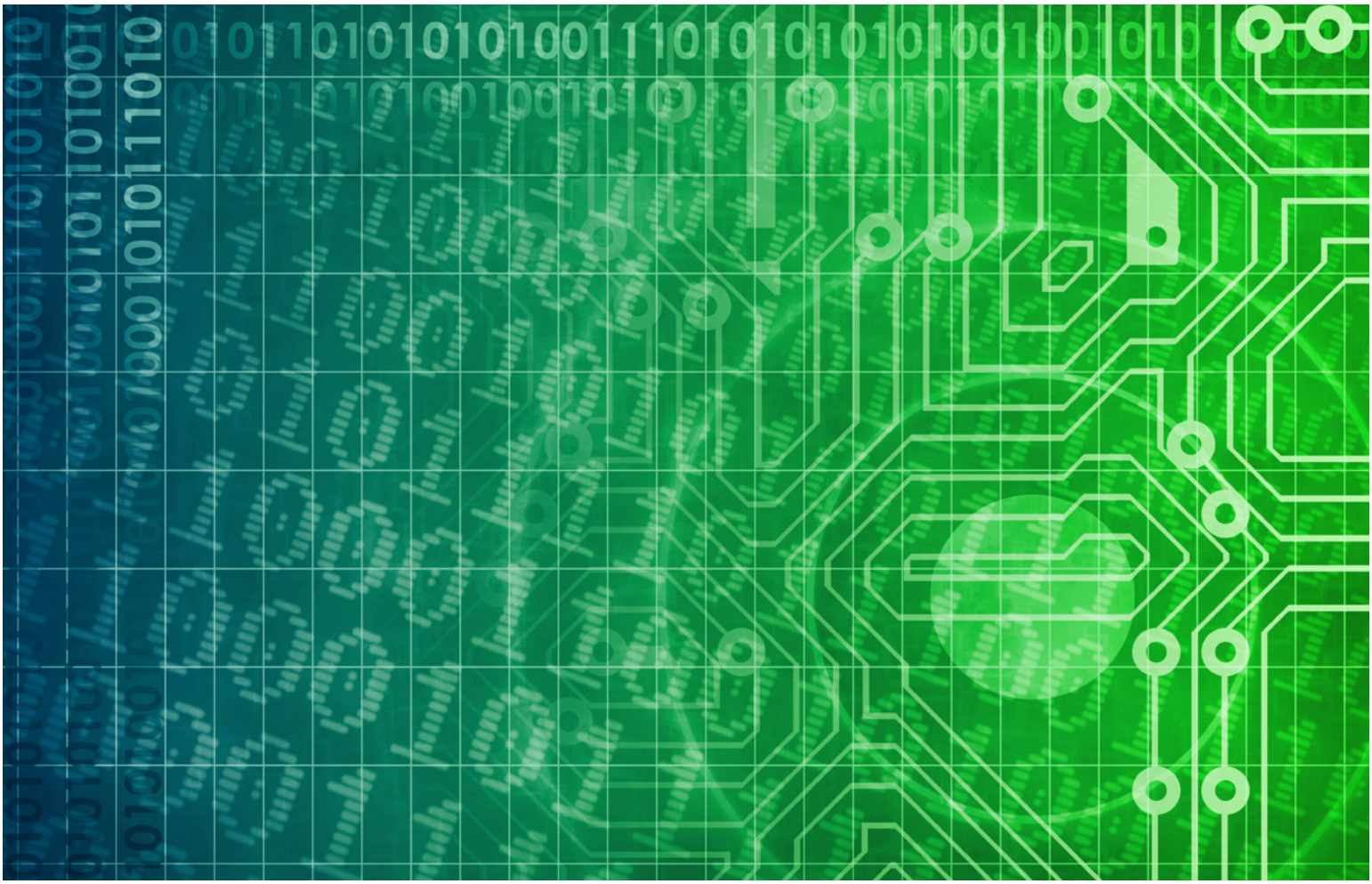
CPA COMPTABLES PROFESSIONNELS AGRÉÉS CANADA

Cadre de contrôle de l'intégrité de l'information

Auteur principal : J. Efrim Boritz, Ph. D., FCPA, FCA, CISA
Coauteur : Malik Datardina, M. Compt., CPA, CA, CISA



AVERTISSEMENT

Le présent document, préparé par Comptables professionnels agréés du Canada (CPA Canada), fournit des indications ne faisant pas autorité.

CPA Canada et les auteurs déclinent toute responsabilité ou obligation pouvant découler, directement ou indirectement, de l'utilisation de cette publication.

Avant-propos

Devant la prodigieuse expansion de l'analyse de données et des nouvelles technologies qui reposent sur les données, telles que l'apprentissage machine, les organisations ont besoin de lignes directrices simples et concrètes sur les risques et les contrôles pour les aider à assurer l'intégrité de l'information qu'elles diffusent ou sur laquelle elles s'appuient. Le présent document se veut un outil dont les organisations pourront se servir pour évaluer et documenter leurs contrôles d'intégrité de l'information et réaliser leurs missions portant sur la conformité et leurs missions d'audit.

Bien des cadres de contrôle ont pour objectif ultime la qualité et l'intégrité de l'information, sans pour autant faire de lien clair et direct entre l'intégrité de l'information et les processus, les leviers et les contrôles nécessaires pour assurer cette intégrité. Cette rupture peut entraîner un déséquilibre entre la mise en place des contrôles indirects (généraux) et directs (des applications) par les dirigeants et les auditeurs et l'effort d'audit qui y est consacré. En outre, elle peut se traduire par des mesures qui sont insuffisantes pour atteindre le niveau d'assurance requis à l'égard de l'intégrité de l'information. Par ailleurs, le caractère suffisant des contrôles de l'intégrité des données d'une organisation varie d'un ensemble de données à l'autre, les données réglementaires et financières faisant l'objet de contrôles plus rigoureux que les données opérationnelles.

La présente publication vise à proposer aux dirigeants, auditeurs, spécialistes de la conformité, administrateurs financiers et professionnels de la gestion de l'information un cadre pour identifier les principaux risques d'entreprise associés à l'intégrité de l'information et y réfléchir, ainsi que pour concevoir et mettre en place des leviers et des contrôles visant à assurer l'intégrité de l'information. Dans la même optique, le cadre peut aussi aider à la planification de procédures pour évaluer l'adéquation de la conception des contrôles et l'efficacité de leur fonctionnement. On trouvera, dans des publications complémentaires, des analyses plus détaillées des risques liés à l'intégrité de l'information, des leviers et des contrôles qui peuvent être utilisés pour répondre à ces risques et des services de certification auxquels il est possible de faire appel pour évaluer l'adéquation de la conception des leviers et des contrôles et l'efficacité de leur fonctionnement.

CPA Canada souhaite remercier J. Efrim Boritz, Ph. D., FCPA, FCA, CISA, auteur principal, et Malik Datardina, M. Compt., CPA, CA, CISA, coauteur, ainsi que le Groupe consultatif pour le temps et les efforts qu'ils ont consacrés à la réalisation de la présente étude. CPA Canada remercie également Andrée Lavigne, CPA, CA, qui a dirigé le projet.

Groupe consultatif

Auteur principal et président

J. Efrim Boritz, Ph. D., FCPA, FCA, CISA
Université de Waterloo
Waterloo (Ontario)

Coauteur

Malik Datardina, M. Compt., CPA, CA, CISA
Auvenir
Toronto (Ontario)

Chris Anderson, CA (Nouvelle-Zélande), CISA, CMC, CISSP
Toronto (Ontario)

Usuff Curim, FCCA, CISA, CPA
PricewaterhouseCoopers
Toronto (Ontario)

Ray Henrickson, CPA, CA, CISA
Banque Scotia (retraité)
Toronto (Ontario)

Darren James ACA, CISA
Deloitte
Toronto (Ontario)

Richard Livesley
BMO Groupe financier (retraité)
Toronto (Ontario)

Madhavan Nayar
Infogix, Inc.
Naperville (Illinois, É.-U.)

Sheryl A. Teed, FCPA, FCA, CISA, CFE
Ernst & Young s.r.l./S.E.N.C.R.L. (retraitée)
Toronto (Ontario)

Directrice du projet

Andrée Lavigne, CPA, CA
Ancienne membre du personnel
de CPA Canada (Montréal)

Table des matières

Cadre de contrôle de l'intégrité de l'information

Objectif

L'information tire sa valeur de sa pertinence, de son utilité ou facilité d'utilisation, et de son intégrité, trois qualités qui peuvent être évaluées en fonction de l'usage auquel l'information est destinée. Si la pertinence et l'utilité ou facilité d'utilisation sont des composantes importantes de la valeur de l'information, la présente publication porte principalement sur l'intégrité. Pour que la planification, la prise de décisions, la surveillance et le contrôle soient efficaces, il est essentiel que l'intégrité de l'information soit préservée. La responsabilité des hauts dirigeants à l'égard de l'intégrité de l'information d'une entité et de ses contrôles internes est aujourd'hui bien connue dans le monde des affaires et le secteur public. On a parfois considéré que les risques d'atteinte à l'intégrité de l'information étaient circonscrits au seul domaine de l'information financière; mais en réalité, ces risques touchent la totalité de l'information qui est recueillie, créée, emmagasinée, utilisée et diffusée par les entreprises et d'autres entités. Les entités ont donc tout intérêt à surveiller leurs activités et à vérifier qu'elles sont conformes aux textes légaux et réglementaires et aux normes pertinents relatifs à l'intégrité de l'information.

