Processus d'évaluation des risques du BVG

Guide de référence sur les risques liés à l'informatique

Bureau du vérificateur général du Canada

Office of the Auditor General of Canada

déc.–2022
Propriétaire du modèle : Audit TI

Guide de référence sur les risques liés à l'informatique

Table des matières

Introduction

Le présent guide de référence donne une vue d'ensemble des concepts et des exigences clés pour acquérir une compréhension de l'environnement informatique de l'entité, d'identifier les risques liés à l'informatique et les CGI qui répondent à ces risques. Ces sujets sont examinés en profondeur dans la section BVG Audit 5035.2, dans le cadre des phases de compréhension et d'identification du processus d'évaluation des risques du BVG.

C'est en identifiant les applications informatiques et d'autres aspects de l'environnement informatique (p. ex. bases de données, système d'exploitation, réseau) pertinents pour la préparation des états financiers que les équipes de mission sont en mesure d'identifier les risques découlant du recours à l'informatique et les contrôles généraux informatiques (CGI) connexes qui répondent à ces risques. Cela permet à l'équipe de mission de comprendre l'entité, d'identifier et d'évaluer les risques d'anomalies significatives, d'évaluer le risque lié aux contrôles tel que documenté par la détermination de l'auditeur du degré d'appui sur les contrôles (c.-à-d. aucun, partiel ou élevé), ainsi que d'élaborer des réponses d'audit efficaces et efficientes à l'égard des risques d'anomalies significatives.

Un sommaire des rappels importants se trouve à la page suivante, suivi d'information détaillée sur les considérations pertinentes par rapport à la compréhension de l'environnement informatique de l'entité et à l'identification des risques informatique et des CGI connexes.

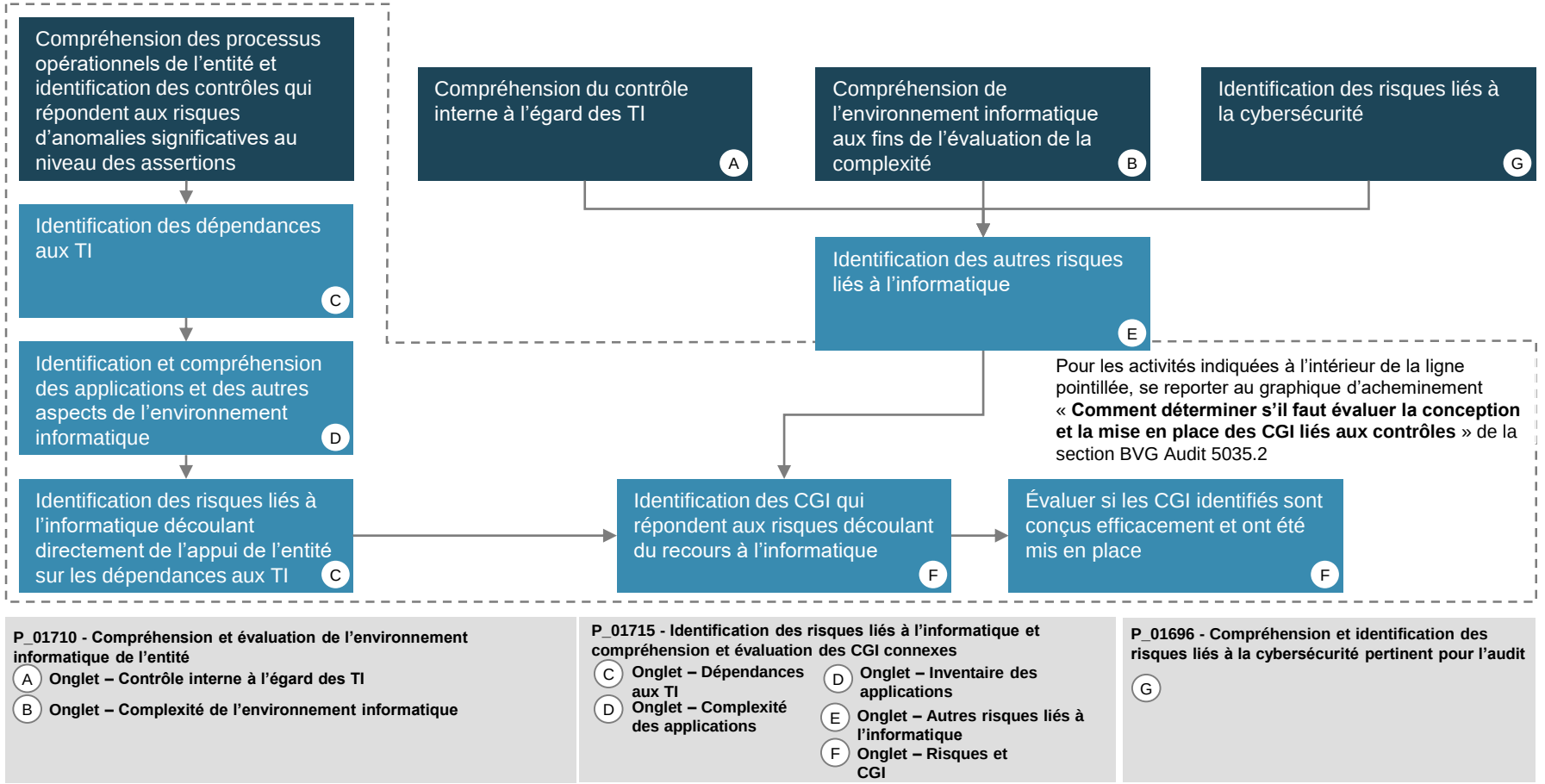
Le présent guide de référence, qui comprend des renvois aux sections pertinentes du Manuel d'audit annuel du BVG, ne remplace pas la lecture des exigences et des directives détaillées dans le Manuel d'audit annuel du BVG. Pour obtenir des directives détaillées, reportez-vous aux sections BVG Audit 5034 et 5035 ou communiquez avec l'Audit des TI et/ou l'Assistance aux missions d'audit (AMA) si vous avez des questions.

Rappels importants

- Il faut acquérir une compréhension détaillée de l'environnement informatique de l'entité pour déterminer le niveau de complexité et, par conséquent, l'étendue des compétences spécialisées nécessaires pour la mission. Cela peut exiger une participation accrue des spécialistes de l'Audit des TI à l'audit et il faut en tenir compte dans la planification des besoins en matière de ressources pour la mission.
- La section BVG Audit 3102 sur la participation de l'Audit des TI a été mise à jour pour l'aligner sur les niveaux de complexité de l'environnement informatique présentés dans la norme d'évaluation des risques révisée (non complexe, modérément complexe et complexe).
- Pour identifier les risques découlant du recours à l'informatique et les CGI connexes qui répondent à ces risques, il faut d'abord acquérir une compréhension rigoureuse des processus opérationnels et identifier les **contrôles de la composante « activités de contrôle »** du système de contrôle interne de l'entité.
- Il faut identifier les risques liés à l'informatique et les CGI connexes peu importe si l'équipe prévoit tester les contrôles de l'entité ou si elle prévoit plutôt adopter une approche entièrement fondée sur les procédures de corroboration, car on s'attend à ce que ces risques soient pertinents pour toute entité ayant recours à l'informatique.
- L'équipe doit évaluer la conception et la mise en place de tous les CGI identifiés qui répondent aux risques découlant du recours à l'informatique.
    - Si les contrôles ont été conçus et mis en place de façon appropriée, il faut déterminer si le test de l'efficacité du fonctionnement de ces CGI est une stratégie efficiente et efficace.
    - Si les contrôles n'ont pas été conçus ou mis en place efficacement, il faut déterminer l'incidence de la déficience et du risque lié à l'informatique sur la nature, le calendrier et l'étendue des procédures de corroboration ou des tests des contrôles en réponse à l'évaluation des risques d'anomalies significatives au niveau des états financiers et des assertions.
- Les nouvelles procédures d'évaluation des risques sont disponibles afin de permettent à l'équipe de documenter de manière efficiente et efficace sa compréhension de l'environnement informatique, d' identifiés des risques liés à l'informatique (y compris l'automatisation de l'identification des risques liés à l'informatique couramment mis en place) et des CGI.

