Processus d’évaluation des risques

Identification des risques liés à l’informatique pertinents pour l’audit
Guide pratique

déc.–2022
Propriétaire du modèle : Audit TI

Bureau du vérificateur général du Canada
Office of the Auditor General of Canada

Identification des risques liés à l'informatique pertinents pour l'audit

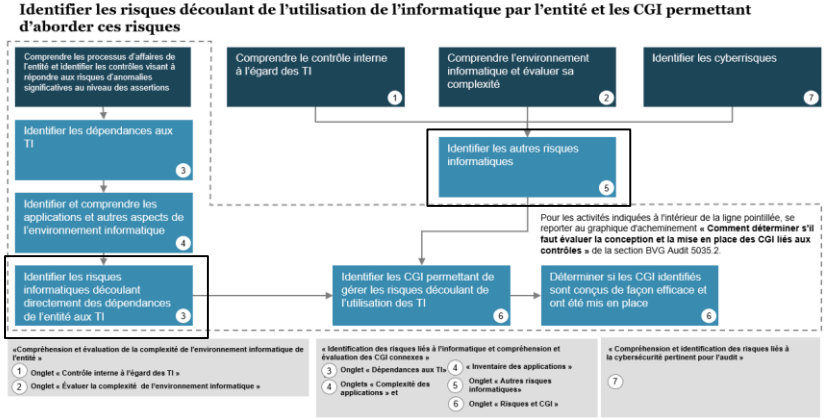
Table des matières

Identification des risques liés à l'informatique pertinents pour l'audit — Introduction (1 de 2)

Le présent guide pratique vise à aider les équipes de mission à appliquer le processus d'évaluation des risques du BVG en vue de déterminer si les risques liés à l'informatique les plus courants sont pertinents pour l'audit. Les risques liés à l'informatique pertinents couramment mis en place sont affichés automatiquement dans la procédure « Identification des risques liés à l'informatique et compréhension et évaluation des CGI connexes » selon le type de dépendance aux TI recensé par l'équipe de mission lors de sa mise en œuvre des procédures d'évaluation des risques ainsi que la pertinence déterminée par l'équipe de chacune de ces dépendances aux TI pour le plan d'audit. Le guide pratique fournit des descriptions en langage clair de chacun des risques liés à l'informatique pertinents les plus courants et décrit les situations dans lesquelles le risque peut **ne pas** être pertinent pour l'audit, et ce, même lorsqu'il s'agit d'un risque pertinent mis en place couramment pour la dépendance aux TI qui a été identifiée par l'équipe de mission. L'équipe de mission peut se servir du guide pratique comme référence pour déterminer et documenter la pertinence des risques liés à l'informatique.

Rappel : au moment d'appliquer la section BVG Audit 5035.2, l'équipe a identifié les types de risques liés à l'informatique suivants lorsqu'elle acquiert une compréhension de l'environnement informatique et élabore son plan d'audit (comme le souligne l'encadré noir entourant les deux boîtes du diagramme ci-contre) :

- Risques liés à l'informatique découlant directement de l'appui de l'entité sur les dépendances aux TI ou qui sont à la base des procédures de corroboration.
- Autres risques liés à l'informatique qui ont lieu au niveau de l'entité, qui ne sont pas associés aux dépendances aux TI sous-jacentes et qui ne sont pas propres à l'application.



Le guide pratique a pour but d'aider les équipes de mission à déterminer la pertinence des deux types de risques pour leur mission. Pour connaître les détails de chaque étape présentée dans le diagramme, veuillez vous reporter au Guide de référence sur le processus d'évaluation des risques liés à l'informatique du Bureau.

Identification des risques liés à l'informatique pertinents pour l'audit — Introduction (2 de 2)

Un sommaire des rappels importants lors de l'identification des risques liés à l'informatique se trouve à la page 5. Aux pages 7 et 8 se trouve un sommaire des risques liés à l'informatique pertinents mis en place couramment qui est intégré à la procédure « Identification des risques liés à l'informatique et compréhension et évaluation des CGI connexes ». Le présent guide pratique explique également la pertinence générale de chacun des 18 risques liés à l'informatique pour chaque type de dépendance aux TI et/ou, le cas échéant, chacun des autres risques liés à l'informatique (des hyperliens vers chacun de ces risques sont compris dans le sommaire à la page 7 et 8).

Le présent document ne dresse pas la liste exhaustive des caractéristiques que l'équipe doit comprendre pour mettre en œuvre les procédures d'évaluation des risques. Les risques présentés dans ce document portent sur tous les risques et les CGI se trouvant dans la procédure « Identification des risques liés à l'informatique et compréhension et évaluation des CGI connexes ». Il est possible que les risques liés à l'informatique et les CGI identifiés pendant l'audit doivent être adaptés aux faits et aux circonstances propres à l'environnement informatique de l'entité auditée.

Le guide pratique ne remplace pas la nécessité de passer en revue les exigences détaillées et les directives dans le Manuel d'audit annuel du BVG. Pour obtenir des directives détaillées, reportez-vous à la section BVG Audit 5035.2 ou communiquez avec l'Audit des TI si vous avez des questions.

Identification des risques liés à l'informatique pertinents pour l'audit — Rappels importants

- 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, y compris l'identification des **contrôles de la composante « activités de contrôle »** du système de contrôle interne de l'entité.
- Lorsque l'équipe détermine des dépendances aux TI, elle identifie aussi les applications informatiques ou d'autres aspects de l'environnement informatique qui y sont liés et évalue leur vulnérabilité aux risques découlant du recours à l'informatique.
- Pour acquérir une compréhension de la composante « activités de contrôle », l'équipe doit aussi évaluer s'il y a des risques liés à l'informatique à l'échelle de l'entité (c.-à-d. des risques liés à l'informatique qui ne sont pas associés aux dépendances aux TI sous-jacentes et qui ne sont pas propres à l'application, comme les risques liés à l'ensemble des CGI, les risques liés à la cybersécurité ou les risques liés à la mise en œuvre de nouveaux systèmes).
- Il faut identifier les risques liés à l'informatique, les CGI connexes découlant des dépendances aux TI et, le cas échéant, d'autres risques liés à l'informatique peu importe si l'équipe prévoit tester les contrôles de l'entité ou si elle prévoit 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.
- Lorsque les seules dépendances aux TI identifiées sont les rapports générés par les systèmes pour lesquels l'équipe prévoit effectuer des tests de corroboration concernant la fiabilité (c.-à-d. l'exhaustivité et l'exactitude) de l'information qu'ils contiennent, l'équipe n'est pas tenue d'évaluer la conception et la mise en place des CGI pertinents pour les rapports générés par les systèmes.
- Comme il peut s'agir d'un domaine complexe, l'équipe peut envisager de recourir aux spécialistes de l'Audit des TI pour l'aider à déterminer les applications informatiques et d'autres aspects de l'environnement informatique qui peuvent être vulnérables aux risques découlant du recours à l'informatique.
- 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 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 documenté par la détermination par 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.