La popularité grandissante de l'analyse des données – qu'elle porte ou non sur les mégadonnées – et d'autres technologies nouvelles qui dépendent des données, telles que l'apprentissage machine, témoigne de la volonté des organisations d'extraire de la valeur de leurs données. Cependant, pour pouvoir en tirer des renseignements significatifs, la direction doit s'assurer de l'intégrité des données sous-jacentes. Le manque d'intégrité des données coûte chaque année des milliards de dollars à l'économie, ébranle la confiance que les dirigeants d'entreprises accordent à l'information sur laquelle ils s'appuient pour prendre des décisions et plonge les utilisateurs dans l'incertitude quant à l'exactitude de leurs données. IBM place d'ailleurs la « véracité » parmi les propriétés des mégadonnées, appelées les « 4 V »[1], soulignant ainsi l'importance du lien qui unit l'intégrité de l'information et l'utilisation efficace de l'analyse des données pour tirer des « observations applicables » de l'information[2].

1 Les trois autres propriétés sont le volume, la variété et la vélocité.

2 https://www.ibmbigdatahub.com/infographic/four-vs-big-data

La présente publication vise à définir l'intégrité de l'information et à la mettre en contexte pour les utilisateurs et les préparateurs de l'information, qui ont besoin de savoir comment atteindre et protéger cette intégrité. Elle décrit plus particulièrement les risques menaçant l'intégrité de l'information ainsi que les contre-mesures apportées par les leviers et les contrôles. Il va sans dire que ceux qui sont appelés à fournir une assurance à l'égard de l'intégrité de l'information pourront aussi tirer profit de la présente publication.

Pour faire face aux risques d'atteinte à l'intégrité de l'information d'une manière ordonnée et rigoureuse, il faut un cadre complet qui saura guider la direction dans l'évaluation des risques et le choix des caractéristiques du système d'information et des contrôles internes qui répondront aux risques cernés. Ce cadre aidera en outre les certificateurs à déterminer les critères à considérer lorsqu'ils sont appelés à fournir des services d'expression d'assurance relatifs à l'intégrité de l'information. La présente publication propose un tel cadre, articulé autour des éléments clés suivants :

- l'information et son cycle de vie;
- les caractéristiques de l'intégrité de l'information;
- les domaines du traitement de l'information;
- les risques, par domaine et par phase du cycle de vie;
- les leviers et les contrôles, par domaine et par phase du cycle de vie.

Des publications complémentaires analysent plus en profondeur les sujets suivants :

- les risques liés à l'intégrité de l'information;
- les leviers et les contrôles pouvant servir à répondre à ces risques;
- les services de certification auxquels il est possible de faire appel pour évaluer le caractère approprié de la conception des leviers et des contrôles et l'efficacité de leur fonctionnement.

Cycle de vie de l'information et cycle du traitement de l'information

L'information est créée à partir d'un contenu (les données brutes) au moyen de processus exécutés dans un environnement de système d'information (SI) dont le rôle est de rassembler et de transformer le contenu en information pouvant servir à la planification, à la prise de décisions, à la surveillance et au contrôle. Le contenu peut prendre diverses formes, telles que des données sensorielles de différents types, des données semi-traitées – structurées ou non –, des métadonnées et des paramètres employés pour produire de l'information. Globalement, le cycle de vie de l'information se divise en plusieurs phases clés :

- la création;
- l'exploitation;
- l'utilisation;
- la modification;
- l'élimination.

La collecte des données et leur transformation en information supposent les étapes suivantes :

1. la détermination des données à recueillir;
2. la collecte des données correspondant à la définition retenue;
3. l'enregistrement des données recueillies dans un fichier ou une base de données;
4. la transformation des données en information en vue de leur utilisation pour :
   a) la planification,
   b) la prise de décisions,
   c) la surveillance,
   d) le contrôle.

Les phases et sous-phases du cycle de vie de l'information et du cycle de traitement de l'information sont exposées à des risques qui doivent être gérés pour assurer l'intégrité de l'information.

Intégrité de l'information = fidélité de l'image

L'intégrité de l'information consiste en la concordance de l'information avec l'objet qu'elle prétend représenter ou dépeindre. Autrement dit, la fidélité de l'image qu'elle donne. Au cours de la crise financière de 2008, par exemple, les obligations à risque élevé jusque-là cotées AAA ont vu leur cote dégringoler de 16 crans pour se fixer à B : tout porte à croire que leur notation initiale ne présentait pas une image fidèle de la réalité[3]. La cote AAA ne concordait pas avec le risque financier réel associé aux obligations au moment de la notation.

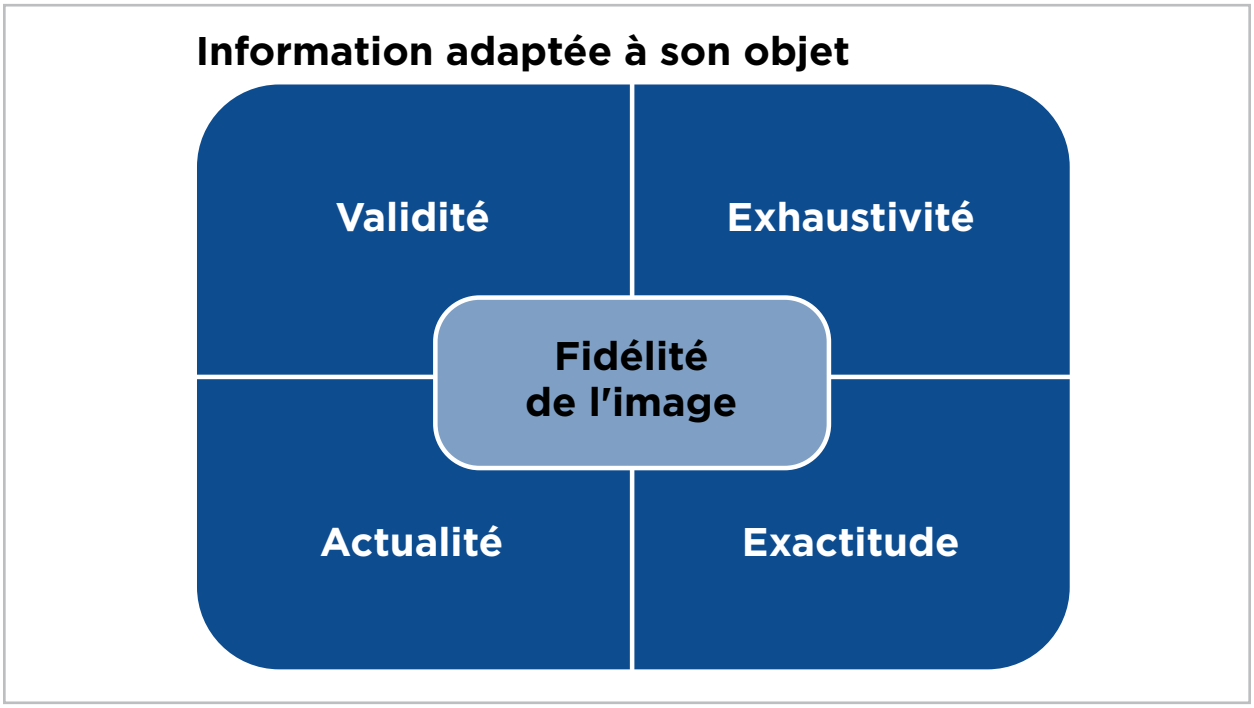
Fidélité de l'image et attributs sous-jacents

Nombre d'attributs peuvent servir à décrire la fidélité de l'image. Nous pensons cependant que les attributs les plus importants, illustrés à la figure 1 ci-après, sont la validité, l'exhaustivité, l'actualité et l'exactitude. Ces attributs sont en effet les critères essentiels au moyen desquels le degré d'intégrité de l'information peut être apprécié. L'appréciation de l'intégrité doit être effectuée en fonction de l'usage auquel l'information est destinée. Voici une définition des quatre attributs de base :

- Validité – L'information donne une image de ce qu'elle prétend dépeindre.
- Exhaustivité – L'information au fil du temps et entre les différents éléments est exhaustive.
- Actualité – L'information est présentée dans sa version la plus récente.
- Exactitude – L'information est exempte d'erreurs et suffisamment précise pour l'usage auquel elle est destinée.

3 Lowenstein, Roger, « Triple-A Failure », *New York Times*, 27 avril 2008. www.nytimes.com/2008/04/27/magazine/27Credit-t.html?pagewanted=all&_r=0

FIGURE 1 : FIDÉLITÉ DE L'IMAGE ET ATTRIBUTS SOUS-JACENTS



Le degré d'intégrité de l'information requis dépend de l'usage auquel l'information est destinée. Les usages liés à la santé et à la sécurité (par exemple, l'information sur l'efficacité d'un médicament proposé) exigent souvent un degré de fidélité très élevé, tandis que le domaine du divertissement (par exemple, le classement des films à l'affiche) peut se contenter d'un degré de fidélité plus faible.