Identification des risques découlant du recours à l'informatique par l'entité et des CGI de l'entité qui répondent à ces risques

(cliquez sur chaque élément pour obtenir des détails)



P_01710 - Compréhension et évaluation de l'environnement informatique de l'entité

- A **Onglet – Contrôle interne à l'égard des TI**
- B **Onglet – Complexité de l'environnement informatique**

P_01715 - Identification des risques liés à l'informatique et compréhension et évaluation des CGI connexes

- C **Onglet – Dépendances aux TI**
- D **Onglet – Complexité des applications**
- D **Onglet – Inventaire des applications**
- E **Onglet – Autres risques liés à l'informatique**
- F **Onglet – Risques et CGI**

P_01696 - Compréhension et identification des risques liés à la cybersécurité pertinent pour l'audit

- G

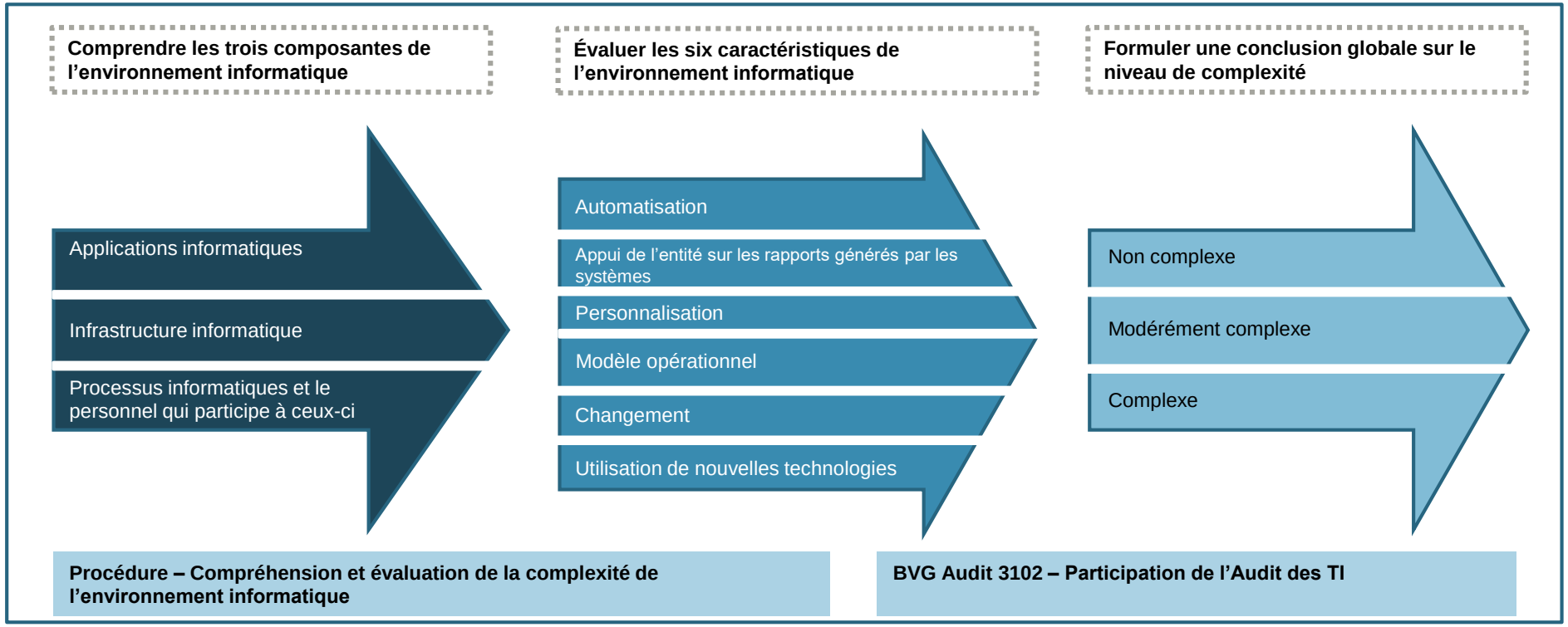
Compréhension de l’environnement informatique et évaluation de la complexité

Compréhension des processus opérationnels de l’entité et identification des contrôles qui répondent aux risques d’anomalies significatives au niveau des assertions

Compréhension du contrôle interne à l’égard des TI (A)

Compréhension de l’environnement informatique aux fins de l’évaluation de la complexité (B)

Identification des risques liés à la cybersécurité (G)



Risques liés à l’informatique découlant directement de l’appui de l’entité sur les dépendances aux TI

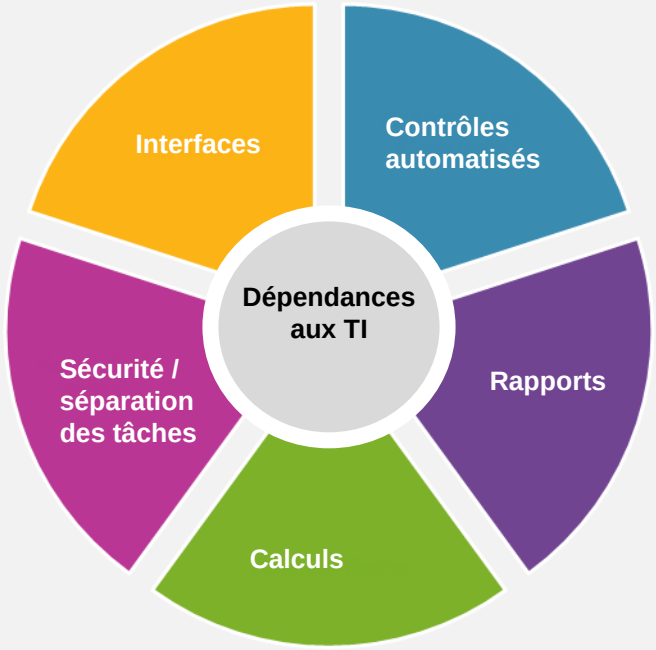
Compréhension des processus opérationnels de l’entité et identification des contrôles qui répondent aux risques d’anomalies significatives au niveau des assertions

Identification des dépendances aux TI C

Identification et compréhension des applications et des autres aspects de l’environnement informatique D

Identification des risques liés à l’informatique découlant directement de l’appui de l’entité sur les dépendances aux TI C

Cliquez sur les zones sensibles pour afficher plus d’informations.



Procédure – Identification des risques liés à l’informatique et compréhension et évaluation des CGI connexes

Guide pratique sur les risques liés à l’informatique

Risques liés à l’informatique découlant directement de l’appui de l’entité sur les dépendances aux TI

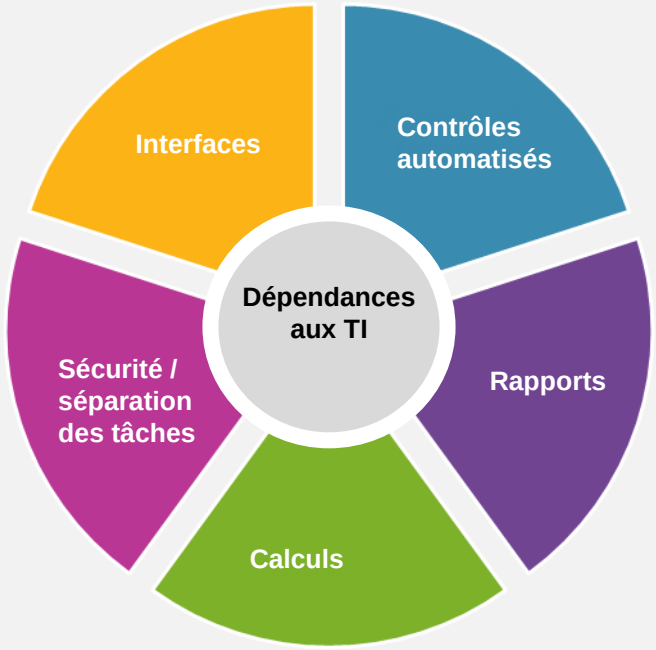
Compréhension des processus opérationnels de l’entité et identification des contrôles qui répondent aux risques d’anomalies significatives au niveau des assertions

Identification des dépendances aux TI C

Identification et compréhension des applications et des autres aspects de l’environnement informatique D

Identification des risques liés à l’informatique découlant directement de l’appui de l’entité sur les dépendances aux TI C

Cliquez sur les zones sensibles pour afficher plus d’informations.



Contrôles automatisés

Les contrôles automatisés sont intégrés dans l’environnement informatique pour appliquer les règles opérationnelles. Par exemple, de nombreuses applications informatiques effectuent des vérifications du format (p. ex. seul un format de date spécifique est accepté), des vérifications de l’existence (p. ex. le numéro du client existe dans le fichier maître) ou des vérifications du caractère raisonnable (p. ex. un montant maximal de paiement) lorsqu’une transaction est saisie.

Procédure – Identification des risques liés à l’informatique et compréhension et évaluation des CGI connexes

Guide pratique sur les risques liés à l’informatique

Risques liés à l’informatique découlant directement de l’appui de l’entité sur les dépendances aux TI

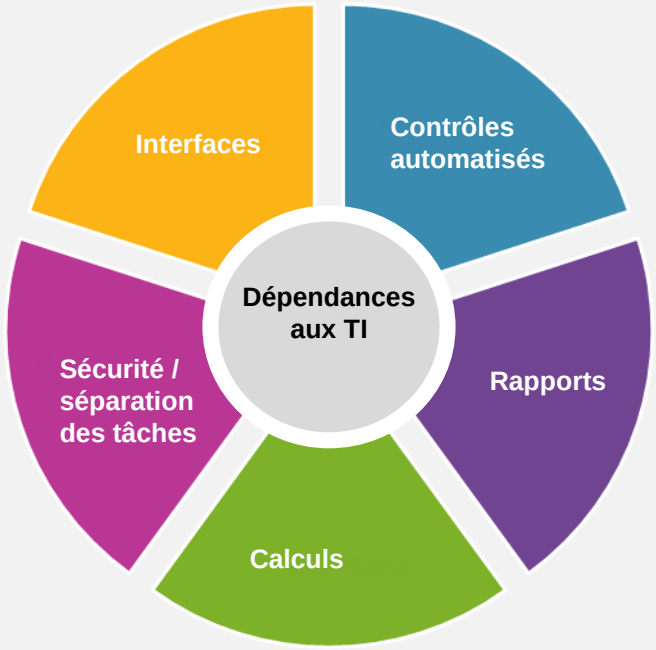
Compréhension des processus opérationnels de l’entité et identification des contrôles qui répondent aux risques d’anomalies significatives au niveau des assertions

Identification des dépendances aux TI C

Identification et compréhension des applications et des autres aspects de l’environnement informatique D

Identification des risques liés à l’informatique découlant directement de l’appui de l’entité sur les dépendances aux TI C

Cliquez sur les zones sensibles pour afficher plus d’informations.



