SPÉCIFICATION TECHNIQUE

ISO/TS 22317

Deuxième édition
2021-11

Sécurité et résilience — Systèmes de management de la continuité d'activité — Lignes directrices pour le bilan d'impact sur l'activité

Security and resilience — Business continuity management systems — Guidelines for business impact analysis

Numéro de référence
ISO/TS 22317:2021(F)

ISO copyright office
Case postale 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Genève
Tél.: +41 22 749 01 11
E-mail: copyright@iso.org
Web: www.iso.org

Publié en Suisse

Sommaire

Page

Avant-propos ..... **iv**
Introduction ..... **vi**
1 Domaine d'application **1**
2 Références normatives **1**
3 Termes et définitions **1**
4 Conditions préalables **1**
4.1 Généralités 1
4.2 Contexte et domaine d'application 2
4.2.1 Contexte 2
4.2.2 Domaine d'application 2
4.3 Rôles et responsabilités 2
4.3.1 Généralités 2
4.3.2 Pilote du BIA 2
4.3.3 Propriétaires d'activité 3
4.4 Engagement 3
5 Le processus de BIA **3**
5.1 Fondamentaux 3
5.2 Planifier le BIA 4
5.3 Convenir de l'approche pour engager le processus de BIA 4
5.3.1 Comprendre les impacts 4
5.3.2 Définir les types d'impacts et les critères 5
5.3.3 Définir les délais 7
5.3.4 Définir une méthodologie 8
5.4 Déterminer les priorités attribuées aux produits et services avec la direction générale 8
5.4.1 Vue d'ensemble 8
5.4.2 Données d'entrée 9
5.4.3 Détermination des priorités pour les produits et services 9
5.4.4 Aboutissements 9
5.5 Déterminer les activités prioritaires 9
5.5.1 Vue d'ensemble 9
5.5.2 Données d'entrée 10
5.5.3 Identifier les activités 10
5.5.4 Établir les RTO des activités 10
5.5.5 Définir les activités prioritaires 10
5.5.6 Résultats 10
5.6 Identifier les ressources et les autres dépendances 11
5.6.1 Identifier les exigences en matière de ressources et autres dépendances 11
5.6.2 Exigences en termes de ressources 11
5.7 Analyser et consolider les résultats du BIA 12
5.8 Obtenir l'approbation de la direction générale pour les résultats du BIA 13
6 Passer en revue le BIA **13**
6.1 Passer en revue le processus et la méthodologie de BIA 13
6.2 Passer en revue les résultats du BIA 13
Annexe A (informative) **Le BIA au sein du SMCA de l'ISO 22301:2019** **15**
Annexe B (informative) **Méthodes de collecte des informations relatives au BIA** **16**
Annexe C (informative) **Autres utilisations du processus de BIA** **23**
Annexe D (informative) **Exemples de réalisation de BIA** **26**
Bibliographie **37**

Avant-propos

L'ISO (Organisation internationale de normalisation) est une fédération mondiale d'organismes nationaux de normalisation (comités membres de l'ISO). L'élaboration des Normes internationales est en général confiée aux comités techniques de l'ISO. Chaque comité membre intéressé par une étude a le droit de faire partie du comité technique créé à cet effet. Les organisations internationales, gouvernementales et non gouvernementales, en liaison avec l'ISO participent également aux travaux. L'ISO collabore étroitement avec la Commission électrotechnique internationale (IEC) en ce qui concerne la normalisation électrotechnique.

Les procédures utilisées pour élaborer le présent document et celles destinées à sa mise à jour sont décrites dans les Directives ISO/IEC, Partie 1. Il convient, en particulier, de prendre note des différents critères d'approbation requis pour les différents types de documents ISO. Le présent document a été rédigé conformément aux règles de rédaction données dans les Directives ISO/IEC, Partie 2 (voir www.iso.org/directives).

L'attention est attirée sur le fait que certains des éléments du présent document peuvent faire l'objet de droits de propriété intellectuelle ou de droits analogues. L'ISO ne saurait être tenue pour responsable de ne pas avoir identifié de tels droits de propriété et averti de leur existence. Les détails concernant les références aux droits de propriété intellectuelle ou autres droits analogues identifiés lors de l'élaboration du document sont indiqués dans l'Introduction et/ou dans la liste des déclarations de brevets reçues par l'ISO (voir www.iso.org/brevets).

Les appellations commerciales éventuellement mentionnées dans le présent document sont données pour information, par souci de commodité, à l'intention des utilisateurs et ne sauraient constituer un engagement.

Pour une explication de la nature volontaire des normes, la signification des termes et expressions spécifiques de l'ISO liés à l'évaluation de la conformité, ou pour toute information au sujet de l'adhésion de l'ISO aux principes de l'Organisation mondiale du commerce (OMC) concernant les obstacles techniques au commerce (OTC), voir www.iso.org/avant-propos.

Le présent document a été élaboré par le comité technique ISO/TC 292, *Sécurité et résilience*.