Méta-information

La méta-information, c'est de l'information sur l'information. La méta-information procure aux utilisateurs le contexte de l'information; elle contribue ainsi à réduire le risque que l'information soit utilisée à des fins autres que celles auxquelles elle est destinée, ou encore, utilisée à des fins concordant avec l'usage prévu, mais d'une manière inappropriée. L'information doit s'accompagner de méta-information qui la décrit, ou y être liée. Les éléments de la méta-information sont notamment les suivants :

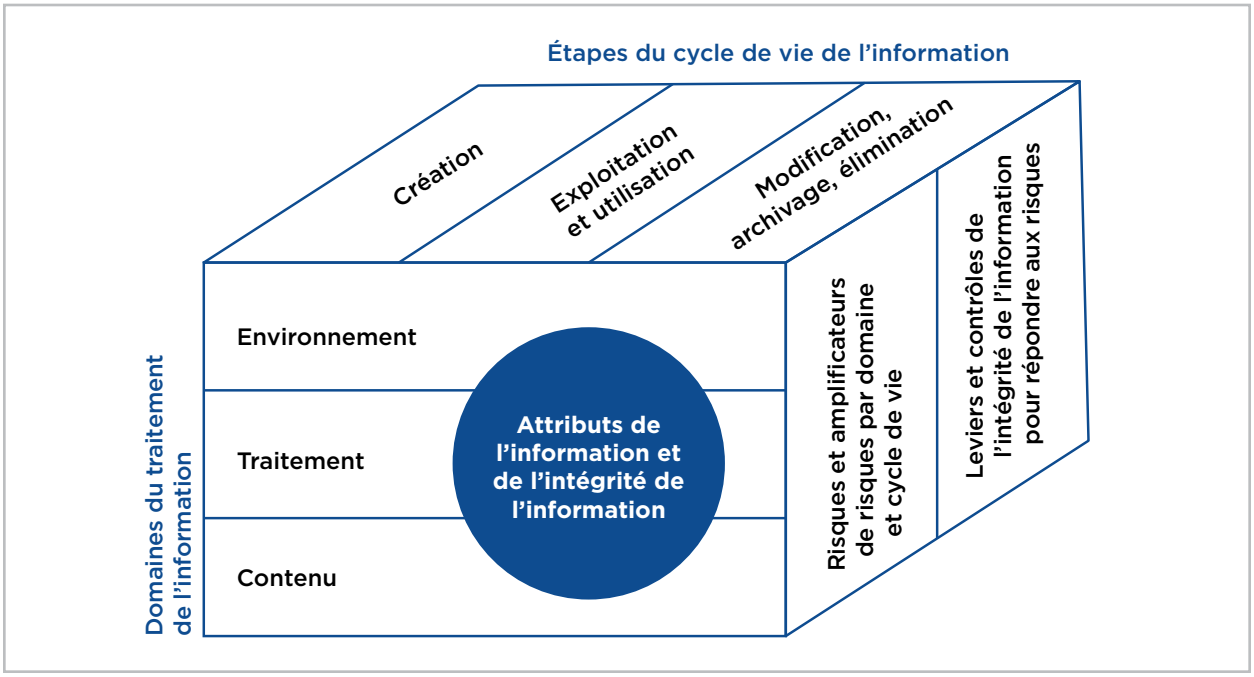
- l'usage prévu de l'information;
- sa ou ses sources;
- la méthode de compilation;
- ses composantes, leurs caractéristiques communes et les relations entre elles;
- ses limites, telles les omissions, et les périodes de temps exclues;
- l'incertitude relative à la mesure;
- d'autres facteurs pouvant jouer sur l'utilisation appropriée de l'information.

Cadre de contrôle de l'intégrité de l'information

Le cadre de contrôle de l'intégrité de l'information illustré à la figure 2 comporte plusieurs composantes :

- l'information et les attributs de son intégrité;
- le cycle de vie de l'information;
- les domaines du traitement de l'information (environnement, traitement et contenu);
- les risques et les amplificateurs de risques liés à l'intégrité de l'information;
- les leviers de l'intégrité de l'information;
- les contrôles conçus pour répondre aux risques.

FIGURE 2 : CADRE DE CONTRÔLE DE L'INTÉGRITÉ DE L'INFORMATION



Toutes les phases et les sous-phases du cycle de vie de l'information doivent être prises en compte pour pouvoir répondre aux besoins des utilisateurs. À des fins de concision, le cycle de vie de l'information est ici résumé en trois phases :

- la création;
- l'exploitation et l'utilisation;
- la modification, l'archivage ou la destruction.

Le cycle de vie de l'information commence par la reconnaissance d'un besoin à l'égard d'une information donnée. Une fois ce besoin cerné, les exigences des utilisateurs prévus et l'usage auquel l'information est destinée, de même que les exigences connexes sur le plan de l'exploitation et de la gestion, sont cernés à leur tour. Puis les conditions, événements ou occurrences d'intérêt sont déterminés ou définis, de même que leurs attributs, qui seront observés, évalués, mesurés, enregistrés et communiqués. La définition des utilisateurs et des usages prévus de l'information est essentielle pour que l'information soit adaptée à son objet.

Domaines

Comme nous l'avons vu plus haut, l'information est créée à partir d'un contenu (les données brutes) au moyen de processus exécutés dans un environnement de système d'information (SI) dont le rôle est de transformer le contenu en information. Le contenu peut prendre diverses formes, dont des données brutes ou sensorielles de différents types, des données semi-traitées – structurées ou non –, des métadonnées, ou méta-information, ainsi que des paramètres employés pour produire de l'information. Un ou plusieurs processus peuvent transformer un ensemble de données d'entrée en données de sortie et les stocker pour utilisation ultérieure à des fins de traitement ou de communication. Les processus sont exécutés dans un ou plusieurs environnements de SI dont dépend leur efficacité opérationnelle continue. Le présent cadre, qui peut servir à organiser les risques liés à l'intégrité de l'information, cerne trois domaines de traitement de l'information ayant une incidence sur l'intégrité :

1. le contenu;
2. le traitement;
3. l'environnement de SI.

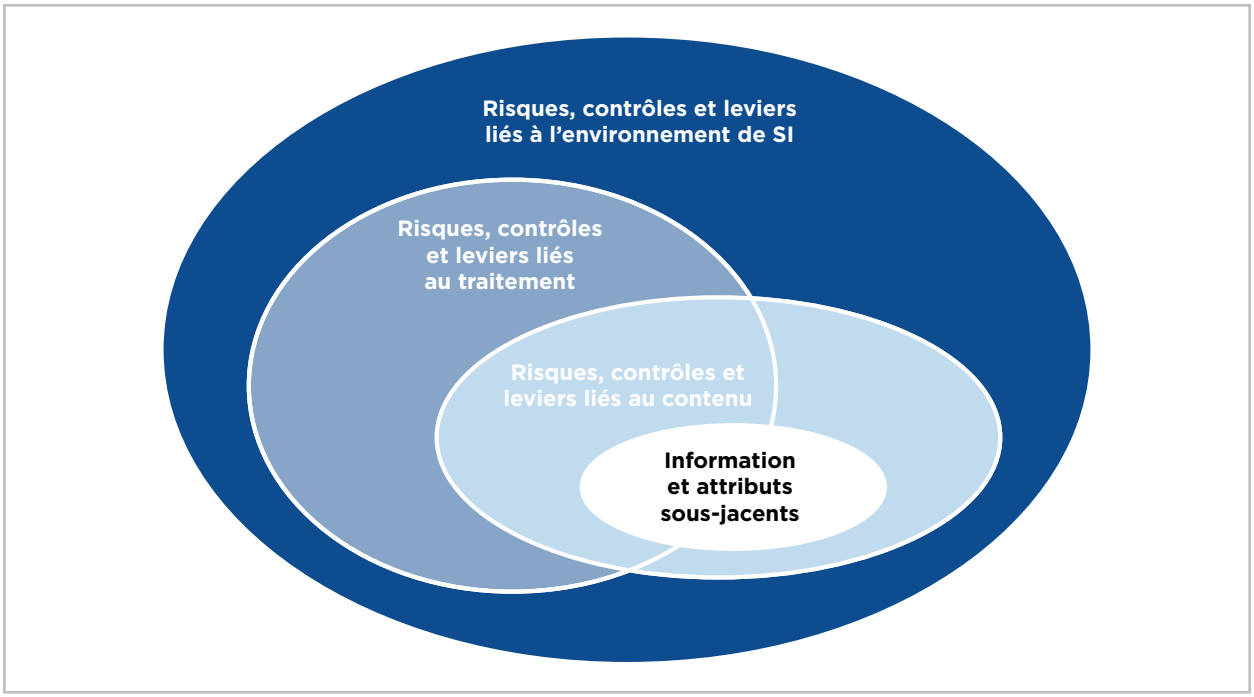
À ces trois domaines sont rattachés divers risques liés à l'intégrité de l'information, dont certains sont communs à plusieurs domaines. Ces risques doivent être atténués par des leviers et des contrôles de l'intégrité adaptés. Dans les trois domaines, les risques interviennent à toutes les phases du cycle de vie de l'information. L'ampleur des risques à chaque phase est déterminée par la présence ou l'absence d'amplificateurs clés des risques tels que la nature du système d'information, la complexité des processus liés à la collecte du contenu ou à sa transformation en information et la présence et le degré d'une intention malveillante d'atteinte à l'intégrité de l'information. Par exemple, la plupart des systèmes en ligne sont visés à un degré élevé par des intentions malveillantes de vol, de falsification, d'utilisation inappropriée ou de destruction de l'information.

Les **leviers** et les **contrôles** sont des composantes, des fonctions et des pratiques associées aux domaines que sont le contenu, le traitement et l'environnement de SI et qui contribuent à préserver l'intégrité de l'information. Certains leviers sont souvent classés parmi les contrôles; pourtant, bon nombre d'entre eux ne sont pas du tout des contrôles, mais des fonctions servant à renforcer l'intégrité de l'information (former le personnel permet à celui-ci d'effectuer efficacement son travail; utiliser des serveurs ayant une capacité excédentaire réduit les occurrences de défauts de fonctionnement, etc.).