Identification des risques liés à l'informatique pertinents pour l'audit — Utilisation du guide pratique

Le présent guide pratique fournit une explication de la pertinence générale de chacun des 18 risques liés à l'informatique pour chaque type de dépendance aux TI et/ou, le cas échéant, d'autres risques liés à l'informatique. La légende suivante indique l'applicabilité prévue de chaque risque aux différents types de dépendances aux TI ou à d'autres risques liés à l'informatique :

De quoi découle-t-il? Type de dépendance aux TI et/ou autres risques liés à l'informatique	**Contrôles automatisés**	**Rapports générés par les systèmes**	**Calculs**	**Accès restreint / séparation des tâches**	**Interfaces**	**Autres risques liés à l'informatique**

Le code de couleurs pour chaque dépendance aux TI détermine la pertinence générale du risque lié à l'informatique :

	Le risque est généralement pertinent pour l'audit.
	Il est possible que le risque soit ou ne soit pas pertinent selon les circonstances propres à l'entité.
	Le risque n'est pas généralement pertinent pour ce type de dépendances aux TI ou ces autres risques liés à l'informatique.

Le guide pratique identifie également les CGI qui répondent aux risques liés à l'informatique. Pour les audits n'ayant jamais nécessité l'intervention des TI, les CGI recommandés seront suivis de la mention **(recommandé)** suivant le control. Noté qu'à la page 14, la mention **(*recommandé)** pour le premier CGI indique que ce CGI peut être recommandé en fonction des paramètres d'authentification. Pour plus d'informations sur l'identification des CGI appropriés, veuillez contacter l'Audit des TI.

Identification des risques liés à l'informatique pertinents pour l'audit

Sommaire des risques liés à l'informatique pertinents les plus courants

(Cliquez sur Risque pour consulter les détails supplémentaires)

Domaine des CGI	Risque	Contrôles automatisés	Rapports générés par les systèmes	Calculs	Accès restreint / séparation des tâches	Interfaces	Autres risques liés à l'informatique
Facteurs relatifs à l'ensemble des CGI	Les tâches ne sont pas adéquatement séparées						✓
	Aucune gouvernance des processus informatiques n'a été établie						✓
Accès aux programmes et aux données	Les utilisateurs finaux des applications contournent les contrôles de la séparation des tâches et de l'autorisation appliqués par les systèmes				✓		
	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	✓	✓	✓	✓	✓	
	Des changements directs inappropriés sont faits aux enregistrements d'opérations et/ou aux données de base connexes	✓	✓	✓	✓	✓	
	À cause de la faiblesse des contrôles d'authentification ou de la déficience des configurations de sécurité, les droits d'accès peuvent être contournés	✓	✓	✓	✓	✓	
	Rien n'empêche un accès physique non autorisé aux installations, à l'équipement et aux ressources						✓
Modifications aux programmes	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'application empêchent les systèmes de traiter les enregistrements de transactions de manière complète et exacte	✓	✓	✓		✓	
	Des modifications non autorisées ou non testées, ou l'omission d'apporter les modifications nécessaires aux bases de données, au système d'exploitation ou au réseau empêchent les systèmes de traiter les enregistrements de transactions de manière complète et exacte						✓
	Des modifications non autorisées ou non testées, ou l'omission d'apporter les modifications nécessaires aux processus par lots empêchent les systèmes de traiter les enregistrements de transactions de manière complète et exacte					✓	

Identification des risques liés à l'informatique pertinents pour l'audit

Sommaire des risques liés à l'informatique pertinents courants

Domaine des CGI	Risque	Contrôles automatisés	Rapports générés par les systèmes	Calculs	Accès restreint / séparation des tâches	Interfaces	Autres risques liés à l'informatique
Développement de programmes	Les systèmes nouvellement implantés (ou améliorés en profondeur) traitent les données de manière incomplète ou inexacte (p. ex. en raison d'erreurs de codage ou de configuration)						✓
	Les transactions enregistrées et/ou les données de base n'ont pas été transférées en totalité et avec exactitude						✓
Opérations informatiques	Présence de changements inappropriés, intervention manuelle ou manquements en rapport avec la planification des travaux de traitement par lots					✓	
	Le transfert des transactions enregistrées entre des systèmes est incomplet ou inexact					✓	
	Des transactions enregistrées sont perdues (p. ex. en raison d'une défaillance du système) et des données sont irrécupérables ou corrompues/inscrites en double lors du processus de récupération						✓
Cybersécurité **(Les risques et les contrôles liés à la cybersécurité peuvent concerner l'accès aux programmes et aux données, les opérations informatiques et/ou d'autres domaines des CGI)**	Les cyberattaques et les attaques par rançongiciel exploitent les vulnérabilités, entraînant ainsi la manipulation et/ou la destruction de données, ce qui compromet les états financiers ou la disponibilité du système et, par le fait même, la présentation de l'information financière en temps opportun						✓
	Les systèmes non corrigés mènent à l'exploitation de vulnérabilités, entraînant ainsi la manipulation ou la destruction de données, ce qui compromet les états financiers ou la disponibilité du système et, par le fait même, la présentation de l'information financière en temps opportun						✓
	Les attaques par rançongiciel rendent les systèmes inaccessibles, ce qui a une incidence sur la disponibilité des systèmes et sur la capacité de l'entité à préparer l'information financière en temps opportun						✓

Remarque : La configuration ou la modification des données sur les fournisseurs et les virements électroniques sont deux expositions courantes pouvant entraîner un risque lié à la cybersécurité; toutefois, comme ces risques ne découlent pas du recours à l'informatique, ils ne font pas partie du présent guide pratique.

Facteurs relatifs à l'ensemble des CGI

Risque	**Les tâches ne sont pas adéquatement séparées**					
Quel est le risque?	**Un manque de séparation des tâches liées au fonctionnement des CGI signifie que les utilisateurs ont la capacité de contourner les contrôles relatifs aux accès et à la modification des applications, des données et d'autres aspects de l'infrastructure informatique.** Ce risque lié à l'informatique pour l'ensemble des CGI concerne la possibilité qu'un manque de séparation des tâches liées aux processus et aux contrôles informatiques puisse entraîner un risque lié à l'informatique. Par exemple, lorsqu'il n'y a aucune séparation physique des tâches et/ou les membres d'autres services (comme le service des finances) peuvent effectuer des activités liées à l'informatique.					
De quoi découle-t-il? Type de dépendances aux TI et/ou autres risques liés à l'informatique	**Contrôles automatisés**	**Rapports générés par les systèmes**	**Calculs**	**Accès restreint / séparation des tâches**	**Interfaces**	**Autres risques liés à l'informatique**
Quand ce risque lié à l'informatique peut-il ne pas être pertinent pour l'audit?	Ce risque est vraisemblablement toujours pertinent pour l'audit, car la compréhension acquise par l'auditeur de la façon dont l'entité gère ce risque contribue à la réponse de l'auditeur au risque de fraude lié au contournement des contrôles par la direction (du point de vue des TI, ce risque comprend la séparation des tâches et l'autorisation appliquées par les systèmes).					
Exemples de dépendances aux TI liées à ce risque	• S. O. Ce risque n'est pas lié aux dépendances aux TI.					
CGI qui répondent au risque lié à l'informatique (adapter, au besoin, aux contrôles propres à l'entité)	• Maintien à jour des politiques aux fins de la séparation des tâches au sein des TI **(recommandé).**					

