations.

Bonnes pratiques

- L'utilisation des « authority-cheks » dans tous les développements spécifiques est obligatoire.
- Tous les programmes spécifiques sont affectés à un groupe d'autorisation.
- Toutes les tables spécifiques sont affectées à un groupe d'autorisation.

CRITÈRE 4 • La version des objets livrés est garantie

Commentaires • Critère 4

S'assurer que la livraison des objets est faite dans un ordre cohérent pour l'application afin d'éviter notamment une régression.

Risques • Critère 4

- Perte de traçabilité.
- Altération ou perte d'intégrité des données.

Critère spécifique à SAP • Critère 4

Critère spécifique à SAP : OUI

Preuves à demander

- Processus de contrôle de cohérence et de gestion des versions des objets.

Bonnes pratiques

- Il existe une gestion des versions des objets.

OBJECTIF DE CONTRÔLE N°3

• SÉCURISER LA PLATEFORME DE PRODUCTION

CRITÈRE 1 • Le mandant de production doit être protégé contre la modification et l'écrasement

Commentaires • Critère 1

La configuration du mandant est structurante vis-à-vis de fonctionnalités offertes en standard.

Risques • Critère 1

- Niveau de service insuffisant.
- Arrêt non planifié de l'exploitation.
- Perte de données.
- Altération ou perte d'intégrité des données.

Critère spécifique à SAP • Critère 1

Critère spécifique à SAP : OUI

Preuves à demander

- La configuration du mandant de production.

Bonnes pratiques

- Configuration en fonctionnement normal : Type de mandant « productif ». Aucune modification autorisée.
- Aucune modification des objets Repository/Customizing inter-mandants.

CRITÈRE 2 • La plateforme productive est séparée des plateformes non-productives

Commentaires • Critère 2

RAS.

Risques • Critère 2

- Niveau de service insuffisant.
- Arrêt non planifié de l'exploitation.
- Perte de données.
- Accès non autorisé ou frauduleux.

Critère spécifique à SAP • Critère 2

Critère spécifique à SAP : NON

Preuves à demander

- Dossier d'architecture technique contenant la définition du réseau et des machines des différents environnements.

Bonnes pratiques

- Le système de production est sur un sous-réseau dédié et indépendant des systèmes non-productifs. Il est sur un ou des serveurs dédiés à la production.

CRITÈRE 3 • Les utilisateurs ayant une clé de développement doivent être identifiés. Leur compte doit être inexistant ou bloqué sur le système de production

Commentaires • Critère 3

RAS.

Risques • Critère 3

- Niveau de service insuffisant.
- Arrêt non planifié de l'exploitation.
- Perte de données.
- Accès non autorisé ou frauduleux.

Critère spécifique à SAP • Critère 3

Critère spécifique à SAP : OUI

Preuves à demander

- Définition des acteurs.
- Seules les personnes dûment habilitées disposent des droits nécessaires et suffisants pour développer en production.

Bonnes pratiques

- Vérifier périodiquement les entrées présentes dans la table DEVACCESS.
- Tout compte utilisateur disposant de droits en développement est bloqué en mode normal.

CRITÈRE 4 • L'utilisation du mode « debug » en production doit être formellement documenté

Commentaires • Critère 4

Le mode « debug » permet d'altérer des données ou d'accéder à des informations non autorisées.

Risques • Critère 4

- Niveau de service insuffisant.
- Arrêt non planifié de l'exploitation.
- Perte de données.
- Altération ou perte d'intégrité des données.
- Accès non autorisé ou frauduleux.

Critère spécifique à SAP • Critère 4

Critère spécifique à SAP : OUI

Preuves à demander

- Processus de mise en œuvre du mode « debug » en production.
- Liste des utilisateurs disposant des droits « debug » en production.
- En mode normal, demander la valeur du paramètre rdisp/wpdbug_max_no

Bonnes pratiques

- En fonctionnement normal, aucun compte utilisateur n'est autorisé à utiliser le mode « debug » en lecture ou en modification sur le système de production.
- En mode normal, la valeur du paramètre rdisp/wpdbug_max_no est à 0.

Référentiel des risques

Les onze risques identifiés sur le sujet sont :

- Accès non autorisés ou frauduleux.
- Arrêt non planifié de l'exploitation.
- Niveau de service insuffisant.
- Non maîtrise des dépenses.
- Non-respect des exigences réglementaires ou légal.
- Perte de données.
- Vol de données.
- Altération ou perte d'intégrité des données.
- Perte de traçabilité.
- Perte d'image.
- Usurpation d'identité.