On peut se représenter les contrôles comme un sous-ensemble de leviers dont le rôle consiste à surveiller et à vérifier si les autres leviers ont été adéquatement conçus et mis en œuvre, si leur fonctionnement est efficace et s'ils sont mis à jour au besoin. Ainsi, les contrôles permettent de surveiller les attributs de l'intégrité de l'information et les aspects du contenu, du traitement et de l'environnement de SI pour prévenir, détecter et corriger les atteintes à l'intégrité de l'information, s'en remettre et en atténuer les conséquences. Un contrôle peut par exemple permettre d'assurer la surveillance des activités d'attribution des accès au système et porter à l'attention de la direction les cas de non-respect de la politique

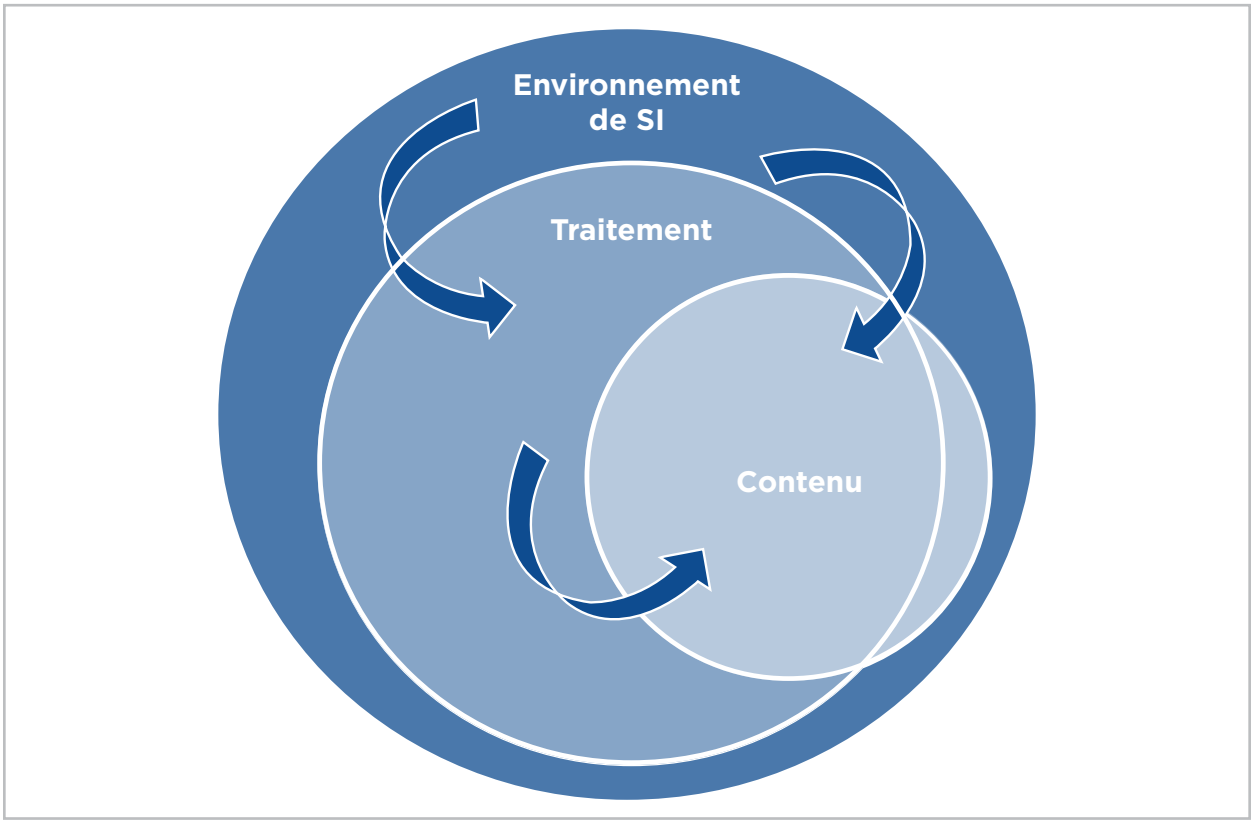
établie pour qu'une mesure corrective soit prise. En plus de corriger les procédures défaillantes, la direction pourra entreprendre une démarche pour analyser et atténuer les effets du non-respect de la politique avant sa découverte.

FIGURE 3 : DOMAINES DE L'INTÉGRITÉ DE L'INFORMATION



Les figures 3 et 4 illustrent la relation qui existe entre les domaines de l'intégrité de l'information. L'environnement de SI englobe le traitement et le contenu, tandis que le traitement englobe partiellement le contenu. Les faiblesses de l'environnement peuvent avoir une incidence défavorable sur la conception du contenu et sur la conception, le fonctionnement et l'utilisation des processus intervenant dans le domaine du traitement. Les faiblesses de conception du contenu ou de conception et de fonctionnement des processus du domaine du traitement peuvent compromettre l'intégrité du contenu. Par exemple, la réduction du budget ou de l'effectif des TI ou l'accroissement du prix des services de TI externalisés pourraient inciter les unités d'exploitation à développer des applications dans des tableurs pour répondre à leurs besoins de traitement de l'information plutôt que de passer par le service de TI centralisé. Pareille initiative risque d'entraîner une faiblesse des processus de définition, de conception, de développement et de déploiement pouvant se traduire à son tour par une atteinte à l'intégrité du contenu.

FIGURE 4 : RELATION ENTRE L'ENVIRONNEMENT DE SI, LE TRAITEMENT ET LE CONTENU



Contenu

Le **domaine du contenu** comprend les divers types de données, de métadonnées, d'information et de méta-information qui constituent l'objet dont l'intégrité de l'information présente un intérêt particulier pour l'organisation et ses décideurs. Il peut comprendre des données brutes (codes à barres), des données semi-traitées (enregistrements alphanumériques des données que les codes représentent) et des paramètres servant à contrôler le traitement et les flux d'information (entrée de table qui envoie les enregistrements à un appareil donné à un moment donné). L'information qui en découle, sous forme d'affichages, de rapports, de messages ou autres, peut être utilisée à des fins de planification, de prise de décisions, de surveillance et de contrôle. Le contenu lui-même peut être enregistré, stocké et transféré vers ou à partir de divers médias.

Les attributs de chaque condition, événement ou occurrence compris dans le contenu sont influencés par les caractéristiques de l'environnement de SI et le traitement agissant sur le contenu, qui sont susceptibles d'évoluer durant la période. Par conséquent, la compréhension des attributs suppose l'appréhension de l'évolution de l'environnement de SI et des processus au cours du cycle de vie de l'information, y compris les leviers et les contrôles connexes. Par exemple, les ventes de crème glacée dans un magasin d'alimentation donné varient en fonction de la température, des activités dans le voisinage immédiat, du nombre

de personnes dans le secteur, etc. Lors de la mise au point de l'information servant à communiquer les ventes de crème glacée à la direction et à d'autres utilisateurs, toutes ces caractéristiques de l'environnement doivent être prises en compte[4].

Certains attributs des conditions, événements et occurrences (ainsi que les caractéristiques de l'environnement) sont difficiles à observer, à évaluer ou à représenter (par exemple, les éléments d'une émission de télévision qui plaisent à l'auditoire) ou sont indéterminables (par exemple, l'intention d'un emprunteur de réaliser des travaux d'entretien sur les actifs donnés en garantie). En d'autres mots, il y a parfois des facteurs non observables qui influent sur la nature et l'interprétation d'une partie ou d'un aspect de l'information. La popularité d'un acteur faisant partie de la distribution d'une émission de télévision peut par exemple influencer la perception que le public a de cette émission et se répercuter directement sur l'audience. Si la popularité de l'acteur varie, il est possible que l'audience s'en ressente immédiatement; toutefois, il se peut que le changement ne puisse pas être mesuré ou décrit facilement. La mise au point de l'information sur l'émission de télévision doit tenir compte de l'incidence de ces attributs sur l'adaptation de l'information à son objet et de la question de savoir si l'omission de ces attributs rendrait l'information trompeuse.

Les attributs peuvent être quantifiables ou qualitatifs et peuvent être mesurables à divers degrés à différents moments du passé, du présent ou de l'avenir. Si un attribut sera mesurable dans l'avenir, certains attributs de l'événement ou occurrence en cours dépendent probablement de la survenance d'un ou de plusieurs événements futurs. Et si le caractère mesurable d'un élément dépend de la survenance d'un événement futur, cet élément peut devenir mesurable à une date certaine ou à une date incertaine. Par exemple, le nombre de retours sur ventes futurs dans un délai de 30 jours se rapporte à une période certaine, tandis que la date de recouvrement d'une créance frappée par une procédure de faillite est plus susceptible d'être incertaine.

L'objectivité ou la subjectivité d'un élément peut aussi avoir une incidence sur la facilité avec laquelle cet élément peut être mesuré. Plus l'élément est subjectif, plus il est difficile à mesurer – voire impossible, dans les cas extrêmes. Néanmoins, les clients de nombreux sites de commerce en ligne se fient aux évaluations subjectives rédigées par d'autres clients pour déterminer s'ils vont acheter ou non l'article désiré. La subjectivité d'un élément d'information n'est donc pas toujours une bonne raison d'exclure cet élément de l'information décisionnelle. Au lieu de l'exclure, il est parfois pertinent d'inclure avec l'élément subjectif de l'information descriptive sur la nature et l'ampleur de la subjectivité.

À chaque élément d'information est associée de la **méta-information**, comme les caractéristiques de l'environnement mentionnées plus haut, qui permet à l'utilisateur de comprendre et d'interpréter l'information. La méta-information s'entend de l'information sur l'information, qui précise en quoi consiste l'information. Elle contribue à la compréhension de l'information et de ses attributs en les contextualisant, assurant ainsi l'adaptation de l'information à son objet.

4 Cet exemple et plusieurs autres sont tirés du livre blanc de l'AICPA sur l'intégrité de l'information, publié en janvier 2013. L'auteur principal de la présente publication a fait partie du groupe de travail qui a publié ce livre blanc.

Par exemple, le nombre « 35 300 » employé seul est dénué de sens puisqu'on ne sait pas à quoi il se rapporte. Il peut s'agir de dollars, de kilomètres ou d'automobiles. Si le symbole « $ » y est ajouté, on sait que c'est une quantité monétaire, mais on ne sait toujours pas ce qu'il représente. Si l'étiquette « stocks » y est ajoutée, on possède déjà plus d'information, mais pas assez encore pour que cette information soit très utile. Par contre, la description « Stocks de produits finis de Jones Corporation au 31 décembre 20XY, évalués selon les IFRS au plus faible du coût et de la valeur nette de réalisation » ajoutée au montant de 35 300 $ fournit une quantité d'information raisonnable, notamment sur la propriété, la date et le mode d'évaluation.