Facteurs relatifs à l'ensemble des CGI

Risque	**Aucune gouvernance des processus informatiques n'a été établie**					
Quel est le risque?	**Un manque de gouvernance de l'environnement informatique peut entraîner un système de contrôle interne inefficace à l'égard de l'informatique.** Comme toute autre fonction au sein de l'entité, une structure de gouvernance claire (politiques, procédures, formation, etc.) est importante pour soutenir l'efficacité du système de contrôle interne. Il est essentiel de mettre en place des contrôles à l'égard de ce risque afin de veiller à l'efficacité de la conception, de la mise en place et du fonctionnement des CGI.					
De quoi découle-t-il? Type de dépendances aux TI et/ou autres risques liés à l'informatique	**Contrôles automatisés**	**Rapports générés par les systèmes**	**Calculs**	**Accès restreint / séparation des tâches**	**Interfaces**	**Autres risques liés à l'informatique**
Quand ce risque lié à l'informatique peut-il ne pas être pertinent pour l'audit?	Ce risque est lié à la compréhension de l'environnement informatique. Ce risque n'est pas pertinent pour l'audit si l'équipe conclut qu'il y a une structure de gouvernance appropriée au sein de l'environnement informatique de l'entité.					
Exemples de dépendances aux TI liées à ce risque	• S. O. Ce risque n'est pas lié aux dépendances aux TI.					
CGI qui répondent au risque lié à l'informatique (adapter, au besoin, aux contrôles propres à l'entité)	• Établissement et mise en place de structures de gouvernance visant les processus informatiques **(recommandé).**					

Accès aux programmes et aux données

Risque	**Les utilisateurs finaux des applications contournent les contrôles de la séparation des tâches et de l'autorisation appliqués par les systèmes**
Quel est le risque?	**Les utilisateurs ont reçu des droits d'accès qui sont supérieurs à ceux qui sont nécessaires à leur rôle et/ou à leurs responsabilités ou qui sont incompatibles avec ces derniers (sur le plan de la séparation des tâches).** Les contrôles au niveau des applications qui automatisent les tâches d'autorisation ou qui appliquent la séparation des tâches dépendent de l'efficacité des contrôles d'accès aux applications. Ce risque existe lorsque la direction se fie au système pour séparer les tâches ou restreindre l'accès. Lorsqu'on accorde aux utilisateurs un accès à des données ou à des fonctionnalités qui sont supérieures à celles nécessaires à leur rôle ou à leurs responsabilités (p. ex. un membre subalterne de la fonction des finances ayant accès aux données sur les primes) ou une combinaison de droits d'accès qui nuisent à l'efficacité de la séparation des tâches (c.-à-d. une combinaison de droits d'accès qui permet à l'utilisateur de contourner les contrôles liés à l'autorisation ou à la séparation des tâches, par exemple les accès nécessaires pour enregistrer et approuver des écritures de journal). Ce risque est généralement lié au risque « À cause de la faiblesse des contrôles d'authentification ou de la déficience des configurations de sécurité, les droits d'accès peuvent être contournés » à la page 14.
De quoi découle-t-il? Type de dépendances aux TI et/ou autres risques liés à l'informatique	**Contrôles automatisés** / **Rapports générés par les systèmes** / **Calculs** / **Accès restreint / séparation des tâches** / **Interfaces** / **Autres risques liés à l'informatique**
Quand ce risque lié à l'informatique peut-il ne pas être pertinent pour l'audit?	Ce risque est toujours pertinent pour l'audit lorsqu'il y a une dépendance aux TI liée à l'accès restreint ou à la séparation des tâches.
Exemples de dépendances aux TI liées à ce risque	• Les écritures de journal sont approuvées par un processus automatisé d'approbation des flux de travail (séparation des tâches). • L'accès aux données sur la paie est limité au dirigeant principal des finances (accès restreint).
CGI qui répondent au risque lié à l'informatique (adapter, au besoin, aux contrôles propres à l'entité)	• Les demandes d'accès à l'application sont examinées avec soin et autorisées par la direction **(recommandé).** • Le caractère approprié des droits d'accès aux applications fait l'objet d'un suivi périodique. • Les droits d'accès aux applications des utilisateurs ayant quitté leur emploi sont révoqués en temps opportun **(recommandé).**

Accès aux programmes et aux données

Risque	**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**
Quel est le risque?	**Les utilisateurs ont reçu un accès d'administrateur ou d'autres droits d'accès privilégié qui leur permet de contourner les contrôles liés à la séparation des tâches ou à l'accès restreint et les contrôles liés au changement.** Ce risque existe lorsque les utilisateurs peuvent créer, modifier ou supprimer des utilisateurs et/ou apporter des modifications à la fonctionnalité du système, en contournant les processus d'examen ou d'autorisation. Les utilisateurs membres de la fonction de TI ont souvent un niveau d'accès supérieur. Dans certains cas, des utilisateurs à l'extérieur de la fonction de TI peuvent aussi avoir un niveau d'accès supérieur. Il y a de bonnes raisons pour accorder ce niveau d'accès, car il est possible que ces utilisateurs aient besoin de ce niveau d'accès pour configurer les dépendances aux TI (p. ex. créer et gérer les seuils d'approbation automatisée des paiements) ou gérer l'accès (p. ex. créer des comptes d'utilisateur pour les nouvelles recrues et limiter leur accès aux applications, aux transactions et aux données nécessaires à leur rôle et à leurs responsabilités). Ce risque est généralement lié au risque « À cause de la faiblesse des contrôles d'authentification ou de la déficience des configurations de sécurité, les droits d'accès peuvent être contournés » à la page 14.
De quoi découle-t-il? Type de dépendances aux TI et/ou autres risques liés à l'informatique	**Contrôles automatisés** / **Rapports générés par les systèmes** / **Calculs** / **Accès restreint / séparation des tâches** / **Interfaces** / **Autres risques liés à l'informatique**
Quand ce risque lié à l'informatique peut-il ne pas être pertinent pour l'audit?	**Pour l'accès restreint et la séparation des tâches :** • Ce risque est toujours pertinent pour l'audit lorsqu'il y a une dépendance aux TI liée à l'accès restreint/la séparation des tâches. **Pour les contrôles automatisés, les rapports générés par les systèmes, les calculs et les interfaces :** • **Fonctionnalité codée :** Ce risque n'est pas pertinent pour l'audit si la fonctionnalité du système ne peut pas être modifiée (c.-à-d. les dépendances aux TI visées ne peuvent pas être modifiées par l'utilisateur sans accéder au code du logiciel et l'entité n'a pas accès au code [p. ex. une application sous licence d'un tiers fournisseur sans accès au code et sans possibilité de personnalisation]). • **Fonctionnalité configurée :** Ce risque n'est pas pertinent pour l'audit si l'entité **a mis en place une séparation des tâches adéquate au sein du service de TI** (c.-à-d. la restriction de l'accès pour empêcher des changements non autorisés et les CGI connexes sont généralement pris en compte par les risques liés à l'informatique dans le domaine des CGI Modifications aux programmes et aucun des utilisateurs de la fonction de TI ne pourrait élaborer des modifications et les publier unilatéralement dans l'environnement réel sans que ces modifications soient examinées et approuvées au préalable).
Exemples de dépendances aux TI liées à ce risque	• L'accès nécessaire pour apporter des modifications aux règles de consolidation dans l'application de consolidation est restreinte aux utilisateurs de la fonction de TI. • La totalité des contrôles automatisés, des rapports générés par les systèmes, des calculs et des interfaces qui sont configurés ou personnalisés.
CGI qui répondent au risque lié à l'informatique (adapter, au besoin, aux contrôles propres à l'entité)	• Les demandes d'accès à la base de données/au fichier de données sont examinées avec soin et autorisées par la direction. • Les droits d'accès à la base de données/au fichier de données des utilisateurs ayant quitté leur emploi sont révoqués en temps opportun. • Les opérations ou les activités liées à la base de données/au fichier de données des super utilisateurs ou des administrateurs et les identificateurs génériques de nature délicate sont soumis à un suivi. • Le caractère approprié des droits d'accès à la base de données/au fichier de données fait l'objet d'un suivi périodique. • Les opérations ou les activités liées au système d'exploitation/au réseau des super utilisateurs ou des administrateurs et les identificateurs génériques de nature délicate sont soumis à un suivi. • Le caractère approprié des droits d'accès au système d'exploitation/au réseau fait l'objet d'un suivi périodique pour vérifier leur pertinence. • Les demandes d'accès au système d'exploitation/au réseau sont examinées avec soin et autorisées par la direction. • Les droits d'accès au système d'exploitation/au réseau des utilisateurs ayant quitté leur emploi sont révoqués en temps opportun. • Les opérations ou les activités liées aux applications des super utilisateurs ou des administrateurs et les identificateurs génériques de nature délicate sont soumis à un suivi. • Les droits d'accès privilégié (p ex. administrateurs de systèmes) sont autorisés et restreints adéquatement **(recommandé).**