Glossaire

Core models : Socle applicatif commun dans le cadre du déploiement d'un ERP « Groupe » généralement au sein d'un groupe afin de promouvoir une structure fonctionnelle commune à l'ensemble des entités du groupe et bénéficier de règles communes. Le paramétrage est dans ce cas définit en central et seulement quelques adaptations aux contraintes locales peuvent être tolérées.

Dialogue : Type de compte représentant les utilisateurs « humain » (par opposition aux utilisateurs de services). Ces types de comptes sont accessibles via l'enregistrement d'un identifiant et d'un mot de passe personnalisés.

Environnement : Un environnement désigne, pour une application, l'ensemble des matériels et des logiciels système, dont le système d'exploitation, sur lesquels sont exécutés les programmes de l'application (environnement de développement, de recette, de production, etc).

Enterprise Resource Planning (ERP) ou Progiciel de Gestion Intégré (PGI) : Signifie littéralement en anglais, « planification des ressources de l'entreprise ». Ce type de logiciel correspond, pour une organisation, au support de base capable d'assurer une « gestion intégrée », définie comme étant l'interconnexion et l'intégration de l'ensemble des fonctions de l'entreprise dans un système informatique centralisé.

Gouvernance du système d'information : La gouvernance par l'entreprise ou l'organisation de son système d'information est une démarche de pilotage, concernant l'ensemble des responsables et pas seulement la Direction des Systèmes d'Information (DSI), ayant pour objectifs :

- d'apporter une contribution maximale à la création de valeur pour l'organisation,
- d'aligner le système d'information sur la stratégie de l'organisation,
- d'optimiser l'utilisation des ressources,
- et de maîtriser les risques en fonction des enjeux de l'organisation.

(Source : guide d'audit : gouvernance du système d'information)

Hacking : Désigne une activité visant à échanger « discrètement » des informations illégales et / ou personnelles, à contourner les protections d'un logiciel, d'un système ou d'un réseau informatique. (Larousse)

IDOC : IDOC est un message type de SAP, conteneur de données, pour assurer une communication entre deux systèmes applicatifs. (Source : SAP)

IDS (Intrusion Detection System) : Système destiné à analyser les activités et à relever celles suspectes ou anormales sur une cible (réseau ou système hôte). Il permet ainsi de prendre connaissance des tentatives d'intrusion.

Incidents : Un incident est un évènement impromptu et non répétitif, affectant le fonctionnement attendu d'un système. La gestion de ces incidents est une démarche réactive.

Interface : Une interface est un ensemble normalisé de classes, de méthodes ou de fonctions qui sert de façade par laquelle un logiciel offre des services à d'autres logiciels.

Logs : Le concept de log désigne l'enregistrement séquentiel dans un fichier ou une base de données de tous les événements affectant un processus particulier (application, activité d'un réseau informatique...). Le journal (en anglais log file ou plus simplement log), désigne alors le fichier contenant ces enregistrements.

Mandant : Niveau le plus élevé des données de SAP. Chaque mandant contient des données propres qui sont complètement séparées des données des autres mandants.

Matrice RACI : La matrice RACI donne une vision simple et claire de qui fait quoi dans le projet, en permettant d'éviter une redondance de rôles ou une dilution des responsabilités.

R = Réalisateur,
A = Autorité ou responsable,
C = Consulté,
I = Informé (en Anglais Responsible, Accountable, Consulted, Informed).

(Source : CI du SI IFACI Cigref)

Mise en production : Début d'utilisation d'un logiciel ou d'un module sur des données réelles dans le cadre d'un travail effectif.

Monitoring réseau : Désigne la surveillance et le pilotage d'un système en vue d'assurer son fonctionnement optimal.

Niveau de service : Niveau de qualité de services en termes d'indicateurs de performance et de délais de résolution des incidents. Un niveau de service est un objectif autour duquel l'entité doit rendre des comptes.

Pare-feux : Désigne les règles d'accès entre deux réseaux. Il permet ainsi de filtrer les paquets de données échangés avec le réseau.

Plan Assurance Qualité (PAQ) : Ce document définit la qualité de service attendue dans le cadre d'une prestation de service. Il contient notamment les indicateurs permettant d'évaluer la performance du prestataire et les pénalités en cas de défaut.