Il se peut que les organisations et les particuliers se préoccupent surtout de l'intégrité du contenu de l'information. Toutefois, comme le montre la figure 3, l'intégrité du contenu dépend de l'efficacité des leviers et des contrôles dans les domaines du traitement et de l'environnement de SI de même que de la relation qui existe entre les deux (c'est-à-dire que les leviers et les contrôles associés aux domaines du contenu, du traitement et de l'environnement de SI devraient se compléter et se renforcer mutuellement et non entrer en conflit les uns avec les autres).

Traitement

Le **domaine du traitement** comprend les activités reliées au contenu visant à identifier, à recueillir et à enregistrer les données brutes, les données semi-traitées et les paramètres et à les transformer en information à des fins de planification, de prise de décisions, de surveillance et de contrôle. Il comprend également le stockage de l'information pour utilisation ultérieure dans de nouveaux traitements ou dans des rapports.

Le domaine du traitement se divise habituellement en plusieurs phases et sous-phases qui contribuent à l'intégrité de l'information : entrée, traitement, sortie et stockage (y compris archivage ou destruction)[5]. Le tableau 1 ci-après résume les activités, leviers et contrôles principaux du domaine du traitement, présentés par phase et sous-phase.

5 Nous faisons une distinction entre le cycle de vie de l'information, qui comprend trois phases clés (création, exploitation et utilisation, modification), et le cycle de vie du *traitement* de l'information, qui renvoie au cheminement d'un élément d'information donné à partir du moment où il est identifiable jusqu'à son archivage ou son élimination.

TABLEAU 1 : PHASES, ACTIVITÉS, LEVIERS ET CONTRÔLES DU DOMAINE DU TRAITEMENT

Phase	Activités, leviers et contrôles principaux
Entrée	• Identification ou constatation des événements ou occurrences pertinents déclenchant d'autres actions • Saisie, observation ou mesure des données • Préparation et enregistrement des données • Autres activités (voir la remarque)
Traitement	• Transformation des données d'entrée au moyen de regroupements • Exécution des calculs, des fonctions logiques et des analyses • Mises à jour des fichiers temporaires (fichiers d'attente) • Mises à jour des fichiers, tables et bases de données permanents ou semi-permanents • Autres activités (voir la remarque)
Sortie	• Affichage des données de sortie • Transmission et diffusion des données de sortie aux utilisateurs et aux autres processus • Autres activités (voir la remarque)
Stockage	• Stockage sur place et à l'extérieur • Mise à jour périodique • Archivage, anonymisation ou élimination/destruction du contenu qui ne doit pas être conservé • Autres activités (voir la remarque)

Remarque : Toutes les phases indiquées ci-dessus comprennent également les activités générales suivantes.

Début de la phase ou du processus :

- Réception des données ou de l'information en provenance d'autres phases ou processus :
  - — consignation, enregistrement ou saisie des entrées (y compris leur origine et leur destination) et des activités effectuées pendant la phase ou le processus;
  - — appariement de catégories de données avec des privilèges d'accès, et d'actions requises avec des accès et des fonctions autorisés :
    - » activités d'entrée, de traitement, de sortie et de stockage décrites dans le tableau précédent,
    - » prévention, détection et correction des erreurs; reprise après défaillance et atténuation des conséquences;
  - — attribution ou mise à jour des métadonnées.
- Transmission ou diffusion des données ou de l'information vers d'autres phases ou processus.
- Sauvegarde et restauration.
- Gestion de la maintenance et du changement de la phase ou du processus.

Fin de la phase ou du processus.

Environnement de SI

Les processus sont exécutés dans des environnements de SI dont dépend leur efficacité opérationnelle continue. Le **domaine de l'environnement de SI** regroupe les pratiques employées pour :

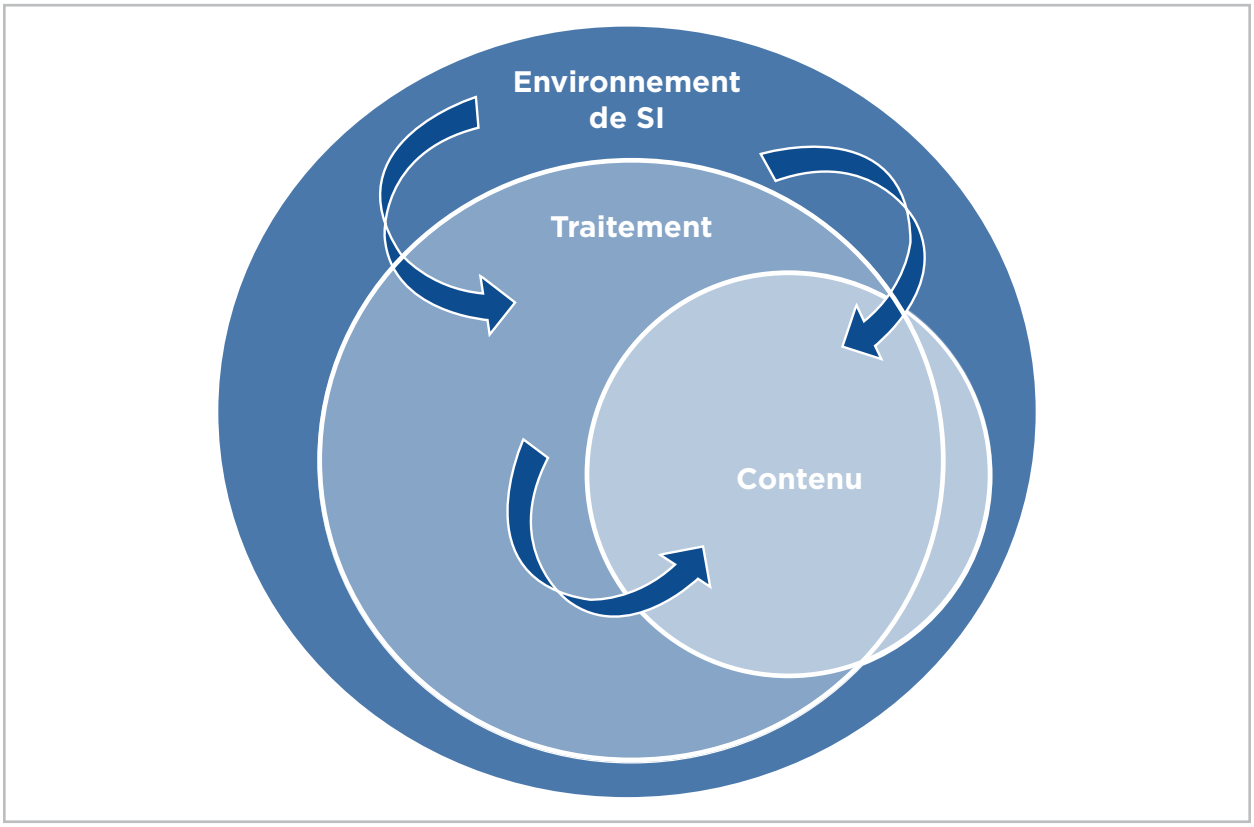
- gérer l'information à extraire et protéger la valeur stratégique qu'une information de grande qualité représente pour l'organisation;
- définir, concevoir, élaborer et mettre en œuvre des processus faisant en sorte que l'information convient aux utilisateurs ciblés et à l'usage auquel elle est destinée et que son intégrité est assurée;
- exécuter les processus en question de manière fiable et cohérente;
- s'assurer que l'information est :
  - protégée du vol, de l'altération, de l'utilisation inappropriée et de la destruction,
  - disponible et accessible pour les utilisateurs autorisés au moment où ils en ont besoin,
  - vérifiable et certifiée.

Il arrive que plus d'un environnement de SI influe sur le traitement. Bon nombre d'entités interagissent avec des clients, des fournisseurs, des partenaires d'affaires et d'autres parties capables d'accéder aux processus ou de les exécuter en leur nom. Par exemple, une entité pourrait confier l'exécution de certains de ses processus à un ou plusieurs fournisseurs. Chaque fournisseur a lui-même un ou plusieurs environnements de SI dans lesquels sont exécutés les processus, et confie peut-être à son tour une partie des traitements à d'autres fournisseurs. De même, de nombreuses entités qui se servent de l'infonuagique pourraient être exposées à des leviers et à des contrôles fonctionnant dans une chaîne de processus externalisés et dans leurs environnements de SI respectifs ainsi que dans leur propre environnement de SI.

Risques et conséquences

Dans la présente publication, l'approche préconisée est une approche fondée sur les risques qui cerne les principaux risques d'entreprise et les conséquences pouvant en découler, dans les domaines du contenu, du traitement et de l'environnement de SI au cours du cycle de vie de l'information. Comme l'illustre la figure 5, les risques liés à l'environnement de SI correspondent aux risques que les leviers et les contrôles à l'égard du système d'information et de la création, de l'exploitation et de l'utilisation de l'information, de même que l'évolution du domaine de l'environnement de SI, ne parviennent pas à protéger l'intégrité des traitements et de l'information. Les risques liés au traitement correspondent aux risques que les leviers et les contrôles à l'égard du traitement de l'information dans les domaines de l'environnement de SI et du traitement ne protègent pas l'intégrité de l'information comme il se doit. Enfin, les risques liés au contenu correspondent aux risques que les leviers et les contrôles à l'égard de l'information et de la méta-information dans les domaines de l'environnement de SI, du traitement et du contenu ne protègent pas l'intégrité de l'information.