Rapports

Les rapports générés par les systèmes sont des renseignements produits par les systèmes informatiques (p. ex. un classement chronologique des comptes clients utilisé pour calculer la correction de valeur pour pertes de crédit attendues). Ces rapports sont souvent utilisés dans l’exécution d’un contrôle manuel de l’entité, y compris les examens du rendement opérationnel, ou peuvent être une source d’information sur l’entité que l’équipe utilise pour sélectionner les éléments visés par des tests de détail ou mettre en œuvre une procédure analytique de corroboration.

Procédure – Identification des risques liés à l’informatique et compréhension et évaluation des CGI connexes

Guide pratique sur les risques liés à l’informatique

Risques liés à l’informatique découlant directement de l’appui de l’entité sur les dépendances aux TI

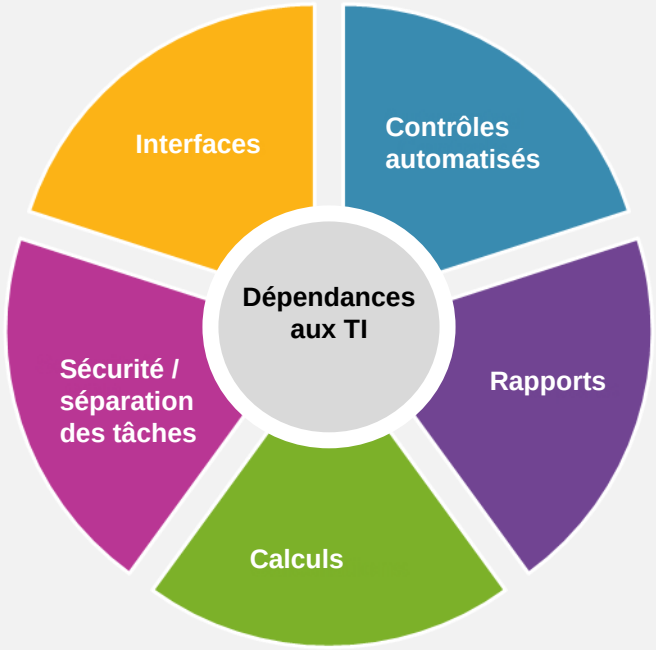
Compréhension des processus opérationnels de l’entité et identification des contrôles qui répondent aux risques d’anomalies significatives au niveau des assertions

Identification des dépendances aux TI C

Identification et compréhension des applications et des autres aspects de l’environnement informatique D

Identification des risques liés à l’informatique découlant directement de l’appui de l’entité sur les dépendances aux TI C

Cliquez sur les zones sensibles pour afficher plus d’informations.



Calculs

Les calculs sont des procédures comptables qui sont exécutées par un système informatique plutôt que par une personne. Par exemple, le système appliquera la méthode de l’amortissement linéaire pour calculer l’amortissement d’un actif (c.-à-d. le coût de l’actif moins la valeur résiduelle de l’actif à la fin de sa durée d’utilité, divisé par sa durée d’utilité) ou le système calculera la valeur du montant facturé à un client en multipliant le prix de l’article par la quantité expédiée.

Procédure – Identification des risques liés à l’informatique et compréhension et évaluation des CGI connexes

Guide pratique sur les risques liés à l’informatique

Risques liés à l’informatique découlant directement de l’appui de l’entité sur les dépendances aux TI

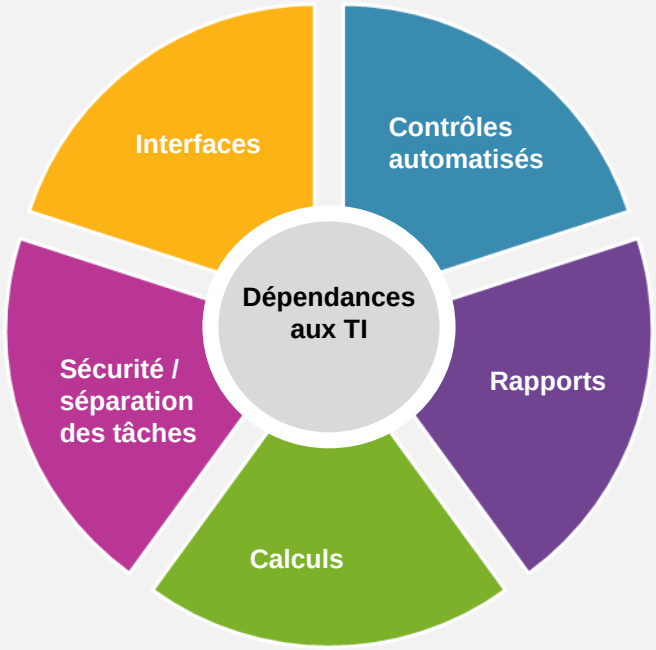
Compréhension des processus opérationnels de l’entité et identification des contrôles qui répondent aux risques d’anomalies significatives au niveau des assertions

Identification des dépendances aux TI C

Identification et compréhension des applications et des autres aspects de l’environnement informatique D

Identification des risques liés à l’informatique découlant directement de l’appui de l’entité sur les dépendances aux TI C

Cliquez sur les zones sensibles pour afficher plus d’informations.



Sécurité / séparation des tâches

La sécurité, notamment la séparation des tâches, est activée par l’environnement informatique pour restreindre l’accès à l’information et pour déterminer la répartition des rôles et des responsabilités qui pourraient permettre à un membre du personnel de faire ou de dissimuler une erreur ou une fraude, ou de traiter des erreurs qui passeraient inaperçues (p. ex. la séparation des rôles permettant de préparer et d’approuver les paiements versés aux fournisseurs).

Procédure – Identification des risques liés à l’informatique et compréhension et évaluation des CGI connexes

Guide pratique sur les risques liés à l’informatique

Risques liés à l’informatique découlant directement de l’appui de l’entité sur les dépendances aux TI

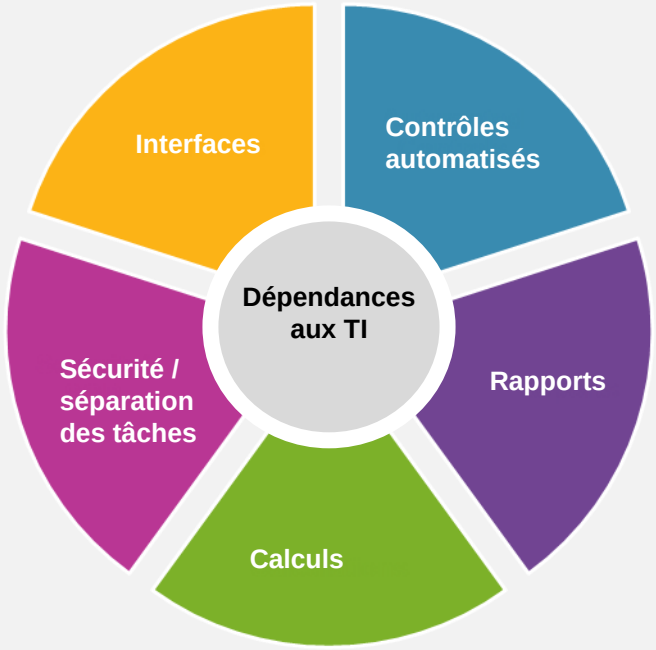
Compréhension des processus opérationnels de l’entité et identification des contrôles qui répondent aux risques d’anomalies significatives au niveau des assertions

Identification des dépendances aux TI C

Identification et compréhension des applications et des autres aspects de l’environnement informatique D

Identification des risques liés à l’informatique découlant directement de l’appui de l’entité sur les dépendances aux TI C

Cliquez sur les zones sensibles pour afficher plus d’informations.



Interfaces

Les interfaces sont des logiques programmées qui transfèrent des données d’un système informatique à un autre. Par exemple, une interface pourrait être programmée pour transférer les données d’un grand livre auxiliaire de paie dans un système informatique au grand livre général dans un autre système informatique.

Procédure – Identification des risques liés à l’informatique et compréhension et évaluation des CGI connexes

Guide pratique sur les risques liés à l’informatique

Risques liés à l’informatique découlant directement de l’appui de l’entité sur les dépendances aux TI

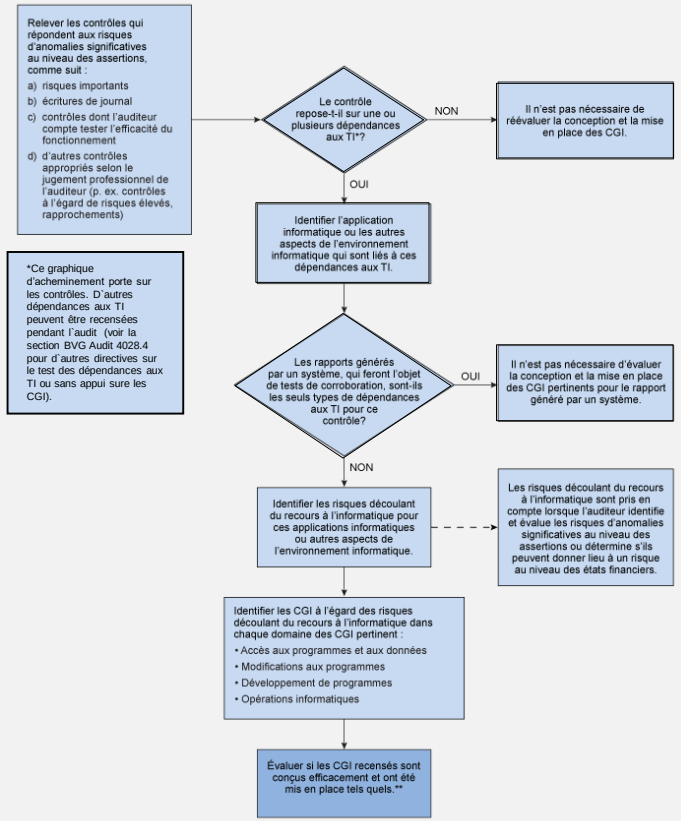
Compréhension des processus opérationnels de l’entité et identification des contrôles qui répondent aux risques d’anomalies significatives au niveau des assertions

Identification des dépendances aux TI C

Identification et compréhension des applications et des autres aspects de l’environnement informatique D

Identification des risques liés à l’informatique découlant directement de l’appui de l’entité sur les dépendances aux TI C

Comment déterminer s’il faut évaluer la conception et la mise en place des CGI liés aux contrôles



Cliquez sur les zones sensibles pour afficher plus d’informations.