Accès aux programmes et aux données

Risque	**Des changements directs inappropriés sont faits aux enregistrements d'opérations et/ou aux données de base connexes**
Quel est le risque?	**La modification ou la suppression de données permanentes est effectuée sans qu'elle ne soit examinée ou autorisée adéquatement.** Les données transactionnelles ou les données permanentes (p. ex. les données de base sur les fournisseurs) sont généralement conservées dans une base de données. Habituellement, les utilisateurs de la fonction de TI, appelés « administrateurs de bases de données », détiendront un accès de modification leur permettant d'apporter des changements ou de corriger les données. Lorsque cet accès n'est pas limité aux activités autorisées, il y a un risque que les données financièrement pertinentes soient modifiées ou supprimées sans les approbations appropriées. Ce risque est généralement lié au risque « À cause de la faiblesse des contrôles d'authentification ou de la déficience des configurations de sécurité, les droits d'accès peuvent être contournés » à la page 14.
De quoi découle-t-il? Type de dépendances aux TI et/ou autres risques liés à l'informatique	**Contrôles automatisés** / **Rapports générés par les systèmes** / **Calculs** / **Accès restreint / séparation des tâches** / **Interfaces** / **Autres risques liés à l'informatique**
Quand ce risque lié à l'informatique peut-il ne pas être pertinent pour l'audit?	Ce risque sera vraisemblablement pertinent pour l'audit, car il a une incidence sur l'intégrité de l'information financière et doit être pris en considération non seulement en tant que risque lié à l'informatique, mais aussi en tant que risque de fraude découlant du contournement des contrôles par la direction.
Exemples de dépendances aux TI liées à ce risque	Il s'agit d'un risque liée à l'intégrité de l'ensemble des données financières; toutefois, ce risque peut aussi découler des calculs ou des rapports générés par les systèmes qui extraient des données permanentes, par exemple : • Le calcul de la conversion en devises étrangères qui utilise les taux de change permanents définis par l'entité. • Un rapport généré par le système qui extrait les données sur les clients.
CGI qui répondent au risque lié à l'informatique (adapter, au besoin, aux contrôles propres à l'entité)	• Les opérations ou les activités liées à la base de données/au fichier de données des super utilisateurs ou des administrateurs et les identificateurs génériques de nature délicate sont soumis à un suivi. • Les opérations ou les activités liées aux applications des super utilisateurs ou des administrateurs et les identificateurs génériques de nature délicate sont soumis à un suivi. • Les demandes d'accès à la base de données/au fichier de données sont examinées avec soin et autorisées par la direction **(recommandé).** • Les demandes d'accès aux applications sont examinées avec soin et autorisées par la direction **(recommandé).** • Le caractère approprié des droits d'accès à la base de données/au fichier de données fait l'objet d'un suivi périodique pour vérifier leur pertinence. • Le caractère approprié des droits d'accès aux applications fait l'objet d'un suivi périodique pour vérifier leur pertinence. • Les droits d'accès à la base de données/au fichier de données des utilisateurs ayant quitté leur emploi sont révoqués en temps opportun **(recommandé).** • Les droits d'accès aux applications des utilisateurs ayant quitté leur emploi sont révoqués en temps opportun **(recommandé).**

Accès aux programmes et aux données

Risque	**À cause de la faiblesse des contrôles d'authentification ou de la déficience des configurations de sécurité, les droits d'accès peuvent être contournés**					
Quel est le risque?	**La faiblesse des mots de passe ou des configurations de sécurité permet l'accès non autorisé.** Même si l'équipe prend en considération les contrôles d'authentification et les configurations de sécurité de manière distincte des autres risques et contrôles, elle examine généralement ce risque avec un ou plusieurs des autres risques du domaine Accès aux programmes et aux données (comme il est indiqué aux pages 11 à 13) au moment de son évaluation. Cela comprend d'autres mécanismes d'authentification, comme l'authentification à deux facteurs (A2F), par exemple lorsque l'utilisateur entre son mot de passe, un code est envoyé à son téléphone mobile et l'utilisateur doit entrer ce code avant d'obtenir l'accès. Ce risque peut différer au niveau des applications, du système d'exploitation et des bases de données.					
De quoi découle-t-il? Type de dépendances aux TI et/ou autres risques liés à l'informatique	**Contrôles automatisés**	**Rapports générés par les systèmes**	**Calculs**	**Accès restreint / séparation des tâches**	**Interfaces**	**Autres risques liés à l'informatique**
Quand ce risque lié à l'informatique peut-il ne pas être pertinent pour l'audit?	**Pour l'accès restreint et la séparation des tâches :** Ce risque est toujours pertinent pour l'audit lorsqu'il y a une dépendance aux TI liée à l'accès restreint/la séparation des tâches. **Pour les contrôles automatisés, les rapports générés par les systèmes, les calculs et les interfaces :** Ce risque est généralement pris en considération avec un ou plusieurs des autres risques du domaine Accès aux programmes et aux données (comme il est indiqué aux pages 11 à 13) et, par conséquent, si l'équipe de mission a conclu que les autres risques du domaine Accès aux programmes et aux données étaient pertinents pour ces types de dépendances aux TI, alors ce risque est pertinent.					
Exemples de dépendances aux TI liées à ce risque	• L'accès au système qui permet de modifier les données de base sur les fournisseurs est restreint et séparé de l'approbation des paiements.					
CGI qui répondent au risque lié à l'informatique (adapter, au besoin, aux contrôles propres à l'entité)	• Les mots de passe donnant accès au système d'exploitation/au réseau et aux configurations de sécurité sont établis efficacement **(*recommandé).** • Les mots de passe donnant accès à la base de données/au fichier de données et aux configurations de sécurité sont établis efficacement **(recommandé).** • Les mots de passe donnant accès aux applications et aux configurations de sécurité sont établis efficacement **(recommandé).**					