FIGURE 5 : RELATION ENTRE LES RISQUES LIÉS À L'ENVIRONNEMENT DE SI, LES RISQUES LIÉS AU TRAITEMENT ET LES RISQUES LIÉS AU CONTENU



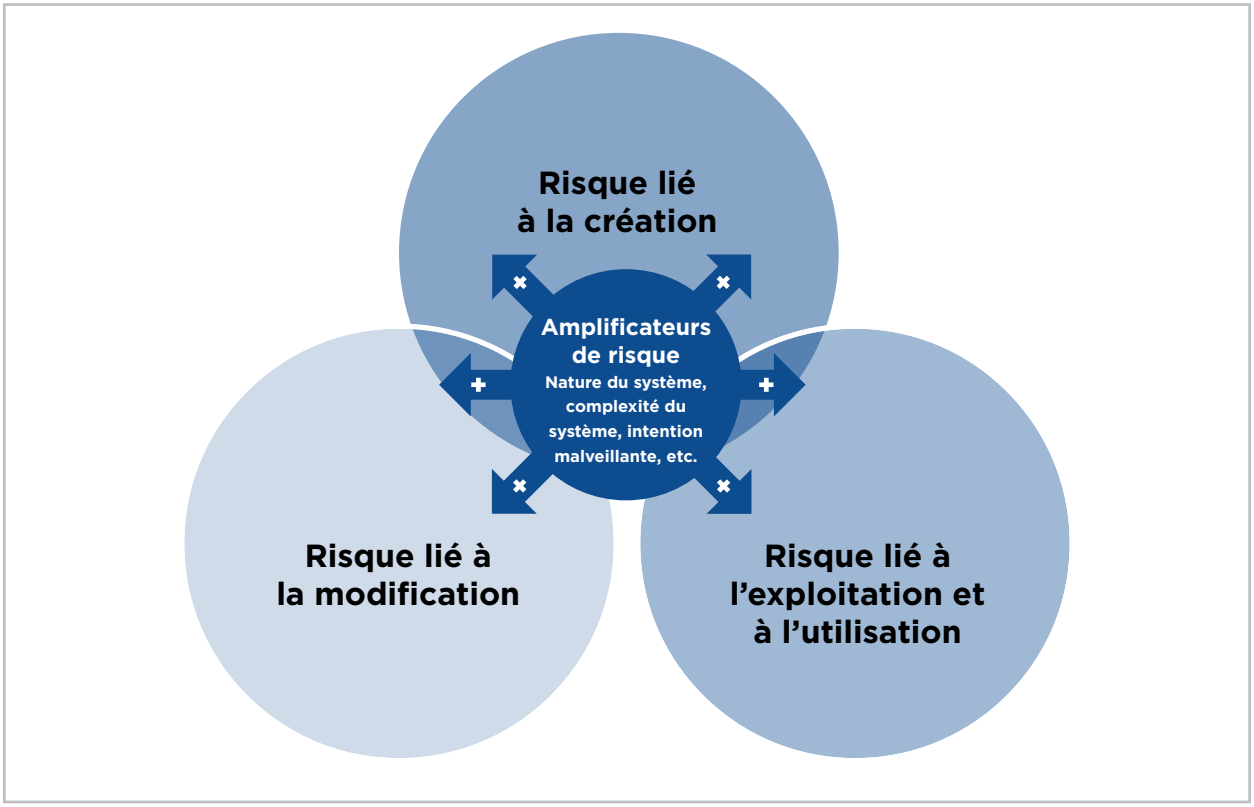
À ces trois domaines sont rattachés divers risques, dont certains sont communs à plusieurs domaines, qu'il faut atténuer par des leviers et des contrôles d'intégrité adaptés. En d'autres mots, les risques du domaine du contenu doivent être atténués par des leviers et des contrôles dans les domaines du contenu, du traitement et de l'environnement de SI. Les risques du domaine du traitement, eux, doivent être atténués par des leviers et des contrôles dans les domaines du traitement et de l'environnement de SI. Quant aux risques du domaine de l'environnement de SI, ils doivent être atténués par des leviers et des contrôles dans le seul domaine de l'environnement de SI. Ainsi, le risque qu'une personne altère de l'information sensible doit faire l'objet de mesures d'atténuation :

- au niveau du domaine de l'environnement de SI, au moyen d'une politique couvrant l'attribution des privilèges d'accès, le classement de l'information dans la catégorie « sensible » et la définition des privilèges d'accès et des droits de traitement relatifs à l'information;
- au niveau du domaine du traitement, au moyen d'un processus d'authentification des codes d'identification des utilisateurs et des privilèges d'accès pour empêcher des parties non autorisées d'accéder à l'information ou d'exécuter des fonctions non autorisées;
- au niveau du domaine du contenu, en associant à l'information des éléments de méta-information qui précisent le caractère sensible de l'information, les parties auxquelles des privilèges d'accès ont été accordés et les droits de traitement qu'elles ont obtenus.

Causes des risques d'atteinte à l'intégrité de l'information

Divers risques menacent l'intégrité de l'information durant le cycle de vie de l'information et accroissent la possibilité que des erreurs et des omissions graves dans l'information entraînent des décisions erronées ou peu judicieuses. Comme l'illustre la figure 6, les risques se classent en trois catégories correspondant aux trois phases du cycle de vie (création, exploitation et utilisation, modification). Certains facteurs, comme la nature même du système, sa complexité et les intentions malveillantes, peuvent amplifier ces risques. Une attention particulière doit y être accordée.

FIGURE 6 : CAUSES DES RISQUES D'ATTEINTE À L'INTÉGRITÉ DE L'INFORMATION



Risques liés à la création

Les risques liés à la création de l'information sont les risques d'atteinte à l'intégrité de l'information découlant d'une conception qui ne correspond pas aux besoins des utilisateurs, au fonctionnement et à l'utilisation du système d'information et de l'information elle-même, ni à l'évolution de ces derniers; ils comprennent aussi les risques inhérents aux activités effectuées tout au long des sous-phases du cycle de vie de l'information. Ils englobent les risques que les attributs ou caractéristiques de l'information à communiquer :

- donnent une image non valable de l'information voulue (ils ne représentent pas ce qu'ils sont censés représenter);
- ne soient pas à jour (mesurés trop tôt ou trop tard);
- soient partiaux, incorrects ou insuffisamment précis pour l'usage prévu;

- soient regroupés ou ventilés à un niveau inadéquat;
- soient incohérents ou non reproductibles (d'un mesureur à l'autre ou d'une mesure à l'autre) en raison de facteurs qualitatifs et de l'incertitude;
- soient incompatibles avec les normes ou d'autres sources.

Une définition inadéquate des exigences en matière de contenu, de traitement et d'environnement de SI peut dresser des obstacles insurmontables à l'intégrité de l'information :

- Une compréhension incomplète ou erronée des besoins et exigences des utilisateurs et autres parties prenantes ainsi que l'omission de faire participer les bonnes personnes au processus de détermination des besoins peuvent engendrer des risques liés à la définition.
- Les risques liés à la conception du contenu, du traitement et de l'environnement de SI peuvent naître de l'adoption d'une méthode de conception inappropriée, de l'omission de faire participer les bonnes personnes au processus de conception et des limites inhérentes au jugement humain pouvant faire en sorte que la conception ne réponde pas tout à fait aux besoins, favorisant ainsi les atteintes à l'intégrité de l'information.
- Les risques liés au développement et au déploiement du contenu, du traitement et de l'environnement de SI peuvent résulter de l'adoption d'une méthode inappropriée d'acquisition, de développement et de déploiement des systèmes et de l'information, de l'omission de faire participer les bonnes personnes au processus de développement et de déploiement, de l'insuffisance des tests, ainsi que de problèmes organisationnels pouvant nuire à la qualité des résultats et favoriser les atteintes à l'intégrité de l'information.

Risques liés au fonctionnement et à l'utilisation

Le fonctionnement des systèmes de même que la production et l'utilisation de l'information exposent les environnements de SI, le traitement et le contenu à divers risques susceptibles de porter atteinte à l'intégrité de l'information : erreur, défaut de fonctionnement, attaque malveillante et exploitation de vulnérabilités connues ou de failles imprévues de la conception du contenu, des processus et des systèmes d'information, et entropie (tendance naturelle de toute chose à se détériorer au fil du temps).

Le risque lié à l'utilisation est le risque que l'information ou la méta-information soit utilisée à d'autres fins que celles auxquelles elle est destinée, utilisée de manière incorrecte, ou non utilisée alors qu'elle le devrait. Il peut en résulter une décision ou un jugement mal éclairé ou erroné. Voici des exemples d'utilisation inappropriée de l'information :

- le choix d'une information inappropriée ou l'omission d'une information appropriée aux fins de la prise de décisions;
- le remplacement inapproprié d'une information disponible par une information non disponible;
- la projection inappropriée d'une information à d'autres événements ou occurrences;
- la combinaison, la transformation ou la synthèse inappropriées de l'information;
- des incohérences dans le processus décisionnel d'un utilisateur et d'un utilisateur à l'autre;
- des incohérences ou malentendus entre l'intention du fournisseur de l'information et celle de l'utilisateur.

Tous ces risques liés à l'utilisation peuvent être le résultat d'une mauvaise interprétation ou d'une application incorrecte, par l'utilisateur cible ou une autre personne, de l'information ou de la méta-information, ou encore du manque d'intégrité de l'information. Une mauvaise interprétation ou une application incorrecte de l'information pourrait survenir si l'information ou la méta-information fournies ne conviennent pas à l'usage voulu, ne sont pas actuelles, sont incomplètes, contiennent des erreurs ou sont autrement trompeuses. Une application incorrecte de la méta-information pourrait par exemple se produire si une importance exagérée est accordée à l'information fournie dans le cadre du processus décisionnel, ou encore si l'information n'est pas accompagnée de tous les éléments de méta-information nécessaires à l'utilisation prévue ou n'est pas bien comprise par l'utilisateur (par exemple, l'utilisation d'une information rédigée en allemand par une personne qui ne possède pas bien cette langue).