Procédure – Identification des risques liés à l’informatique et compréhension et évaluation des CGI connexes

Guide pratique sur les risques liés à l’informatique

Risques liés à l’informatique découlant directement de l’appui de l’entité sur les dépendances aux TI

Précédent

Compréhension des processus opérationnels de l’entité et identification des contrôles qui répondent aux risques d’anomalies significatives au niveau des assertions

Identification des dépendances aux TI

C

Identification et compréhension des applications et des autres aspects de l’environnement informatique D

Identification des risques liés à l’informatique découlant directement de l’appui de l’entité sur les dépendances aux TI C

Comment déterminer s’il faut évaluer la conception et la mise en place des CGI liés aux contrôles

Relever les contrôles qui répondent aux risques d’anomalies significatives au niveau des assertions, comme suit :

a. risques importants
b. écritures de journal
c. contrôles dont l’auditeur compte tester l’efficacité du fonctionnement
d. autres contrôles appropriés selon le jugement professionnel de l’auditeur (p. ex. contrôles à l’égard de risques élevés, rapprochements)

La première étape consiste à identifier les contrôles de la composante « activités de contrôle » du système de contrôle interne de l’entité et à déterminer si ces contrôles s’appuient sur les dépendances aux TI.

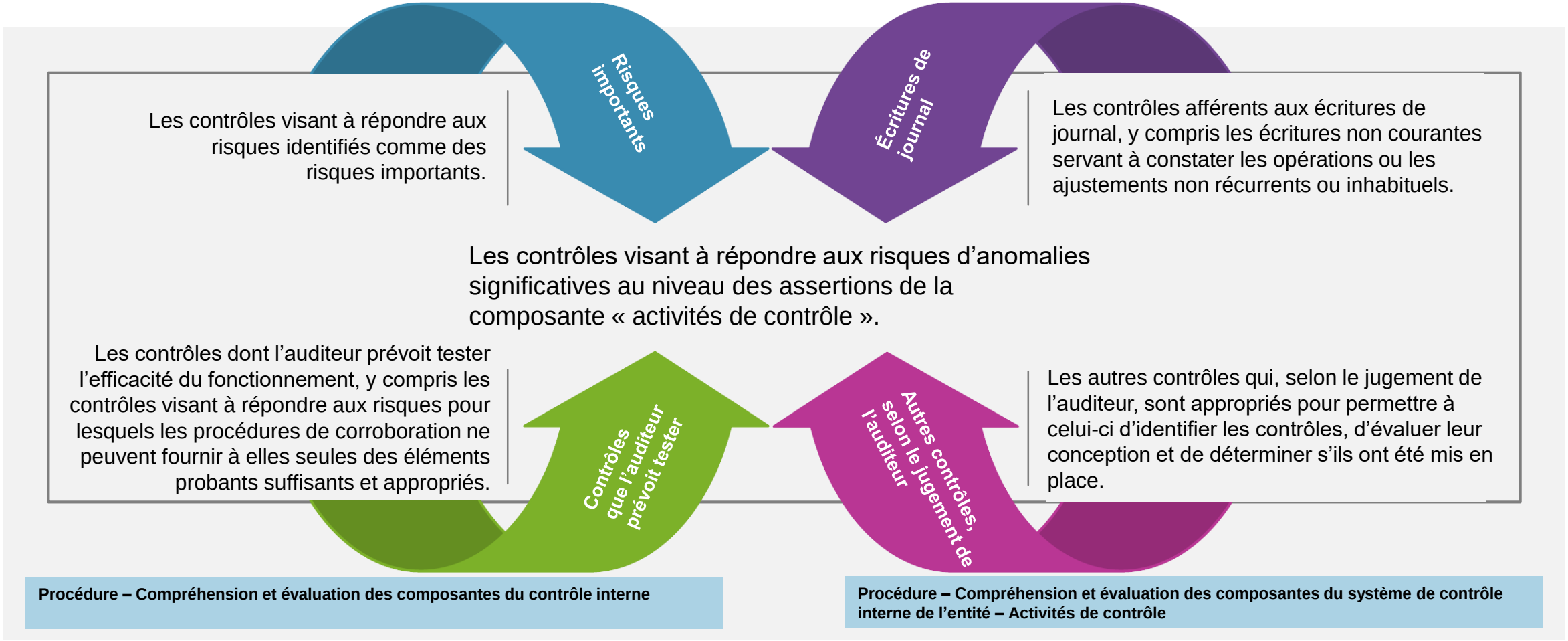
Voir la section BVG Audit 5035.1 pour obtenir des directives supplémentaires sur les types de contrôles faisant partie de cette composante.

Voir la section BVG Audit 5034 pour obtenir des directives sur les dépendances aux TI.

Procédure – Identification des risques liés à l’informatique et compréhension et évaluation des CGI connexes

Guide pratique sur les risques liés à l’informatique

Qu’est-ce qu’un contrôle de la composante « activités de contrôle »?



Risques liés à l’informatique découlant directement de l’appui de l’entité sur les dépendances aux TI

Précédent

Compréhension des processus opérationnels de l’entité et identification des contrôles qui répondent aux risques d’anomalies significatives au niveau des assertions

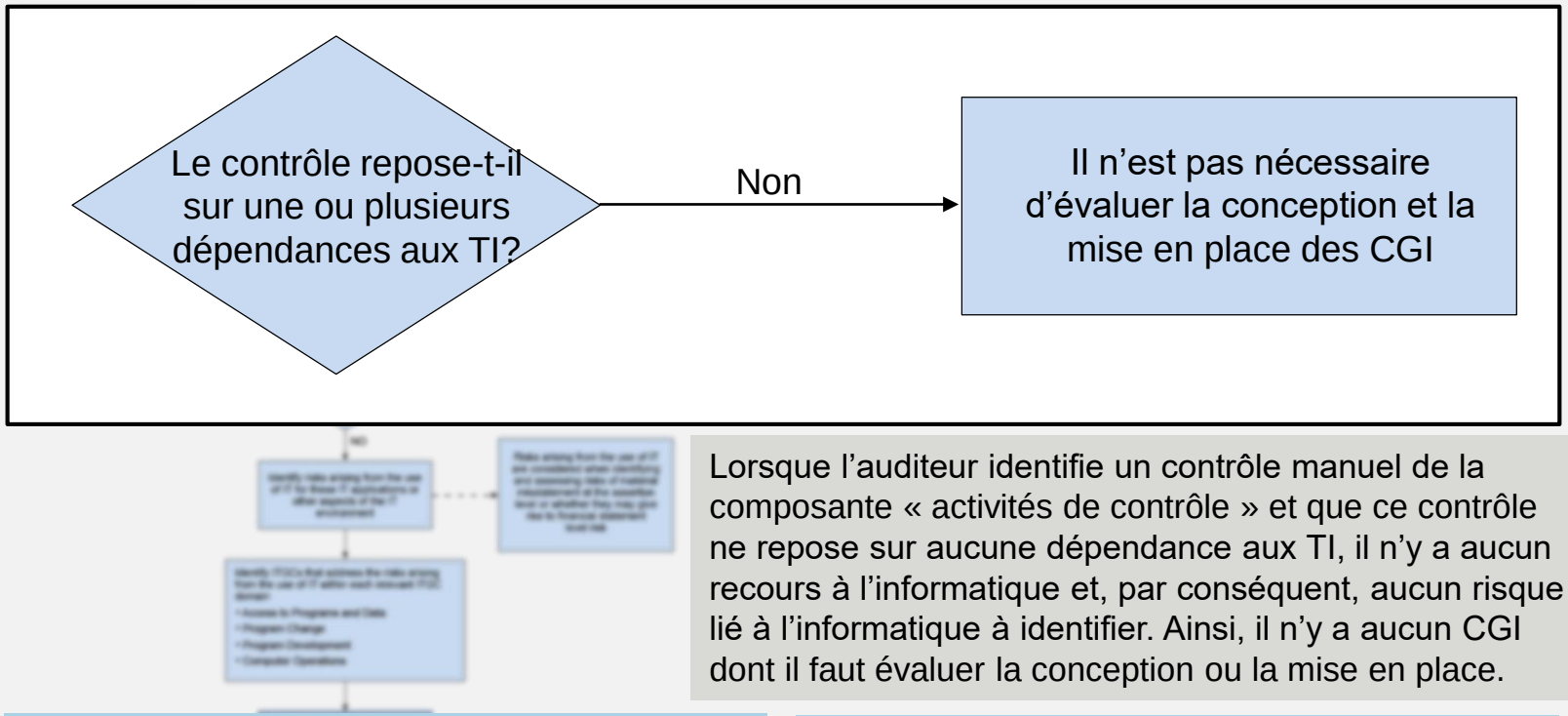
Identification des dépendances aux TI

C

Identification et compréhension des applications et des autres aspects de l’environnement informatique D

Identification des risques liés à l’informatique découlant directement de l’appui de l’entité sur les dépendances aux TI C

Comment déterminer s’il faut évaluer la conception et la mise en place des CGI liés aux contrôles



Lorsque l’auditeur identifie un contrôle manuel de la composante « activités de contrôle » et que ce contrôle ne repose sur aucune dépendance aux TI, il n’y a aucun recours à l’informatique et, par conséquent, aucun risque lié à l’informatique à identifier. Ainsi, il n’y a aucun CGI dont il faut évaluer la conception ou la mise en place.