Accès aux programmes et aux données

Risque	**Rien n'empêche un accès physique non autorisé aux installations, à l'équipement et aux ressources**					
Quel est le risque?	**Un accès physique non autorisé peut entraîner la non disponibilité ou le traitement inexact ou incomplète de données et de systèmes.**					
De quoi découle-t-il? Type de dépendances aux TI et/ou autres risques liés à l'informatique	**Contrôles automatisés**	**Rapports générés par les systèmes**	**Calculs**	**Accès restreint / séparation des tâches**	**Interfaces**	**Autres risques liés à l'informatique**
Quand ce risque lié à l'informatique peut-il ne pas être pertinent pour l'audit?	Il est peu probable que ce risque soit pertinent pour la plupart des missions. Cependant, les équipes de mission doivent prendre en considération la probabilité que l'accès physique non autorisé ait une incidence sur les données nécessaires pour préparer les états financiers dans le cadre de l'ensemble de l'environnement de contrôle. Lorsqu'une entité a établi des ententes d'impartition, comme un logiciel-service, une plateforme-service, une infrastructure-service ou un centre de données de tierce partie, si l'équipe conclut que cela constitue un risque lié à l'informatique qui concerne l'accès physique pour l'audit, il est important que le risque soit maîtrisé par des contrôles visés par l'étendue du rapport de l'auditeur choisi par l'organisation de services à l'égard des contrôles internes et tout contrôle complémentaire pertinent de l'entité utilisatrice devra être mis en place par l'entité auditée.					
Exemples de dépendances aux TI liées à ce risque	• S. O. Les risques liés à l'accès physique n'ont généralement pas d'incidence directe sur les risques découlant des dépendances aux TI.					
CGI qui répondent au risque lié à l'informatique (adapter, au besoin, aux contrôles propres à l'entité)	• Des mesures de sécurité matérielle sont en place **(recommandé).**					

Modifications aux programmes

Risque	**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'application empêchent les systèmes de traiter les enregistrements de transactions de manière complète et exacte**
Quel est le risque?	**L'appui sur une fonctionnalité de système qui traite des données inexactes ou qui traite les données de manière inexacte, ou les deux.** La configuration est un aspect important de nombreuses applications, car celle-ci a un impact sur comment l'application répond aux besoins de l'entité. **Pour les modifications apportées à la configuration des applications** : les utilisateurs (fonction de TI ou secteur d'activités) peuvent contourner les contrôles liés au changement et apporter des modifications non autorisées aux paramètres de configuration des applications. De plus, l'entité peut omettre d'apporter les modifications nécessaires à la configuration (p. ex. des modifications devant être mise en œuvre en raison de l'adoption de nouveaux règlements, de normes comptables ou de politiques). **Pour les modifications apportées aux programmes d'applications :** Le code est écrit dans la fonctionnalité inhérente de l'application, généralement par le fournisseur, et ne peut être modifié selon les besoins de l'entité à moins que la fonction de TI ou d'autres utilisateurs peuvent modifier le code. Il y a donc un risque dans un tel cas. Il y a aussi un risque lorsqu'il faut modifier le code en raison de changements apportés, par exemple, à la présentation de l'information financière ou aux règlements et que le code n'est pas modifié. De plus, il y a un risque lorsque des tiers ont les accès nécessaires pour modifier le code directement dans l'environnement informatique de l'entité. Ce risque peut être pris en considération avec les risques liés à la gestion des incidents, c.-à-d. le risque que des défauts ou des erreurs dans les changements traités ne soient pas détectés et résolus. La différence entre les modifications apportées à la configuration et celles apportées aux programmes est la suivante : les modifications apportées à la configuration modifient le fonctionnement de l'application sans avoir à modifier le code (p. ex. la sélection d'options configurables pour les seuils d'approbation).
De quoi découle-t-il? Type de dépendances aux TI et/ou autres risques liés à l'informatique	**Contrôles automatisés** | **Rapports générés par les systèmes** | **Calculs** | **Accès restreint / séparation des tâches** | **Interfaces** | **Autres risques liés à l'informatique**
Quand ce risque lié à l'informatique peut-il ne pas être pertinent pour l'audit?	**Pour les modifications apportées à la configuration des applications :** Ce risque n'est pas pertinent pour l'audit si aucune des dépendances aux TI n'ont été ou ne peuvent être configurées. **Pour les modifications apportées aux programmes d'applications :** Ce risque n'est pas pertinent pour l'audit si l'entité n'a pas de service interne de développement ou de programmation ou si les développeurs (y compris les tiers) ne peuvent modifier la fonctionnalité codée.
Exemples de dépendances aux TI liées à ce risque	**Pour les contrôles automatisés, les rapports générés par les systèmes et les calculs :** •Ce risque est pertinent pour les dépendances aux TI qui ont été configurées ou peuvent l'être. Par exemple, un contrôle automatisé lié au triple rapprochement qui peut être configuré de manière à faire un rapprochement en deçà d'un certain seuil (p. ex. un rapprochement est effectué si la différence est inférieure à 5 %). **Pour les interfaces :** •Ce risque est généralement pertinent si l'interface ou le processus par lots s'appuie sur un programme pour déclencher le transfert de données.
CGI qui répondent au risque lié à l'informatique (adapter, au besoin, aux contrôles propres à l'entité)	• Les modifications apportées à la configuration des applications et/ou aux programmes d'applications sont adéquatement testées et approuvées avant d'être transférées à l'environnement de production **(recommandé).** • Le caractère approprié des modifications apportées à la configuration des applications et/ou aux programmes d'applications fait l'objet d'un suivi périodique. • Les environnements de développement, de test et de production sont séparés pour ce qui est des modifications apportées à la configuration des applications et/ou aux programmes d'applications **(recommandé).**

Modifications aux programmes

Risque	**Des modifications non autorisées ou non testées, ou l'omission d'apporter les modifications nécessaires aux bases de données, au système d'exploitation ou au réseau empêchent les systèmes de traiter les enregistrements de transactions de manière complète et exacte**					
Quel est le risque?	**Des modifications ou l'omission d'apporter les modifications nécessaires à l'environnement informatique dans lequel les applications sont exécutées (c.-à-d. les bases de données, les systèmes d'exploitation et les réseaux) peuvent entraîner le traitement de données inexactes ou le traitement inexacte de données par les systèmes, ou les deux.** Des modifications (ou l'omission d'apporter les modifications nécessaires) peuvent entraîner le non fonctionnement de l'application comme prévu et/ou l'impossibilité pour les utilisateurs d'accéder à l'application (c.-à-d. l'application plante ou fige). Ce risque doit être pris en considération lorsque des mise à niveau importantes sont apportées à l'infrastructure informatique. Ce risque peut être pris en considération avec les risques liés à la gestion des incidents, c.-à-d. le risque que des défauts ou des erreurs dans les changements traités ne soient pas détectés et résolus.					
De quoi découle-t-il? Type de dépendances aux TI et/ou autres risques liés à l'informatique	Contrôles automatisés	Rapports générés par les systèmes	Calculs	Accès restreint / séparation des tâches	Interfaces	Autres risques liés à l'informatique
Quand ce risque lié à l'informatique peut-il ne pas être pertinent pour l'audit?	Si les seuls changements apportés à l'environnement de TI sont des correctifs de routine ou d'urgence du fournisseur apportés au niveau du système d'exploitation, alors il est peu probable que ce risque soit pertinent pour l'audit. Si le plan d'audit ne prévoit pas tester l'efficacité du fonctionnement des CGI, il peu probable que ce risque soit pertinent pour l'audit.					
Exemples de dépendances aux TI liées à ce risque	• S. O. Les risques liés aux modifications non autorisées ou non testées, ou à l'omission d'apporter les modifications nécessaires aux bases de données, aux systèmes d'exploitation ou au réseau n'ont généralement pas d'incidence directe sur les risques découlant des dépendances aux TI.					
CGI qui répondent au risque lié à l'informatique (adapter, au besoin, aux contrôles propres à l'entité)	• Les modifications apportées au système d'exploitation ou au réseau sont adéquatement testées et approuvées avant d'être transférés à l'environnement de production. • Le caractère approprié des modifications apportées au système d'exploitation ou au réseau fait l'objet d'un suivi périodique. • Les modifications apportées aux bases de données sont adéquatement testées et approuvées avant d'être transférés à l'environnement de production. • Le caractère approprié des modifications apportées aux bases de données fait l'objet d'un suivi périodique. • Les environnements de développement, de test et de production sont séparés pour ce qui est des modifications apportées au système d'exploitation ou au réseau. • Les environnements de développement, de test et de production sont séparés pour ce qui est des modifications apportées aux bases de données.					