Il est possible de réduire les risques de mauvaise interprétation ou d'application incorrecte de l'information en fournissant l'information dans un format dont les utilisateurs visés peuvent se servir et en y rattachant des éléments de méta-information (une description) qui précisent l'utilisateur cible et l'usage auquel l'information est destinée, la méthode de compilation de l'information (les éléments inclus et exclus) et les limitations qu'elle comporte.

Risques liés à la modification

Lorsqu'il se produit des changements dans l'organisation, les pratiques, le personnel, les infrastructures et les logiciels d'une entité, celle-ci est exposée à des risques accrus :

- de détérioration de ses environnements de SI et de ses processus de traitement;
- de contournement des contrôles mis en place;
- d'ajouts ou de modifications non autorisés ou non testés;
- de non-pertinence du contenu actuel et de la nécessité de sa mise à jour, de son archivage ou de sa destruction.

Tous ces risques peuvent porter atteinte à l'intégrité de l'information. Pour les atténuer, l'utilisation coordonnée de leviers et de contrôles de l'intégrité de l'information est indiquée.

Leviers de l'intégrité de l'information

Les leviers et les contrôles peuvent s'avérer efficaces pour répondre à certains risques, tandis que dans d'autres cas, il peut être nécessaire de recourir à d'autres stratégies d'atténuation des risques, tel l'évitement. Les leviers de l'intégrité de l'information comprennent des leviers et des contrôles s'appliquant aux domaines du contenu, du traitement et de l'environnement de SI. Ils regroupent des politiques, des procédures et des techniques visant le renforcement de l'intégrité de l'information.

Les leviers appartenant au domaine du contenu comprennent le type de contenu, le type de média, le contenu des métadonnées, la création de métadonnées, ainsi que les processus de gestion de l'utilisation et des changements. Un bon exemple de levier de cette catégorie est l'intégration d'attributs dans l'information (données sources, codes uniques d'identification des transactions, estampilles temporelles et autres données) qui permettent aux utilisateurs, à la direction et aux auditeurs internes et externes de vérifier l'intégrité de l'information dans la base de données d'une organisation.

Les leviers du domaine du traitement comprennent les activités constituant le cycle du traitement de l'information (entrée, traitement, sortie et stockage) ainsi que les mécanismes de ces quatre phases du cycle qui contribuent à l'intégrité de l'information. Une table contenant les codes d'identification de tous les utilisateurs autorisés d'une base de données, qui peut être consultée avant l'octroi à un utilisateur d'une permission d'accès ou de modification, est un exemple de levier de cette catégorie.

Les leviers appartenant au domaine de l'environnement de SI comprennent les pratiques de gouvernance en matière d'information, les pratiques de conception de l'information visant à adapter l'information à son objet, les pratiques de sécurité visant à protéger l'information contre la création, la modification, l'utilisation ou la destruction non autorisées, les pratiques relatives à la disponibilité visant à rendre l'information disponible et accessible pour les utilisateurs autorisés, ainsi que les pratiques opérationnelles servant à assurer la fiabilité des activités et la cohérence de la production d'information. Un bon exemple de levier de cette catégorie est un plan antisinistre global protégeant l'entité contre la perte d'information par suite de menaces, intentionnelles ou non.

Contrôles

L'information, c'est du contenu qui a été traité; c'est pourquoi la fiabilité des processus de transformation du contenu en information doit faire partie du cadre de contrôle de l'intégrité de l'information. De même, comme le traitement a lieu dans un environnement de SI, la fiabilité de cet environnement de SI doit aussi faire partie du cadre de contrôle. On peut se représenter les contrôles comme un sous-ensemble de leviers tactiques. Leur rôle consiste à surveiller et à vérifier si les autres leviers ont été correctement conçus et mis en œuvre, si leur fonctionnement est efficace et s'ils sont mis à jour au besoin pour prévenir, détecter et corriger toute atteinte à l'intégrité de l'information, permettre la reprise des activités après une telle atteinte et en atténuer les conséquences. Autrement dit, les leviers sont des mécanismes intégrés au contenu, au traitement et à l'environnement de SI qui contribuent à l'intégrité de l'information, tandis que les contrôles sont des processus de vérification et des services de certification qui surveillent ces mécanismes et s'assurent de leur efficacité.

Un contrôle qui vérifie que les attributs du contenu sont passés en revue et approuvés par un employé autorisé avant l'enregistrement des données ou des éléments d'information dans une base de données de l'organisation constitue un exemple de contrôle du domaine du contenu. Un contrôle qui vérifie que l'identité de l'utilisateur a été validée avant que l'utilisateur ait la permission d'accéder à l'information d'une base de données ou de la modifier est un exemple de contrôle appartenant au domaine du traitement. Un processus de mise à l'essai périodique et d'examen de l'efficacité du plan antisinistre global protégeant l'entité contre la perte d'information par suite de menaces, intentionnelles ou non, est un exemple de contrôle du domaine de l'environnement de SI.

Relation entre les attributs, les risques, les leviers et les contrôles de l'intégrité de l'information

Les attributs fondamentaux de la fidélité de l'image sont les critères minimaux qui doivent être satisfaits à un degré acceptable pour qu'un élément ou un ensemble d'éléments d'information soit considéré comme inaltéré. C'est dire que tous ces attributs sont nécessaires, mais qu'aucun pris isolément n'est suffisant pour que l'on conclue à l'intégrité de l'information. Voici des exemples de cas où l'image donnée par l'information n'est pas fidèle : un chiffre de ventes mensuel, par ailleurs juste, mais dans lequel les ventes d'une journée ne sont pas prises en compte (information non exhaustive); un tableau des prix d'un supermarché qui n'a pas été mis à jour en fonction des prix de vente annoncés de la semaine (information non actuelle); un classement chronologique des créances dans lequel certaines dates sont erronées (information inexacte); une liste de fournisseurs comprenant des fournisseurs fictifs (information non valide).

Étant donné les limitations inhérentes aux systèmes de traitement de l'information et aux personnes qui les conçoivent et les mettent en œuvre, il est impossible d'atteindre la perfection en matière d'exhaustivité, d'actualité, d'exactitude et de validité. Les limites des leviers et des contrôles impliquent que la fidélité de l'image est sujette à un certain degré d'imperfection; quant au degré d'imperfection tolérable (seuil de signification), il sera différent selon les domaines et les contextes.

Une évaluation de l'efficacité des leviers et des contrôles peut aider les décideurs à apprécier le degré de fidélité de l'image donnée par un élément ou un ensemble d'éléments d'information, pour que des mesures correctives puissent être prises au besoin afin de ramener l'intégrité de l'information à un degré acceptable ou de réduire la mesure dans laquelle on s'appuie sur cette information.

Le cadre présenté dans la présente publication devrait constituer un outil précieux pour les organisations qui ont besoin d'indications sur l'intégrité de l'information. On trouvera, dans des publications complémentaires, des analyses plus détaillées des risques liés à l'intégrité de l'information, des leviers et des contrôles pouvant être utilisés pour répondre à ces risques et des services de certification auxquels il est possible de faire appel pour évaluer l'adéquation de la conception des leviers et des contrôles et l'efficacité de leur fonctionnement.

Définitions

Certains termes clés ont un sens particulier dans la présente publication. Ces termes sont définis ci-dessous.

Activité d'aval : utilisation ultérieure d'une **information** actuelle (voir aussi **Activités d'amont**).

Activités d'amont : création ou traitement préalable d'une information actuelle (voir aussi **Activité d'aval**).

Activités d'information : composantes ou tâches individuelles qui se regroupent pour former un processus (voir **Processus**).

Actualité : caractéristique de l'information évaluée en fonction de la période de temps ou de la date limite de l'**information** par rapport à son objet et au moment où elle est utilisée.

Amplificateur de risque : facteur qui aggrave un risque (complexité, nature, intention malveillante, etc.).

Certification de l'information : information supplémentaire ou **méta-information** rattachée à l'objet considéré et servant à accroître la confiance d'un utilisateur dans l'intégrité de cet objet.

Complexité : présence d'un grand nombre ou d'une grande variété de composantes en interaction.

Compréhensibilité (de l'information) : degré approprié de détail ou de regroupement, d'appellation et d'**information** contextuelle pour les fins prévues.

Contenu : données de tous types utilisées pour générer de l'**information** : **données brutes**, données sensorielles, **données** semi-traitées, **métadonnées** et paramètres.

Contrôle : mécanisme ou activité visant à surveiller et à vérifier des éléments du contenu, du traitement ou de l'environnement de SI en fonction de critères précisés pour prévenir, détecter et corriger toute atteinte à l'**intégrité de l'information**. On peut se représenter les contrôles comme un sous-ensemble de leviers tactiques dont le rôle consiste à surveiller et à vérifier si les autres leviers ont été correctement conçus et mis en œuvre, si leur fonctionnement est efficace et s'ils sont mis à jour au besoin.

Création : une des trois phases clés du cycle de vie des systèmes (les autres étant **l'exploitation et l'utilisation** et **la modification**) servant à organiser les risques dans la présente publication, qui englobe des activités telles que la définition, la conception, l'acquisition, le développement et le déploiement.

Cycle de vie de l'information : processus allant de la spécification de l'**information** jusqu'à son élimination par archivage ou destruction. Dans la présente publication, le cycle de vie se divise en trois phases : la création; l'exploitation et l'utilisation; et la modification, qui comprend l'élimination, l'archivage permanent, l'anonymisation et la destruction.