Procédure – Identification des risques liés à l’informatique et compréhension et évaluation des CGI connexes

Guide pratique sur les risques liés à l’informatique

Risques liés à l'informatique découlant directement de l'appui de l'entité sur les dépendances aux TI

Précédent

Compréhension des processus opérationnels de l'entité et identification des contrôles qui répondent aux risques d'anomalies significatives au niveau des assertions

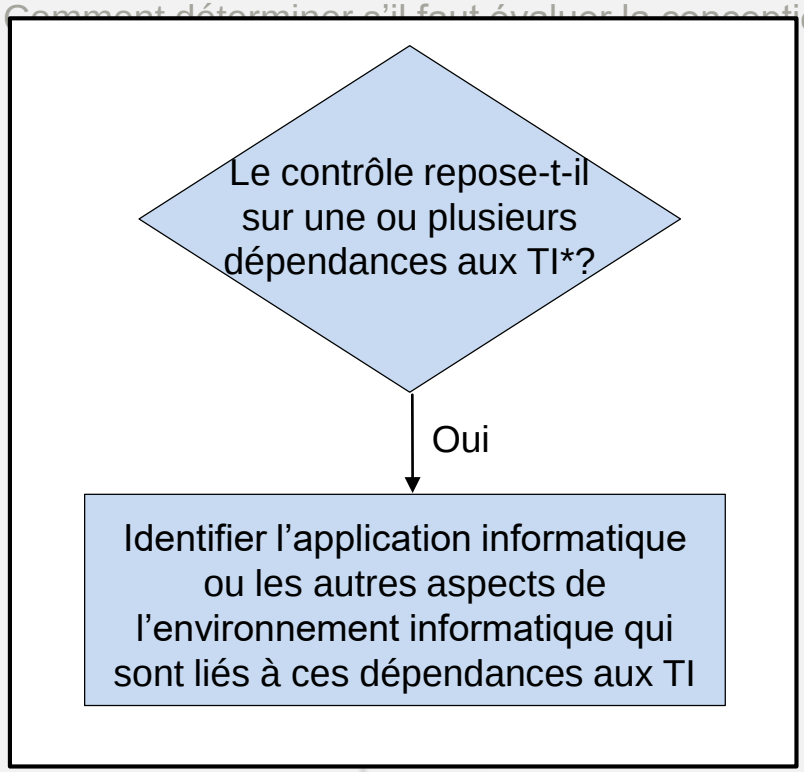
Identification des dépendances aux TI

C

Identification et compréhension des applications et des autres aspects de l'environnement informatique D

Identification des risques liés à l'informatique découlant directement de l'appui de l'entité sur les dépendances aux TI C

Comment déterminer s'il faut évaluer la conception et la mise en place des CGI liés aux contrôles



Lorsque l'équipe identifie un contrôle de la composante « activités de contrôle » et que ce contrôle repose sur une ou plusieurs dépendances aux TI (c.-à-d. un contrôle automatisé ou un contrôle manuel dépendant des TI), elle identifie, pour chaque dépendance aux TI, l'application et les autres aspects de l'environnement informatique afférents (y compris le type d'application, la base de données, le centre de données, le système d'exploitation et le nom du serveur) et détermine si ceux-ci sont exposés à des risques découlant du recours à l'informatique.

Procédure – Identification des risques liés à l'informatique et compréhension et évaluation des CGI connexes

Guide pratique sur les risques liés à l'informatique

Risques liés à l’informatique découlant directement de l’appui de l’entité sur les dépendances aux TI

Précédent

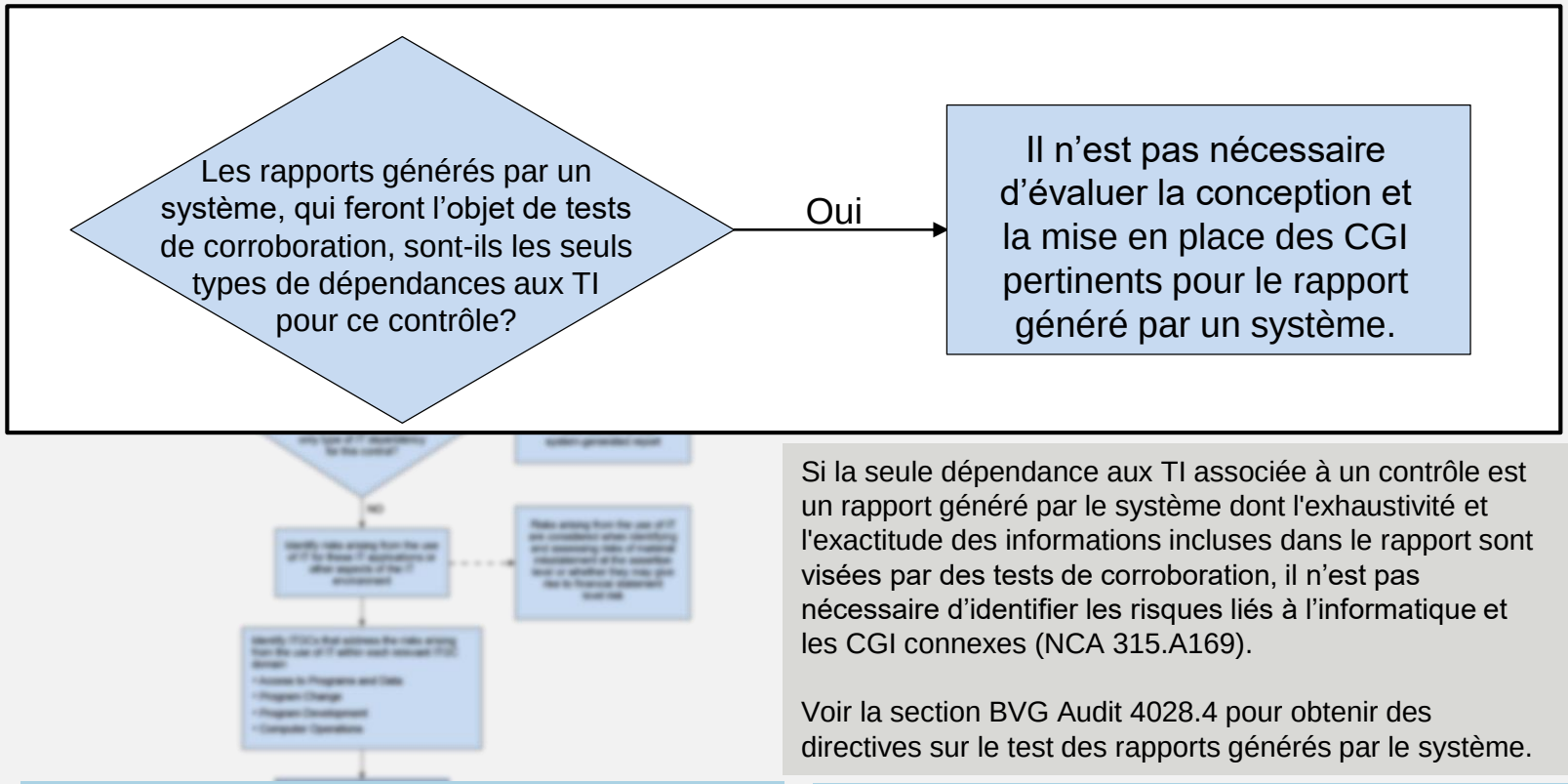
Compréhension des processus opérationnels de l’entité et identification des contrôles qui répondent aux risques d’anomalies significatives au niveau des assertions

Identification des dépendances aux TI

C

Identification et compréhension des applications et des autres aspects de l’environnement informatique D

Identification des risques liés à l’informatique découlant directement de l’appui de l’entité sur les dépendances aux TI C



Si la seule dépendance aux TI associée à un contrôle est un rapport généré par le système dont l'exhaustivité et l'exactitude des informations incluses dans le rapport sont visées par des tests de corroboration, il n’est pas nécessaire d’identifier les risques liés à l’informatique et les CGI connexes (NCA 315.A169).

Voir la section BVG Audit 4028.4 pour obtenir des directives sur le test des rapports générés par le système.