Modifications aux programmes

Risque	**Des modifications non autorisées ou non testées, ou l'omission d'apporter les modifications nécessaires aux processus par lots empêchent les systèmes de traiter les enregistrements de transactions de manière complète et exacte**
Quel est le risque?	**Les données ne sont pas transférées en totalité ou avec exactitude entre les systèmes ou de multiples opérations traitées automatiquement comme un seul ensemble ne sont pas traitées.** Une interface permet le transfert de données transactionnelles d'une application à l'autre (p. ex. le transfert des niveaux de stocks dans le système de gestion de l'entrepôt à l'application financière). Les processus par lots sont des mises à jour automatiques configurées dans le système qui remplacent ce qui normalement aurait été une saisie manuelle de données (p. ex. la mise à jour automatique et quotidienne de données sur les prix liées à un produit de placement). Des modifications non autorisées, ou l'omission d'apporter les modifications nécessaires, peuvent entraîner des données financières incomplètes et/ou inexactes. Ce risque peut être pris en considération avec les risques liés à la gestion des incidents, c.-à-d. le risque que des défauts ou des erreurs dans les changements traités ne soient pas détectés et résolus.
De quoi découle-t-il? Type de dépendances aux TI et/ou autres risques liés à l'informatique	Contrôles automatisés | Rapports générés par les systèmes | Calculs | Accès restreint / séparation des tâches | **Interfaces** | Autres risques liés à l'informatique
Quand ce risque lié à l'informatique peut-il ne pas être pertinent pour l'audit?	Ce risque sera toujours pertinent pour l'audit lorsqu'il y a des interfaces ou de multiples transactions qui sont traitées comme un seul ensemble au moyen de processus par lots.
Exemples de dépendances aux TI liées à ce risque	• Une interface entre un système de gestion de l'entrepôt et une application financière. • Une interface entre un système du point de vente et une application financière. • La mise à jour par lots des données sur les prix.
CGI qui répondent au risque lié à l'informatique (adapter, au besoin, aux contrôles propres à l'entité)	• Les modifications apportées à la configuration des applications sont adéquatement testées et approuvées avant d'être transférées à l'environnement de production. • Le caractère approprié des modifications apportées à la configuration des applications fait l'objet d'un suivi périodique. • Les environnements de développement, de test et de production sont séparés pour ce qui est des modifications apportées à la configuration des applications. • Seules les modifications approuvées et testées sont apportées au planificateur de lots **(recommandé).**

Développement de programmes

Risque	**Les systèmes nouvellement implantés (ou améliorés en profondeur) traitent les données de manière incomplète ou inexacte (p. ex. en raison d'erreurs de codage ou de configuration)**					
Quel est le risque?	**L'implantation de nouvelles applications ou la modification en profondeur d'applications existantes peuvent entraîner un traitement inexact des données.** Cela peut découler du fait que le système ne fonctionne pas comme les utilisateurs opérationnels le prévoyaient, soit parce que les exigences ont été mal comprises et les essais n'ont pas relevé le problème, soit parce qu'on a sciemment pris la décision de faire la mise en service malgré les défauts connus.					
De quoi découle-t-il? Type de dépendances aux TI et/ou autres risques liés à l'informatique	**Contrôles automatisés**	**Rapports générés par les systèmes**	**Calculs**	**Accès restreint / séparation des tâches**	**Interfaces**	**Autres risques liés à l'informatique**
Quand ce risque lié à l'informatique peut-il ne pas être pertinent pour l'audit?	Si aucune nouvelle application ni aucun autre aspect de l'environnement informatique n'a été mis en place ou modifié en profondeur au cours de la période considérée, alors ce risque n'est probablement pas pertinent pour l'audit.					
Exemples de dépendances aux TI liées à ce risque	• S. O. Les risques découlant de systèmes nouvellement implantés ou modifiés en profondeur n'ont généralement pas d'incidence directe sur les dépendances aux TI.					
CGI qui répondent au risque lié à l'informatique (adapter, au besoin, aux contrôles propres à l'entité)	• Les nouveaux systèmes et les améliorations sont adéquatement testés et approuvés avant d'être transférés à l'environnement de production **(recommandé).** • Les problèmes qui surgissent pendant le développement de programmes font l'objet d'un suivi et sont résolus. • Une formation appropriée est offerte.					

Développement de programmes

Risque	**Les transactions enregistrées et/ou les données de base n'ont pas été transférées en totalité et avec exactitude**					
Quel est le risque?	**Les données ne sont pas transférées en totalité et avec exactitude lors de l'implantation d'un nouveau système ou de la migration vers ce dernier.** Lorsqu'une entité implante une nouvelle application et/ou fait la migration des applications existantes vers une autre base de données, un autre serveur ou le nuage, il y a un risque que les données permanentes, comme les données de base sur les fournisseurs, les données des grands livres auxiliaires ou les données transactionnelles, ne soient pas transférées en totalité et/ou avec exactitude.					
De quoi découle-t-il? Type de dépendances aux TI et/ou autres risques liés à l'informatique	**Contrôles automatisés**	**Rapports générés par les systèmes**	**Calculs**	**Accès restreint / séparation des tâches**	**Interfaces**	**Autres risques liés à l'informatique**
Quand ce risque lié à l'informatique peut-il ne pas être pertinent pour l'audit?	Il est probable que ce risque soit pertinent seulement dans les cas où l'entité a entrepris l'implantation d'un système, si les données d'une ancienne application ne sont pas transférées à la nouvelle application (c.-à-d. lorsque la nouvelle application sera utilisée seulement pour traiter les transactions de manière prospective à partir de la date de mise en œuvre).					
Exemples de dépendances aux TI liées à ce risque	• S. O. Les risques découlant de la migration des transactions enregistrées et/ou des données de base n'ont généralement pas d'incidence directe sur les risques découlant des dépendances aux TI.					
CGI qui répondent au risque lié à l'informatique (adapter, au besoin, aux contrôles propres à l'entité)	• La migration ou la conversion des données est effectuée adéquatement **(recommandé).**					

Opérations informatiques

Risque	**Présence de changements inappropriés, intervention manuelle ou manquements en rapport avec la planification des travaux**
Quel est le risque?	**Les données ne sont pas transférées en totalité et/ou avec exactitude entre les systèmes ou de multiples transactions automatiquement traitées comme un seul ensemble ne sont pas traitées en raison de l'apport de modifications inappropriées aux processus par lots (manuels ou autres) ou de problèmes au moment de l'exécution des processus par lots.** Les processus par lots sont des mises à jour automatiques configurées dans le système qui remplacent ce qui normalement aurait été une saisie manuelle pour de multiples transactions en un seul groupe (p. ex. la mise à jour automatique et quotidienne de données sur les prix liées à un produit de placement). Si ces processus par lots sont modifiés ou si leur exécution comporte des erreurs ou des défaillances, cela peut entraîner des données financières incomplètes et/ou inexactes.
De quoi découle-t-il? Type de dépendances aux TI et/ou autres risques liés à l'informatique	**Contrôles automatisés** | **Rapports générés par les systèmes** | **Calculs** | **Accès restreint / séparation des tâches** | **Interfaces** | **Autres risques liés à l'informatique**
Quand ce risque lié à l'informatique peut-il ne pas être pertinent pour l'audit?	Ce risque sera toujours pertinent pour l'audit lorsqu'il y a des interfaces ou de multiples transactions qui sont traitées comme un seul ensemble et qui sont mises à jour automatiquement au moyen de processus par lots.
Exemples de dépendances aux TI liées à ce risque	• La mise à jour par lots des données sur les prix. • La mise à jour automatique des taux de change dans l'application d'information financière tous les mois.
CGI qui répondent au risque lié à l'informatique (adapter, au besoin, aux contrôles propres à l'entité)	• Les erreurs liées au traitement dans l'environnement de production sont détectées et corrigées. • Seules les modifications approuvées et testées sont apportées au planificateur de lots **(recommandé).**