Cycle du traitement de l'information : partie du **cycle de vie de l'information** qui comprend les phases suivantes :

a) entrée – création ou identification de **données**, observation ou mesure, documentation ou enregistrement;
b) traitement – analyse, calcul, transformation ou regroupement (servant à transformer les données en information);
c) stockage ou archivage;
d) mise à jour périodique;
e) affichage des données de sortie, transmission et diffusion;
f) utilisation;
g) archivage, anonymisation ou destruction.

Données : ensemble enregistré de mesures qualitatives et quantitatives des caractéristiques ou attributs d'événements ou d'occurrences. Les données se présentent en divers formats : caractères alphanumériques structurés, texte non structuré, enregistrement audio ou images (voir **Données brutes**).

Données brutes : données qui, pour être utiles, doivent être soumises à un traitement (voir **Information**).

Environnement de SI : ensemble des éléments de l'infrastructure organisationnelle sous-jacente sur lesquels repose le domaine du traitement, y compris les politiques, les normes, les procédures et les services de TI.

Événement : catégorie d'occurrences que doit saisir un système de règles.

Exactitude : ensemble de notions telles que la véracité et la précision d'un calcul, d'une mesure ou d'une estimation de même que la cohérence d'un traitement dans le temps et d'un élément d'information à l'autre.

Exhaustivité : caractère exhaustif du traitement de l'information, qui couvre toutes les périodes, toutes les données et tous les attributs des données requis pour que l'information soit adaptée à son objet, ainsi que les **métadonnées** et les éléments d'**information contextuelle** nécessaires à la compréhension de l'**information**.

Exploitation et utilisation : une des trois phases du **cycle de vie de l'information** et des systèmes (les autres étant **la création** et **la modification**). Activité supposant l'utilisation de contenus, d'**information** ou de systèmes.

Fidélité de l'image (donnée par l'information) : description correspondant aux phénomènes réels (ou conformité de l'**information** à l'élément auquel elle correspond). Selon le Financial Accounting Standards Board® (FASB), pour qu'une image soit considérée comme parfaitement fidèle, il faut qu'elle soit exhaustive, neutre et exempte d'erreurs[6]. Dans la présente publication, la fidélité de l'image donnée par l'**information** est établie en fonction de l'exhaustivité, de l'actualité, de l'exactitude et de la validité. Ces caractéristiques doivent être appréciées dans le contexte de l'usage prévu ou réel de l'**information** (voir **Intégrité du traitement**).

Gouvernance de l'information : politiques, normes, procédures et autres mécanismes mis en place par le conseil d'administration et la haute direction pour faire de l'**intégrité de l'information** une priorité au sein de l'organisation.

Information : données présentées à un utilisateur dans un contexte significatif et dans un but donné (voir **Données** et **Données brutes**).

Information adaptée à son objet : information pertinente pour son usage réel ou prévu, applicable, claire, compréhensible, et présentée selon un degré approprié de granularité ou de regroupement.

Information contextuelle : voir **Méta-information**.

Information sur l'objet considéré : information et **méta-information** dépeignant un objet ou un objet considéré en se fondant sur l'observation, l'évaluation, la mesure et la représentation de l'objet considéré par rapport à des critères[7].

Intégrité de l'information : fidélité de l'image que l'**information** donne de la condition ou de l'objet qu'elle représente.

Intégrité du traitement : exhaustivité, rapidité, exactitude et validité du traitement par un système compte tenu du but ou de l'objet du système et des besoins de ses utilisateurs cibles (voir **Intégrité de l'information**).

Levier : composante, mécanisme ou pratique associé au domaine du contenu, du traitement ou de l'environnement de SI qui contribue à l'**intégrité de l'information**.

Menace (contre l'intégrité de l'information) : indice d'un danger provenant de sources internes et externes, susceptible de venir des personnes, de la technologie ou de l'environnement et pouvant naître d'actions intentionnelles ou non (voir **Risque**).

6 FASB (septembre 2010). *Conceptual Framework for Financial Reporting: Objective of Financial Reporting and Qualitative Characteristics of Decision-Useful Financial Reporting Information*.

7 Adapté du *Handbook of International Quality Control, Auditing, Review, Other Assurance, and Related Services Pronouncements*, vol. 1, publié par le Conseil des normes internationales d'audit et d'assurance (International Auditing and Assurance Standards Board - IAASB) (2012).

Métadonnées : données décrivant le contenu, le contexte et la structure des **données brutes** avant leur transformation en **information** (description, objet, origine, utilisateur, propriété, responsabilité, norme, classement aux fins de la sécurité et de la confidentialité, privilèges d'accès, emplacement, version, estampille temporelle, exigence en matière de conservation et d'élimination, piste d'audit, certification) (voir **Méta-information** et **Données brutes**).

Méta-information : données permettant aux systèmes de traitement de l'information d'assurer l'intégrité de l'information au cours du traitement et aux utilisateurs de comprendre et d'utiliser l'information de manière appropriée; contexte permettant la compréhension des données traitées (voir **Métadonnées**).

Modification : une des trois phases du **cycle de vie de l'information** et des systèmes (les autres phases étant **la création** et **l'exploitation et l'utilisation**) servant à organiser les risques dans la présente publication. Elle comprend le remplacement d'un élément organisationnel, d'une pratique, d'une infrastructure ou d'un logiciel préexistant par une version révisée. La modification comprend également le départ ou le remplacement de membres du personnel ou l'archivage et la destruction d'éléments d'information.

Objet ou **objet considéré :** ensemble de phénomènes (conditions, événements ou occurrences) à propos desquels sont fournies l'**information** et la **méta-information** qui l'accompagne.

Occurrence d'événement : occurrence réelle et particulière d'un type d'événement devant être saisi.

Pertinence (de l'information) : applicabilité de l'**information** à l'usage pour lequel elle a été créée; capacité de l'**information** à influer sur les décisions que l'utilisateur prendra en s'appuyant sur cette information.

Processus : ensemble des activités servant à transformer un groupe de données d'entrée (c'est-à-dire de **données brutes** ou d'autres éléments appartenant au domaine du contenu) en données de sortie et à les stocker pour utilisation ultérieure à des fins de traitement ou de communication.

Qualité de l'information : appellation donnée aux attributs souhaitables de l'**information** (pertinence[8], utilité et **fidélité de l'image**[9]).

Qualité des données : appellation donnée à diverses notions décrivant les attributs souhaitables des données (pertinence, utilité, intégrité). À tout le moins, le degré d'exhaustivité et d'exactitude des données valides recueillies et traitées en vue d'un usage particulier.

8 Selon le FASB (2010), une information financière est pertinente si elle a la capacité d'influencer les décisions prises par les utilisateurs. L'information peut avoir la capacité d'influencer les décisions même si certains utilisateurs choisissent de ne pas s'en servir ou la connaissent déjà parce qu'ils ont consulté d'autres sources. L'information financière a la capacité d'influencer les décisions si elle a une valeur prédictive, une valeur de confirmation ou les deux.

9 Le COSO (2013) énonce les critères de qualité de l'information suivants : rapidité, actualité, exactitude, exhaustivité, accessibilité, protection, vérifiabilité et conservation.

Rapidité : se dit de l'**information** qui est accessible à temps pour être utilisée aux fins prévues.

Risque (d'atteinte à l'intégrité de l'information) : facteur susceptible de compromettre ou de menacer un ou plusieurs des attributs fondamentaux de l'**intégrité de l'information**. Un risque peut naître d'actions intentionnellement malveillantes ou d'erreurs involontaires. Les risques peuvent être regroupés selon les trois phases du **cycle de vie de l'information** et des systèmes, à savoir la création, l'exploitation et l'utilisation, et la modification.

Utilité ou facilité d'utilisation (de l'information) : compréhensibilité, pertinence et intégrité suffisantes pour l'usage auquel l'**information** est destinée.

Validité : se dit de l'**information** qui représente ce qu'elle est censée représenter. Une information valide résulte de traitements autorisés et est conforme aux politiques et aux textes légaux et réglementaires; elle est authentique et formatée correctement; elle peut être suivie de sa source (ou de ses sources) jusqu'à sa destination ultime; elle est vérifiable et impartiale.

Références

AICPA (2013). *Information Integrity*. Livre blanc (janvier). AICPA.

Boritz, J. E. (2004). *Managing Enterprise Information Integrity: Security, Control and Audit Issues.* IT Governance Institute.

Boritz, J. E. (2005). « IS Practitioners' Views on Core Concepts of Information Integrity ». *International Journal of Accounting Information Systems*, vol. 6, 20 pages.

COSO (2013). *Internal Control – Integrated Framework.* Committee of Sponsoring Organizations de la Treadway Commission. COSO.

Financial Accounting Standards Board® (FASB) (2010). Concepts Statement No. 8, Conceptual Framework for Financial Reporting, chapitre 3, « Qualitative Characteristics of Useful Financial Information ». FASB.

ICCA (1998). *La gestion du contrôle de l'informatique*, 3e édition. ICCA.

ISACA (2012). COBIT (Objectifs de contrôle de l'Information et des technologies associées) 5 Cadre de référence. ISACA.

ISO (2001) 15489-1. Information et documentation – « Records management » – Partie 1 : Principes directeurs. ISO.

Neely, M. P. et Cook, J. S. (2011). « Fifteen Years of Data and Information Quality Literature: Developing a Research Agenda for Accounting ». *Journal of Information Systems*, vol. 25, n° 1 (printemps), p. 79 à 108.

Wang, R. Y. et Strong, D. M. (1996). « Beyond accuracy: What data quality means to data consumers ». *Journal of Management Information Systems*, vol. 12, n° 4, p. 5 à 34.

CPA
COMPTABLES
PROFESSIONNELS
AGRÉÉS
CANADA

277, RUE WELLINGTON OUEST
TORONTO (ONTARIO) CANADA M5V 3H2
TÉL. : 416 977.3222 TÉLÉC. : 416 977.8585
WWW.CPACANADA.CA