Procédure – Identification des risques liés à l’informatique et compréhension et évaluation des CGI connexes

Guide pratique sur les risques liés à l’informatique

Risques liés à l’informatique découlant directement de l’appui de l’entité sur les dépendances aux TI

Précédent

Compréhension des processus opérationnels de l’entité et identification des contrôles qui répondent aux risques d’anomalies significatives au niveau des assertions

Identification des dépendances aux TI

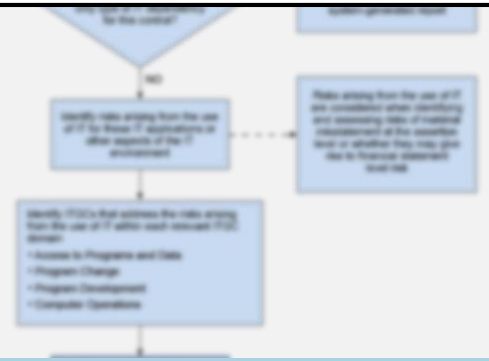
C

Identification et compréhension des applications et des autres aspects de l’environnement informatique D

Identification des risques liés à l’informatique découlant directement de l’appui de l’entité sur les dépendances aux TI C

Identifier les risques découlant du recours à l’informatique pour ces applications informatiques ou autres aspects de l’environnement informatique.

Les risques découlant du recours à l’informatique sont pris en compte lorsque l’auditeur identifie et évalue les risques d’anomalies significatives au niveau des assertions ou détermine s’ils peuvent donner lieu à un risque au niveau des états financiers.



Pour les rapports générés par le système dont les données d’entrée et de sortie ne seront pas visées par des tests de corroboration ou ne sont associées à aucune dépendance aux TI,
il faut identifier les risques pertinents découlant du recours à l’informatique.

Procédure – Identification des risques liés à l’informatique et compréhension et évaluation des CGI connexes

Guide pratique sur les risques liés à l’informatique

Risques liés à l'informatique découlant directement de l'appui de l'entité sur les dépendances aux TI

Précédent

Compréhension des processus opérationnels de l'entité et identification des contrôles qui répondent aux risques d'anomalies significatives au niveau des assertions

Identification des dépendances aux TI

C

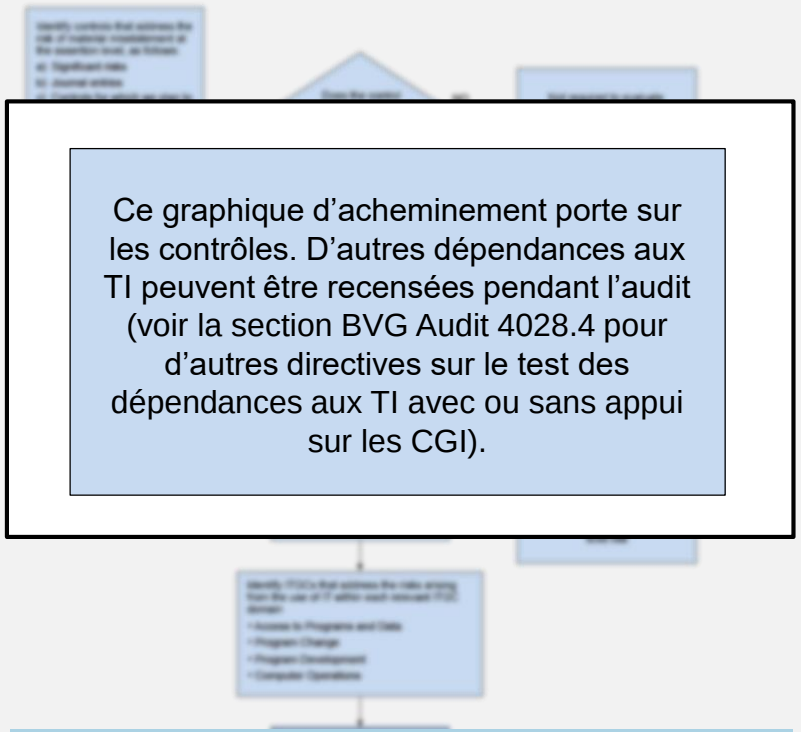
Identification et compréhension des applications et des autres aspects de l'environnement informatique

D

Identification des risques liés à l'informatique découlant directement de l'appui de l'entité sur les dépendances aux TI

C

Comment déterminer s'il faut évaluer la conception et la mise en place des CGI liés aux contrôles



Ce graphique d'acheminement porte sur les contrôles. D'autres dépendances aux TI peuvent être recensées pendant l'audit (voir la section BVG Audit 4028.4 pour d'autres directives sur le test des dépendances aux TI avec ou sans appui sur les CGI).

Si la dépendance aux TI a été jugée pertinente pour l'audit parce qu'elle sera utilisée comme base pour les procédures de corroboration (p. ex. un rapport généré par le système utilisé pour tester la valeur nette de réalisation des stocks, mais qui n'est pas utilisé par un contrôle de la composante « activités de contrôle »), l'auditeur applique le même processus présenté dans le graphique d'acheminement comme si la dépendance aux TI était un contrôle de la composante « activités de contrôle ».

Procédure – Identification des risques liés à l'informatique et compréhension et évaluation des CGI connexes

Guide pratique sur les risques liés à l'informatique

Autres risques liés à l'informatique

L'acquisition d'une compréhension des processus de l'entité liés à la cybersécurité dans les domaines ci-après permet à l'auditeur de comprendre et d'identifier les risques liés à la cybersécurité.

1	**Évaluation des risques –** Compréhension de la façon dont le processus d'évaluation des risques de l'entité examine la cybersécurité.
2	**Rôles et responsabilités –** Compréhension des rôles et des responsabilités en matière de cybersécurité établis par l'entité, comme le dirigeant principal de la sécurité de l'information (DPSI), le dirigeant principal de l'information (DPI) ou l'agent de gestion des risques liés à la cybersécurité.
3	**Protection des actifs –** Compréhension des processus utilisés par l'entité pour protéger les actifs numériques et/ou électroniques importants inscrits à son bilan et exposés à un risque lié à la cybersécurité (p. ex. propriété intellectuelle, brevets, objet protégé par le droit d'auteur, secrets commerciaux) ainsi que des processus utilisés par la direction pour recenser ces actifs et établir l'ordre de priorité de leur protection.
4	**Atteintes à la sécurité** – Compréhension des procédures et des contrôles mis en place par l'entité pour surveiller et détecter les atteintes à la sécurité ou les incidents de sécurité.
5	**Informations à fournir ou risques et incidents –** Compréhension des processus utilisés par l'entité pour divulguer les risques et les incidents liés à la cybersécurité (conformément aux exigences en matière de présentation de l'information).
6	**Expositions courantes aux risques liés à la cybersécurité –** Compréhension de la mesure dans laquelle les expositions courantes liées à la cybersécurité peuvent représenter un risque d'anomalies significatives au niveau des états financiers et de la réponse de l'entité à ce risque.

Procédure – Identification des risques liés à l'informatique et compréhension et évaluation des CGI connexes

Guide pratique sur les risques liés à l'informatique

Identification des risques liés à la cybersécurité

G

es à l'intérieur de la ligne pointillée, se
cheminement « Comment déterminer
tion et la mise en place des CGI liés
tion BVG Audit 5035.2

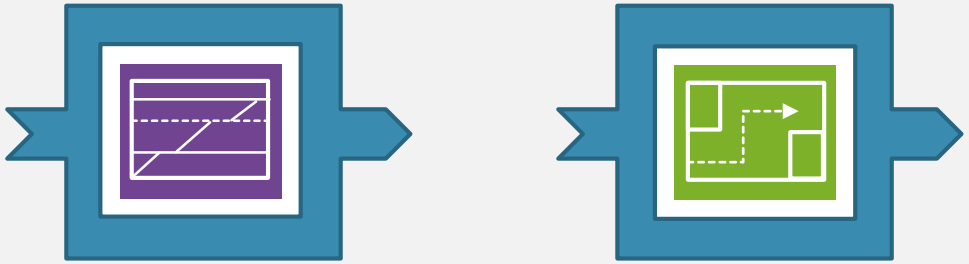
identifiés sont
ent et ont été

F

- Compréhension et identification des
liés à la cybersécurité pertinent pour

Autres risques liés à l'informatique

Autres risques liés à l'informatique, y compris les risques liés à la cybersécurité :



Risques liés à l'informatique au niveau de l'entité

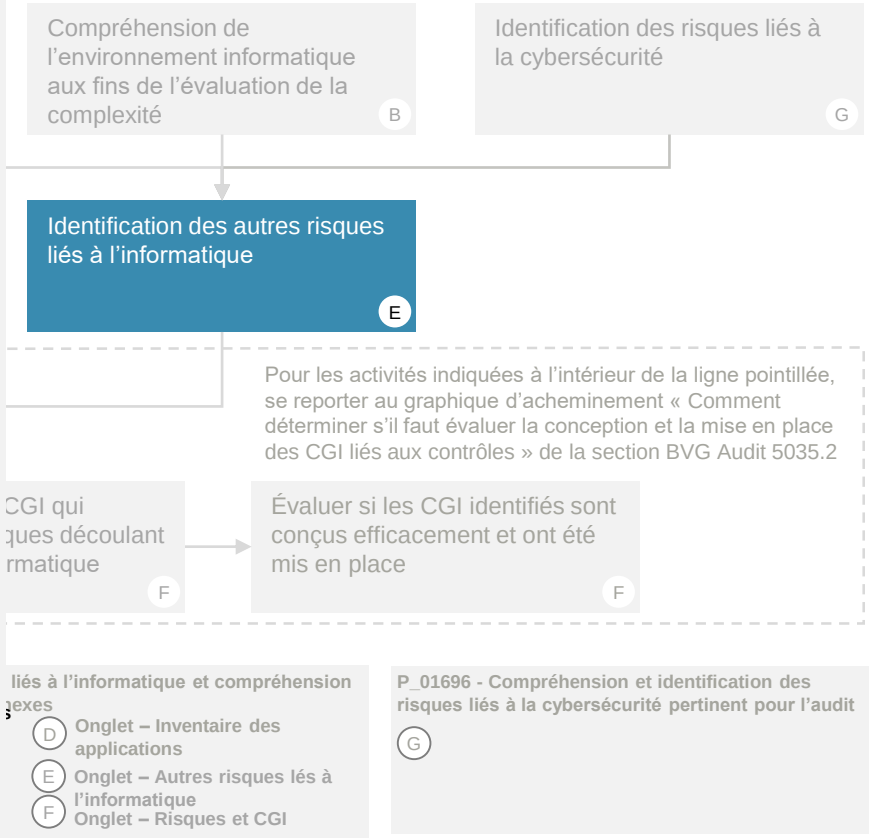
Les risques liés à l'informatique qui se produisent au niveau de l'entité et qui ne sont pas toujours propres à une application ou à d'autres aspects de l'environnement informatique, comme une séparation insuffisante des tâches ou des droits d'accès incompatibles.