Problèmes : Un problème désigne un incident récurrent pour laquelle un diagnostic spécifique de l'origine et de la source afin de traiter de manière préventive.

Politique de sécurité des systèmes d'information (PSSI) : La politique de sécurité des systèmes d'information (PSSI) est un plan d'actions définies pour maintenir un certain niveau de sécurité. Elle reflète la vision stratégique de la direction de l'organisme en matière de sécurité des systèmes d'information (SSI).

RACI : R = Responsible,
A = Accountable (on utilise aussi parfois le terme Approuver),
C = Consulted,
I = Informed.

Requêter : Désigne l'action de « questionner » une base de données au travers d'une requête formulée en langage informatique.

Remote Function Call (RFC) : Interface propriétaire SAP AG pour la communication entre un système SAP et un système SAP ou un autre compatible tiers.

Salles blanches : Salle conçue pour maintenir à température, et l'hygrométrie à des valeurs déterminées. On y place les serveurs informatiques.

SAP Router : Un routeur SAP est un programme SAP qui agit comme une poste intermédiaire (proxy) dans une connexion réseau entre systèmes SAP ou entre des systèmes SAP et des réseaux externes.

Sécurité du SI : Regroupe les problématiques de restriction des accès à l'information à un niveau logique et physique.

Service Level Agreement (SLA) ou Contrat de services : Un plan d'assurance qualité décrit les dispositions mises en œuvre quant à la réalisation d'un produit ou d'un service afin de répondre aux exigences de qualité exigée par un client. Il permet aux différents partis de s'accorder sur le contexte, le périmètre et les enjeux concernant la prestation à réaliser.

Transport : Désigne un groupement utilisé pour transférer des données d'une installation de SAP à une autre.

Virus : Automate auto-réplicatif conçu pour se propager à d'autres ordinateur en s'insérant dans des logiciels légitimes « hôtes ».

Règles de pare-feu : Il s'agit des paramètres utilisés dans les règles d'accès entre deux réseaux. Il permet ainsi de filtrer les paquets de données échangés avec le réseau (cf pare-feu).

Zone démilitarisée (DMZ) : Désigne une zone isolée du réseau hébergeant les applications mises à disposition du public. Elle permet ainsi de séparer le réseau à protéger du réseau « hostile ».

Référentiel : Ensemble de bases de données contenant les « références » d'un système d'information. Un référentiel clair, logique et précis est un des gages de bonne interopérabilité d'un système d'information. Les « données de référence » (ou métadonnées) :

- Ce sont les données principales : clients, nomenclatures de produits / services, annuaires (de l'organisation, des personnes, des équipements, etc), etc.
- Elles sont décrites dans un dictionnaire de données, vocabulaire commun de l'organisation, visant à préciser leurs définitions (sens) et leurs propriétés.
- Elles sont stockées physiquement dans une base de données spéciale, où les applications peuvent les retrouver chaque fois qu'elles en ont besoin.

(Source : wikipedia)

Security, Audit and Control Features : SAP ERP, 3rd Edition - Audit / Assurance Programs and ICQs.

This publication updates the 2006 edition of this practical, how-to guide in the technical and risk management series. It enables assurance, security and risk professionals (both IT and non-IT) to evaluate risks and controls in existing ERP implementations and facilitates the design and building of better practice controls into system upgrades and enhancements. While many of the features and testing techniques described are also applicable to the earlier versions of SAP R / 3, namely 4.6c and 4.7, this publication is designed to be a practical guide based on SAP ECC versions 5.0 and 6.0.

Publié par "**Information Systems Audit and Control Association**" (ISACA).

Global Technology Audit Guide (GTAGs) disponiblent sur le site de l'IFACI et notamment les GTAG suivants :

- GTAG 10 - Business Continuity Management.
- GTAG 9 - Identity and Access Management.
- GTAG 15 - Information Security Governance.
- GTAG 8 - Auditing application controls.

Qu'est-ce que SAP ?

Créée en 1972, SAP est une entreprise allemande qui conçoit et vend des logiciels de gestion principalement à destination des entreprises et institutions dans le monde entier. C'est le plus gros concepteur de logiciels en Europe et l'un des cinq premiers dans le monde. Son produit le plus connu est le progiciel de gestion intégré SAP ERP[2] permettant de gérer les fonctions de l'entreprise (finances, ventes, achats, production, logistique, ressources humaines, etc). Ces fonctionnalités sont très souvent proposées sous la forme de modules, comme par exemple :

- **FI** pour la comptabilité.
- **CO** pour le contrôle de gestion.
- **SRM** pour la gestion des relations fournisseurs.