Opérations informatiques

Risque	**Le transfert des transactions enregistrées entre des systèmes est incomplet ou inexact**
Quel est le risque?	**Les données ne sont pas transférées en totalité ou avec exactitude entre les applications.** Une interface permet le transfert de données transactionnelles d'une application à l'autre. Ce risque concerne en particulier l'information qui doit être transférée d'une application à l'autre afin que les CGI fonctionnent efficacement (p. ex. lorsque l'information sur les personnes qui se joignent à l'organisation, changent de service ou quittent l'organisation est transférée automatiquement entre le système de RH et le système de gestion de l'identité utilisé par le service de TI pour gérer les droits d'accès, afin que les droits d'accès puissent être accordés en temps opportun en fonction des rôles et des responsabilités de la nouvelle recrue ou qu'ils puissent être révoqués en temps opportun lorsqu'une personne quitte l'entreprise).
De quoi découle-t-il? Type de dépendances aux TI et/ou autres risques liés à l'informatique	**Contrôles automatisés** / **Rapports générés par les systèmes** / **Calculs** / **Accès restreint / séparation des tâches** / **Interfaces** / **Autres risques liés à l'informatique**
Quand ce risque lié à l'informatique peut-il ne pas être pertinent pour l'audit?	Ce risque n'est pas pertinent pour un audit lorsqu'aucun dossier de transaction n'est transféré entre des systèmes qui sont importants pour les CGI (c.-à-d. pour assurer l'efficacité du fonctionnement des CGI, ces derniers n'ont pas besoin de recevoir des informations ou des dossiers d'un autre système).
Exemples de dépendances aux TI liées à ce risque	• La révocation automatisée des droits d'accès dépend du transfert automatisé des données des personnes quittant l'organisation à partir du système de RH. • L'information sur les employés actifs conservée dans les données du service des finances, y compris leurs rôles, est transférée automatiquement du système de ressources humaines au système de gestion des accès utilisé par le service de TI pour faire l'examen périodique des droits d'accès.
CGI qui répondent au risque lié à l'informatique (adapter, au besoin, aux contrôles propres à l'entité)	• Les erreurs liées au traitement dans l'environnement de production sont détectées et corrigées **(recommandé).** • Seules les modifications approuvées et testées sont apportées au planificateur de lots.

Opérations informatiques

Risque	**Des transactions enregistrées sont perdues (p. ex., en raison d'une défaillance du système) et des données sont irrécupérables ou corrompues/inscrites en double lors du processus de récupération**				
Quel est le risque?	**Des données sont perdues, corrompues ou inscrites en double.** Si l'entité ne peut pas avoir accès à des données complètes et exactes qui sont pertinentes pour l'information financière, l'entité ne sera pas en mesure de préparer des états financiers complets et exacts. Ce risque est associé au risque lié à la cybersécurité concernant les attaques par rançongiciel – voir la page 26.				
De quoi découle-t-il? Type de dépendances aux TI et/ou autres risques liés à l'informatique	Contrôles automatisés	Rapports générés par les systèmes	Calculs	Accès restreint / séparation des tâches	Interfaces	**Autres risques liés à l'informatique**
Quand ce risque lié à l'informatique peut-il ne pas être pertinent pour l'audit?	Si l'équipe n'a pas déterminé qu'il y avait un risque d'anomalies significatives lié à la perte ou à la corruption de données découlant d'un incident de cybersécurité, il est possible que ce risque ne soit pas pertinent pour l'audit.					
Exemples de dépendances aux TI liées à ce risque	• S. O. Les risques liés aux sauvegardes ou à la disponibilité des données n'ont généralement pas d'incidence sur les risques découlant des dépendances aux TI.					
CGI qui répondent au risque lié à l'informatique (adapter, au besoin, aux contrôles propres à l'entité)	• Les données sont sauvegardées de manière appropriée et récupérables **(recommandé).**					

Cybersécurité

Risque	**Les cyberattaques et les attaques par rançongiciel exploitent les vulnérabilités, entraînant ainsi la manipulation et/ou la destruction de données, ce qui compromet les états financiers ou la disponibilité du système et, par le fait même, la présentation de l'information financière en temps opportun**				
Quel est le risque?	**L'entité ne peut pas prévenir ni limiter les dommages causés par les cyberattaques.** Une vulnérabilité est une faiblesse dans un système qui pourrait être exploitée ou déclenchée par une source de menace (p. ex. un pirate informatique). Tous les systèmes possèdent un certain degré de vulnérabilité et si ces vulnérabilités ne sont pas gérées par l'entité au moyen d'un programme de cybersécurité, elles pourraient entraîner la perte de données, la destruction de données, ou barrer l'accès de l'entité aux systèmes, ce qui aurait une incidence sur sa capacité de mener ses activités et de présenter des rapports en temps opportun.				
De quoi découle-t-il? Type de dépendances aux TI et/ou autres risques liés à l'informatique	**Contrôles automatisés**	**Rapports générés par les systèmes**	**Calculs**	**Accès restreint / séparation des tâches**	**Interfaces**	**Autres risques liés à l'informatique**
Quand cela peut-il ne pas représenter un risque d'anomalies significatives? (*)	Il ne s'agit pas d'un risque d'anomalies significatives si, compte tenu de la compréhension de l'évaluation du risque lié à la cybersécurité de l'entité et de l'exposition courante « Prévention/détection et surveillance des intrusions », y compris la compréhension du programme de surveillance des incidents et de l'architecture de réseau de l'entité, l'équipe de mission détermine que les cyberattaques ou les attaques par rançongiciel ne donnent pas lieu à un risque d'anomalies significatives au niveau des états financiers de l'entité.				
Exemples de dépendances aux TI liées à ce risque	• S. O. Les risques liés aux vulnérabilités n'ont généralement pas d'incidence directe sur les risques découlant des dépendances aux TI.				
CGI qui répondent au risque lié à l'informatique (adapter, au besoin, aux contrôles propres à l'entité)	• Un programme de prévention et/ou de détection des intrusions est en place pour veiller à ce que les incidents de sécurité soient surveillés et signalés aux parties prenantes pertinentes **(recommandé).** • Un programme de gestion des correctifs est en place pour veiller à ce que les vulnérabilités de sécurité soient traitées, surveillées et signalées **(recommandé).** • Les données financièrement importantes sont sauvegardées à une fréquence appropriée et leur recouvrabilité est périodiquement vérifiée **(recommandé).**				

(*) Compte tenu de la nature et de l'omniprésence du cybercrime, toutes les entités peuvent être exposées à des risques liés à la cybersécurité; toutefois, les équipes de mission doivent déterminer si ces risques sont pertinents pour l'entité en ce qui concerne la façon dont le modèle d'activité de l'entité intègre l'utilisation de l'informatique et la façon dont les expositions courantes aux risques liés à la cybersécurité peuvent entraîner des **risques d'anomalies significatives** dans les états financiers. Voir la section BVG Audit 5035.2 – Considérations relatives à l'évaluation des risques liés à la cybersécurité pour d'autres directives et se reporter aux considérations additionnelles relatives au risque dans la procédure « Compréhension et identification des risques liés à la cybersécurité associés à l'audit ».