Risques liés à l'informatique propres aux applications

Les risques liés à l'informatique propres aux applications qui ne sont pas directement associés à une dépendance aux TI spécifique comme le développement de programmes ou la migration des données. L'auditeur identifie ces risques en se fondant sur sa compréhension de l'entité et de son environnement informatique (p. ex. sa connaissance de la mise en œuvre d'un nouveau système peut amener l'auditeur à identifier un risque lié à la migration des données découlant du transfert des données de l'ancienne application à la nouvelle).

Procédure – Identification des risques liés à l'informatique et compréhension et évaluation des CGI connexes

Guide pratique sur les risques liés à l'informatique



CGI répondant aux risques découlant du recours à l'informatique

Lors de l'identification des CGI qui répondent aux risques liés à l'informatique, il faut tenir compte des quatre domaines suivants :

Accès aux programmes et aux données

L'objectif de ce domaine consiste à veiller à ce que l'accès autorisé aux applications informatiques et à d'autres aspects de l'environnement informatique soit accordé uniquement lorsque l'identité d'un utilisateur est authentifiée. Les contrôles d'accès englobent les processus utilisés par l'entité pour ajouter, supprimer et modifier des utilisateurs et leurs droits d'accès connexes, selon les objectifs de contrôle établis dans la conception du contrôle.

L'objectif de ce domaine consiste à veiller à ce que les modifications apportées aux applications informatiques et aux autres aspects de l'environnement informatique soient demandées, autorisées, exécutées, testées et mises en place de manière à atteindre les objectifs de la direction en matière de contrôles informatiques

Modifications apportées aux programmes

Développement de programmes

L'objectif de ce domaine consiste à veiller à ce que les applications informatiques et d'autres aspects de l'environnement informatique soient élaborés, configurés et mis en place de manière à atteindre les objectifs de la direction en matière de contrôle. Cela comprend des contrôles portant sur des projets de développement, d'acquisition ou de mise en œuvre de contrôles ou de contrôles relatifs à la conversion de données.

L'objectif de ce domaine consiste à veiller à ce que l'information des applications informatiques et d'autres aspects de l'environnement informatique soient traitée de façon exhaustive et exacte, conformément aux objectifs de la direction en matière de contrôle, et à ce que les problèmes de traitement soient détectés et réglés de façon exhaustive et exacte pour assurer l'intégrité des données financières.

Opérations informatiques

Procédure – Identification des risques liés à l'informatique et compréhension et évaluation des CGI connexes

Guide pratique sur les risques liés à l'informatique

CGI – Les contrôles afférents aux processus informatiques de l'entité qui contribuent à assurer le bon fonctionnement continu de l'environnement informatique, notamment le maintien du fonctionnement efficace des contrôles du traitement de l'information et l'intégrité (c'est-à-dire l'exhaustivité, l'exactitude et la validité) des informations se trouvant dans le système d'information de l'entité.

Identification des CGI qui répondent aux risques découlant du recours à l'informatique (F)

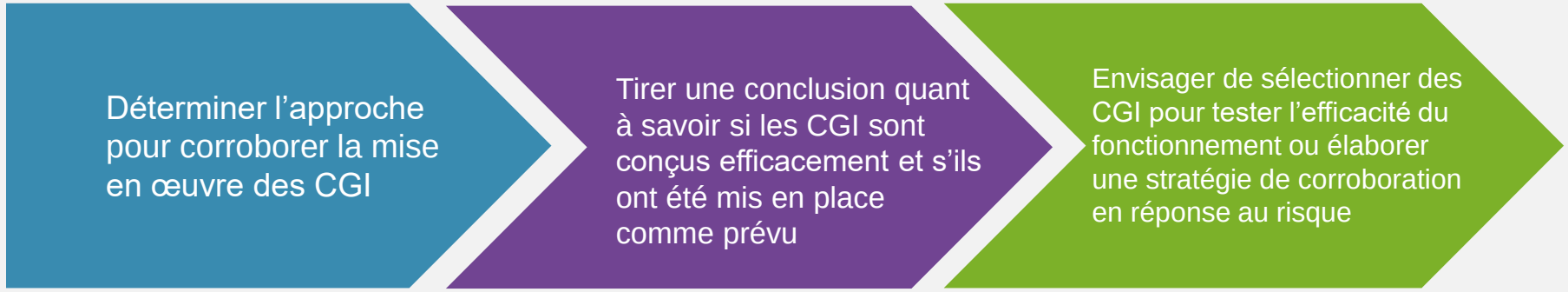
Évaluer si les CGI identifiés sont conçus efficacement et ont été mis en place (F)

*Identification des risques liés à l'informatique et compréhension et évaluation des CGI connexes
- (C) Onglet – Dépendances aux TI
- (D) Onglet – Complexité des applications
- (D) Onglet – Inventaire des applications
- (E) Onglet – Autres risques liés à l'informatique
- (F) Onglet – Risques et CGI

P_01696 - Compréhension et identification des risques liés à la cybersécurité pertinent pour l'audit (G)

Autres risques liés à l'informatique

Évaluer si les CGI sont conçus efficacement et s'ils ont été mis en place :



Procédure – Identification des risques liés à l'informatique et compréhension et évaluation des CGI connexes

Guide pratique sur les risques liés à l'informatique

Identification des risques liés à l'informatique découlant directement de l'appui de l'entité sur les dépendances aux TI (C)

Identification des CGI qui répondent aux risques découlant du recours à l'informatique (F)

Évaluer si les CGI identifiés sont conçus efficacement et ont été mis en place (F)

P_01710 - Compréhension et évaluation de l'environnement informatique de l'entité

- (A) Onglet – Contrôle interne à l'égard des TI
- (B) Onglet – Complexité de l'environnement informatique

P_01715 - Identification des risques liés à l'informatique et compréhension et évaluation des CGI connexes

- (C) Onglet – Dépendances aux TI
- (D) Onglet – Complexité des applications
- (D) Onglet – Inventaire des applications
- (E) Onglet – Autres risques liés à l'informatique
- (F) Onglet – Risques et CGI

P_01696 - Compréhension et identification des risques liés à la cybersécurité pertinent pour l'audit

- (G)

Procédure – Compréhension et évaluation de la complexité de l'environnement informatique de l'entité

La procédure permet de documenter les secteurs suivants :

- Compréhension des composantes clés du système de contrôle interne de l'entité à l'égard de l'informatique.
- Compréhension des caractéristiques de l'environnement informatique de l'entité.
- Évaluation de la complexité de l'environnement informatique selon la compréhension acquise.

Compréhension des principales composantes du système de contrôle à l'égard des TI de l'entité	
Compréhension	**Renseignements supplémentaires, y compris l'identification des changements dans la période**
***Note** - Cette section porte sur la compréhension acquise par l'auditeur des composantes du système de contrôle interne à l'égard des TI de l'entité.*	
Niveau des ressources de TI qualifiées/expérimentées (les éléments qui s'appliquent ont été cochés) ☐ Manque de ressources ☐ Ressources adéquates ☐ Ressources suffisantes	
Structure organisationnelle de la fonction des TI (les éléments qui s'appliquent ont été cochés) ☐ Organigramme de la structure des TI obtenu dans le lien fourni ☐ Fonction décentralisée ☐ Fonction centralisée ☐ Fonction mixte	
Politiques liées aux TI (les éléments qui s'appliquent ont été cochés) ☐ Politiques informelles et généralement non documentées ☐ Politiques documentées pour des secteurs précis uniquement ☐ Politiques liées aux TI exhaustives et documentées	
Rôles et responsabilités à l'égard des TI (les éléments qui s'appliquent ont été ☐ Informels ☐ Officiels et clairement définis	
Niveau de séparation des tâches liées aux activités de TI (les éléments qui s'appliquent ont été cochés) ☐ Exhaustif (p. ex. les rôles des équipes des TI et des Finances sont clairement définis et conçus de manière à éviter des accès inappropriés) ☐ Modéré ou varié à l'échelle des différents processus ☐ Restreint ou inexistant (p. ex. les rôles des équipes des TI et des Finances ne sont pas clairement définis ou conçus de manière à éviter des accès inappropriés)	

Tableau sommaire et conclusion globale sur la complexité de l'environnement informatique	
Caractéristiques de l'environnement informatique de l'entité	**Évaluation globale - reflétant les évaluations ci-dessus**
Automatisation	
Utilisation par l'entité de rapports générés par le système	
Personnalisation	
Modèle opérationnel	
Changement	
Utilisation de nouvelles technologies	
Autres facteurs pertinents	
Évaluation de la complexité de l'environnement informatique global de l'entité	*[Veuillez choisir]*
Justification de l'évaluation de la complexité globale, si elle ne ressort pas de l'évaluation des caractéristiques individuelles	

Procédure – Identification des risques liés à l'informatique et compréhension et évaluation des CGI connexes

Aller à la page 2 de 2

La procédure permet de documenter les secteurs suivants :

- Un sommaire des dépendances aux TI identifiées pendant l'audit, ainsi que leur type, leur nature et leur pertinence pour le plan d'audit.
- Identification des risques liés à l'informatique les plus courants et pertinents selon le type de dépendance aux TI en utilisant l'automatisation intégrée à la procédure.
- Applications et autres aspects de l'environnement informatique sur lesquels reposent les dépendances aux TI.
- Évaluation de la complexité des applications identifiées.