Depuis quelques années, SAP a eu une croissance forte en rachetant d'autres éditeurs de progiciels dont les plus significatifs sont :

- BusinessObjects en 2008, spécialisé dans la Business Intelligence et le décisionnel, et qui détenait dans son périmètre le progiciel de consolidation très répandu sur le marché français MAGNITUDE (devenu SAP BFC).
- Sybase en 2010, spécialisée dans les bases de données et mobilité.
- SuccessFactors en 2012, solutions de Gestion des Ressources Humaines (GRH) en mode Cloud Computing.
- Ariba en 2012, solutions de e-commerce en mode Cloud Computing.

[2] Enterprise Resource Planning (ERP), signifiant littéralement en anglais, « planification des ressources de l'entreprise », et traduit en français par « Progiciel de Gestion Intégré » (PGI). Ce type de logiciel correspond, pour une organisation, au système capable d'assurer une « gestion intégrée », définie comme étant l'interconnexion et l'intégration de l'ensemble des fonctions de l'entreprise dans un système informatique centralisé.

Les groupes d'utilisateurs sont des organisations plus ou moins indépendantes de l'éditeur et des fournisseurs (en fonctions des pays) et permettent à ses membres de s'informer, d'influencer sur la conception et l'amélioration des produits SAP, d'échanger des conseils et d'illustrer les besoins et tendances du marché. Parmi les groupes d'utilisateurs les plus importants, on peut citer l'ASSUG (Etats Unis), le DSAG (Allemagne), VSNG (Hollande), SAP UK and Ireland et l'USF (le club des utilisateurs francophones). Il est à noter que l'USF est totalement indépendant de SAP (pas de financement de SAP notamment) et qu'aucun fournisseur de services n'est membre de l'USF.

En 2007, le SUGEN (SAP User Group Executive Network) a été créé en associant les quinze plus grands clubs utilisateurs mondiaux.

Présentation des 3 associations

L'AFAI est le chapitre français de l'ISACA, organisation internationale qui regroupe 110 000 membres dans 180 pays. L'association rassemble plus de 1000 professionnels autour des problématiques transversales liées à la gouvernance, au risque, à l'audit et la sécurité des systèmes d'information, ainsi qu'à la diffusion des meilleures pratiques associées. Elle a également une activité de formation tournée notamment vers la certification professionnelle.

L'AFAI conduit ses travaux autour des deux piliers que sont la confiance dans les systèmes d'information et la création de valeur, tout en décloisonnant la réflexion par la prise en compte des enjeux stratégiques, managériaux, humains, technologiques, financiers ou juridiques. Elle est la seule association à accueillir au sein de ses groupes de travail l'ensemble des acteurs concernés par les systèmes d'information dans l'entreprise et hors de l'entreprise.

Plus d'informations sur : www.afai.fr

L'Institut Français de l'Audit et du Contrôle Interne (IFACI) rassemble plus de 5 600 professionnels de l'audit et du contrôle internes et, plus largement, de toutes les fonctions contribuant à la maîtrise des risques. L'Institut favorise la diffusion des normes internationales de l'audit interne et des meilleures pratiques des métiers de la maîtrise des risques. Lieu de partage et d'accompagnement, il est l'organisme de référence en matière de formation professionnelle dans ces domaines.

Ainsi, l'IFACI constitue le partenaire privilégié des organisations publiques et privées de toutes tailles souhaitant améliorer l'efficacité de leurs dispositifs de gouvernance, de maîtrise des risques et de contrôle interne.

L'IFACI est affilié à The Institute of Internal Auditors (The IIA) qui bénéficie d'un réseau de 180 000 adhérents.

www.ifaci.com

Créée en 1989, l'association des utilisateurs francophones des solutions SAP est une association 1901, indépendante de l'éditeur. L'USF a pour objectif **l'échange de connaissances** et **le partage d'expériences** entre les utilisateurs francophones de toutes les solutions SAP et les personnes intéressées par ce domaine ainsi que l'influence sur l'éditeur SAP.

www.usf.fr

www.afai.fr

www.ifaci.com

www.usf.fr

Conception : K-factory.fr] 02 40 58 21 06 / Imprimerie Imprimatur 01 55 90 29 20