Cybersécurité

Risque	**Les systèmes non corrigés mènent à l'exploitation de vulnérabilités, entraînant ainsi la manipulation et/ou la destruction de données, ce qui compromet les états financiers ou la disponibilité du système et, par le fait même, la présentation de l'information financière en temps opportun**				
Quel est le risque?	**Les vulnérabilités connues ne sont pas réglées par un correctif, ce qui augmente le risque que ces vulnérabilités soient exploitées par l'auteur d'une cyberattaque.** Lorsqu'un fournisseur a connaissance qu'une application ou un autre logiciel contient une faille de sécurité, il corrige généralement le problème en diffusant un correctif ou une mise à jour logicielle que les entités doivent mettre en œuvre afin de se protéger contre le piratage. Si un correctif est oublié ou s'il n'est pas appliqué en temps opportun, les pirates pourraient en tirer avantage pour accéder aux systèmes de l'entité.				
De quoi découle-t-il? Type de dépendances aux TI et/ou autres risques liés à l'informatique	**Contrôles automatisés**	**Rapports générés par les systèmes**	**Calculs**	**Accès restreint / séparation des tâches**	**Interfaces**	**Autres risques liés à l'informatique**
Quand cela peut-il ne pas représenter un risque d'anomalies significatives? (*)	Les systèmes non corrigés ne représentent pas un risque d'anomalies significatives si, compte tenu de la compréhension de l'évaluation du risque lié à la cybersécurité de l'entité et de l'exposition courante « Gestion des correctifs », y compris la compréhension des politiques et des procédures de gestion des correctifs de l'entité, l'équipe de mission détermine que les systèmes non corrigés ne donnent pas lieu à un risque d'anomalies significatives au niveau des états financiers de l'entité.				
Exemples de dépendances aux TI liées à ce risque	• S. O. Les risques liés aux systèmes non corrigés n'ont pas généralement d'incidence directe sur les risques découlant des dépendances aux TI.				
CGI qui répondent au risque lié à l'informatique (adapter, au besoin, aux contrôles propres à l'entité)	• Un programme de gestion des correctifs est en place pour veiller à ce que les vulnérabilités de sécurité soient traitées, surveillées et signalées **(recommandé).**				

(*) Compte tenu de la nature et de l'omniprésence du cybercrime, toutes les entités peuvent être exposées à des risques liés à la cybersécurité; toutefois, les équipes de mission doivent déterminer si ces risques sont pertinents pour l'entité en ce qui concerne la façon dont le modèle d'activité de l'entité intègre l'utilisation de l'informatique et la façon dont les expositions courantes aux risques liés à la cybersécurité peuvent entraîner des **risques d'anomalies significatives** dans les états financiers. Voir la section BVG Audit 5035.2 – Considérations relatives à l'évaluation des risques liés à la cybersécurité pour d'autres directives et se reporter aux considérations additionnelles relatives au risque dans la procédure « Compréhension et identification des risques liés à la cybersécurité associés à l'audit ».

Cybersécurité

Risque	**Les attaques par rançongiciel rendent les systèmes inaccessibles, ce qui a une incidence sur la disponibilité des systèmes et sur la capacité de l'entité à préparer l'information financière en temps opportun**					
Quel est le risque?	**L'entité ne peut pas accéder aux données ou aux systèmes pertinents pour la présentation de l'information financière.** Le rançongiciel est un maliciel qui empêche l'utilisation des données ou des systèmes jusqu'à ce que la victime effectue un paiement (« rançon »). Ce risque est lié au risque « Des transactions enregistrées sont perdues (p. ex., en raison d'une défaillance du système) et des données sont irrécupérables ou corrompues/inscrites en double lors du processus de récupération » (voir la page 23).					
De quoi découle-t-il? Type de dépendances aux TI et/ou autres risques liés à l'informatique	**Contrôles automatisés**	**Rapports générés par les systèmes**	**Calculs**	**Accès restreint / séparation des tâches**	**Interfaces**	**Autres risques liés à l'informatique**
Quand cela peut-il ne pas représenter un risque d'anomalies significatives? (*)	Un rançongiciel ne représente pas un risque d'anomalies significatives si, compte tenu de la compréhension de l'évaluation du risque lié à la cybersécurité de l'entité et de l'exposition courante « Sauvegarde et récupération », y compris la compréhension de la stratégie de sauvegarde et des plans de récupération de l'entité, l'équipe de mission détermine qu'une attaque par rançongiciel ne donne pas lieu à un risque d'anomalies significatives au niveau des états financiers de l'entité.					
Exemples de dépendances aux TI liées à ce risque	• S. O. Les risques liés aux rançongiciels n'ont généralement pas d'incidence directe sur les risques découlant des dépendances aux TI.					
CGI qui répondent au risque lié à l'informatique (adapter, au besoin, aux contrôles propres à l'entité)	• Les données financières importantes sont sauvegardées à intervalles appropriés, et la capacité de les récupérer est périodiquement testée **(recommandé).**					

(*) Compte tenu de la nature et de l'omniprésence du cybercrime, toutes les entités peuvent être exposées à des risques liés à la cybersécurité; toutefois, les équipes de mission doivent déterminer si ces risques sont pertinents pour l'entité en ce qui concerne la façon dont le modèle d'activité de l'entité intègre l'utilisation de l'informatique et la façon dont les expositions courantes aux risques liés à la cybersécurité peuvent entraîner des **risques d'anomalies significatives** dans les états financiers. Voir la section BVG Audit 5035.2 – Considérations relatives à l'évaluation des risques liés à la cybersécurité pour d'autres directives et se reporter aux considérations additionnelles relatives au risque dans la procédure « Compréhension et identification des risques liés à la cybersécurité associés à l'audit ».

Droit d’auteur s’appliquant au BVG

© Sa Majesté le Roi du chef du Canada, représenté par la Vérificatrice générale du Canada, 2022.

AVIS CONCERNANT LE DROIT D’AUTEUR — Ce document est destiné à un usage interne. Il ne peut être reproduit par ou distribué à des tierces parties par courriel, par télécopieur, par courrier, en main propre ou par tout autre moyen de distribution ou de reproduction sans le consentement écrit du Coordonnateur des droits d’auteur du Bureau du vérificateur général du Canada.

Licence conventionnelle de CPA Canada

© 2022 Comptables professionnels agréés du Canada. Tous droits réservés.
© 2022 *IFRS Foundation*. Tous droits réservés.
© 2022 *International Federation of Accountants*. Tous droits réservés.
© 2022 *American Institute of Certified Public Accountants* (NCMC 3416). Tous droits réservés.

Les paragraphes du Manuel de CPA Canada sont reproduits ici pour votre utilisation non-commerciale avec l’autorisation des Comptables professionnels agréés du Canada (CPA Canada). Ils ne peuvent pas être modifiés, copiés ou distribués, sous une forme quelconque, car cela transgresserait le droit d’auteur de CPA Canada.

Reproduit à partir du Manuel de CPA Canada avec l’autorisation des Comptables professionnels agréés du Canada, Toronto, Canada.