Sommaire des dépendances aux TI

Sélectionner le bouton « **Traiter les données saisies** » chaque fois que des modifications sont apportées à la documentation entrée dans les colonnes B à J.
Sélectionner le bouton « **Transférer les données à l'onglet Risques et CGI** » lorsqu'il s'affiche.

No de référence	Nom de la dépendance aux TI — Traiter les données saisies	Type (contrôle automatisé, rapport, calcul, séparation des tâches ou accès restreint, interfaces)	Nature de la dépendance aux TI (application standard ou personnalisée)	Description (y compris les détails du test (contrôles et/ou test de corroboration) lié à la dépendance aux TI)	Processus opérationnels connexes	Applications associées (Remarque – Vérifier que chaque application est incluse dans l'onglet « Complexité des applications »)	Pertinence de la dépendance aux TI par rapport au plan d'audit (1. Contrôle dans la composante des activités de contrôle uniquement. 2. Fondement des tests de corroboration uniquement. 3. Fondement des tests de corroboration et du contrôle dans la composante des activités de contrôle 4. Aucune de ces réponses (aucune autre évaluation nécessaire)	Si la dépendance aux TI est un rapport généré par le système, a-t-on l'intention de tester les intrants et les extrants du rapport généré par le système au moyen de tests de corroboration? (O/N)
		[Veuillez choisir]	[Veuillez choisir]				[Veuillez choisir]	
		[Veuillez choisir]	[Veuillez choisir]				[Veuillez choisir]	
		[Veuillez choisir]	[Veuillez choisir]				[Veuillez choisir]	
		[Veuillez choisir]	[Veuillez choisir]				[Veuillez choisir]	
		[Veuillez choisir]	[Veuillez choisir]				[Veuillez choisir]	
		[Veuillez choisir]	[Veuillez choisir]				[Veuillez choisir]	

Complexité des applications

Une fois que les dépendances aux TI ont été identifiées dans l'onglet « Dépendances aux TI », les applications connexes et d'autres aspects de l'en
L'auditeur documente les applications dans cet onglet et dans l'onglet « Inventaire des applications », peu importe s'il prévoit tester les CGI ou ef
l'informatique.

Applications, y compris les outils informatiques des utilisateurs finaux, comme les entrepôts de données et les rédacteurs de rapports	Les caractéristiques documentées des applications et d'autres aspects de l'environnment informatique dans l'onglet « Inventaire des applications »	Le niveau de complexité évalué de cette application est-il conforme à la complexité globale de l'environnement informatique (documentée dans la procédure « Compréhension et évaluation de la complexité de l'environnement informatique de l'entité » du répertoire « Cadre de contrôle interne »)?	Évaluation de la complexité de l'application informatique (complexe, modérément complexe ou non complexe) Remarque – Lorsque le niveau de complexité diffère de la complexité globale de l'environnement informatique, cela peut influer sur l'approche d'audit – voir la colonne G	Dét suppl conc
		[Veuillez choisir]		
		[Veuillez choisir]		
		[Veuillez choisir]		
		[Veuillez choisir]		
		[Veuillez choisir]		

Procédure – Identification des risques liés à l'informatique et compréhension et évaluation des CGI connexes

La procédure permet de documenter les secteurs suivants :

- Identification des risques liés à l'informatique qui ne découlent pas directement des dépendances aux TI sous-jacentes, y compris les risques liés à la cybersécurité.
- Évaluation de la pertinence des risques liés à l'informatique et identification des CGI répondant à ces risques.
- Évaluation de la conception et de la mise en œuvre des CGI.
- Détermination de la réponse prévue aux risques liés à l'informatique identifiés (test de l'efficacité du fonctionnement des contrôles ou procédures de corroboration).

Retour à la page 1 de 2

Identification des risques liés à l'informatique qui ne découlent pas directement des dépendances aux TI sous-jacentes

Les risques découlant du recours à l'informatique se divisent en deux aspects :
- L'appui par l'entité sur des activités de contrôle nécessitant des dépendances aux TI (voir l'onglet « Dépendances aux TI »)
- Les autres risques liés à l'informatique qui ne découlent pas directement des dépendances aux TI sous-jacentes (à documenter ci-dessous), ce qui comprend :
  - Les risques liés à l'informatique qui surviennent à un niveau différent (p. ex., au niveau de l'entité) et qui peuvent ne pas être propres à une application ou à d'autres aspects de l'environnement informatique.
  - Risques informatiques propres aux applications qui ne sont pas liés aux dépendances aux TI. Ces risques sont identifiés en fonction de la compréhension acquise par l'auditeur de l'entité et de son environnement informatique.

Cet onglet comprend un certain nombre d'autres risques liés à l'informatique courants. D'autres risques liés à l'informatique qui sont pertinents pour l'audit seront indiqués dans l'onglet « Risques et CGI » en vue d'une évaluation approfo
l'identification des contrôles connexes
Lorsque d'autres risques liés à l'informatique sont identifiés, l'auditeur évalue également s'ils représentent des risques au niveau des états financiers.

Domaine des CGI	Risques découlant du recours à l'informatique	Directives	Risque lié à l'informatique pertinent? (Oui/Non)	Applications et d'autres aspects de l'environnement informatique touchés par ce risque
Considérations relatives à l'ensemble des CGI	Les tâches ne sont pas adéquatement séparées (CGI)	*Ce risque est généralement pertinent si des déficiences dans le(s) contrôle(s) indirect(s) de l'entité portant sur la séparation des tâches peuvent donner lieu à un risque lié à l'informatique. Par exemple, dans le cas où des membres de la fonction des finances de l'entité peuvent modifier l'accès ou le code source d'une application.*	*[Veuillez choisir]*	
	Aucune gouvernance des processus informatiques n'a été établie	*Ce risque est généralement pertinent si un manque de gouvernance dans l'environnement informatique de l'entité peut donner lieu à un risque lié à l'informatique. Par exemple, la fonction des TI n'a pas de structure de gouvernance claire ou n'est pas intégrée au modèle opérationnel global.*	*[Veuillez choisir]*	

Identification des risques liés à l'informatique pertinents et évaluation de la conception et de la mise en place des contrôles généraux informatiques (CGI) en réponse à ces ri

Les risques découlant du recours à l'informatique indiqués ci-dessous sont les risques identifiés dans les onglets « Dépendances aux TI » et « Autres risques liés à l'informatique ». Dans ce tableau, l'auditeur identifie les CGI qui répondent aux risques pertinents et évalue l'efficacité de la conception et la
Cet onglet se remplit automatiquement en fonction de l'information contenue dans les onglets « Dépendances aux TI » et « Autres risques informatique ». Sélectionner le bouton « Transférer les données à l'onglet Risques et CGI » dans la cellule C2 de l'onglet « Dépendances aux TI » pour envoyer les dc

DOCUMENTATION DES RISQUES ET DES CONTRÔLES IDENTIFIÉS

Domaine des CGI	Risque découlant du recours à l'informatique (identifié dans les onglets « Dépendances aux TI » et « Autres risques informatique »)	Applications et d'autres aspects de l'environnement informatique touchés par ce risque	Le risque est-il pertinent (Oui/Non)	Justification si le risque n'est pas pertinent ou s'il est en partie non pertinent (p. ex., pertinent seulement pour des applications particulières)	Ajouter / Supprimer des CGI	CGI répondant à ce risque (sélectionner un contrôle de la bibliothèque à partir du menu déroulant et le personnaliser au besoin)	Applica aspects de informatiq se (mettre à est lié à u pa
Accès aux programmes et aux données	Des comptes à risque élevé/donnant des pouvoirs (p. ex. super utilisateurs) permettent de contourner les contrôles de la séparation des tâches et de l'autorisation appliqués par les systèmes	*Application*	*[Veuillez choisir]*		✚		*Application*
	Des changements directs inappropriés sont faits aux enregistrements d'opérations et/ou aux données de base connexes	*Application*	*[Veuillez choisir]*		✚		*Application*
	Des modifications non autorisées ou non testées, ou l'omission d'apporter les modifications nécessaires à la configuration des applications et / ou aux programmes d'applications empêchent les systèmes de traiter les	*Application*	*[Veuillez choisir]*		✚		*Application*

Droit d’auteur d’appliquant au BVG

Licence conventionnelle de CPA Canada