Cette deuxième édition annule et remplace la première édition (ISO/TS 22317:2015), qui a fait l'objet d'une révision technique. Les principales modifications sont les suivantes:

— le document a été mis à jour pour être aligné sur l'ISO 22301:2019;

— la structure du document a été mise à jour afin d'améliorer la description du processus relatif au bilan d'impact sur l'activité (BIA);

— l'accent a été davantage mis sur le processus relatif au BIA et moins sur le programme de continuité d'activité;

— le BIA et le processus de BIA ont été clairement différenciés;

— les rôles relatifs au processus du BIA ont été consolidés au niveau du pilote du BIA et des propriétaires d'activité;

— le paragraphe «Considérations initiales relatives au BIA» a été retiré et les lignes directrices redistribuées;

— le paragraphe «Sélectionner la stratégie» a été retiré, car il fait partie de l'ISO/TS 22331;

— l'annexe sur la terminologie a été retirée;

— l'annexe sur les méthodes de collecte des informations du BIA a été améliorée;

— une nouvelle annexe accompagnée d'exemples de réalisation de BIA a été incluse.

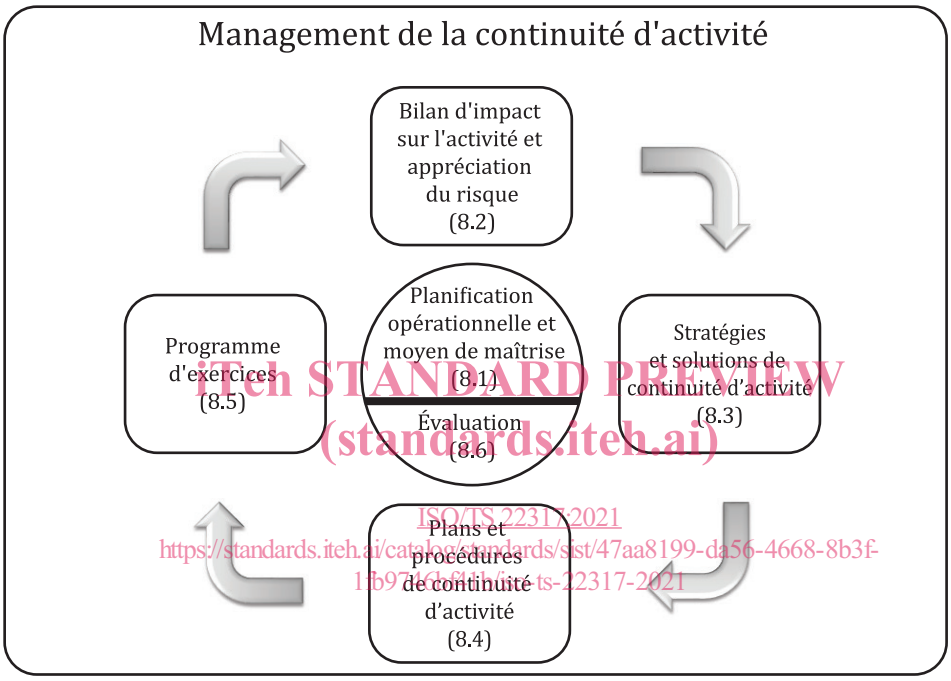
Il convient que l'utilisateur adresse tout retour d'information ou toute question concernant le présent document à l'organisme national de normalisation de son pays. Une liste exhaustive desdits organismes se trouve à l'adresse www.iso.org/fr/members.html.

Introduction

Le présent document fournit des lignes directrices détaillées pour la mise en œuvre et le maintien d'un processus de bilan d'impact sur l'activité (BIA) qui soit cohérent avec l'ISO 22301. Ce document est applicable à la réalisation de tout processus de BIA.

La terminologie utilisée est cohérente avec l'ISO 22300 et l'ISO 22301, mais un organisme peut utiliser des termes différents à condition qu'ils soient clairement compris.

La Figure 1 montre la relation entre le processus de BIA et le système de management de la continuité d'activité (SMCA) dans son ensemble. Il convient que l'organisme réalise un cycle complet de processus de BIA avant de sélectionner les stratégies et solutions de continuité d'activité.



NOTE Source: ISO 22313:2020, Figure 5.

Figure 1 — Éléments de management de la continuité d'activité

Le processus de BIA analyse les effets d'une perturbation sur un organisme. L'aboutissement est un inventaire des priorités et des exigences relatives à la continuité d'activité et leur justification.

La première étape d'un BIA est la priorisation des produits et services, suivie par un certain nombre de BIA de processus (en option) et de BIA d'activités. Le domaine d'application de chacun de ces BIA peut être limité, mais il convient qu'ils couvrent ensemble la totalité du domaine d'application du SMCA. Il convient que les organismes revoient et effectuent régulièrement (par exemple annuellement) le processus du BIA et à chaque fois que des modifications importantes sont apportées à l'organisme ou à son contexte.

Dans le présent document, les termes «BIA» et «processus de BIA» sont utilisés, ainsi que les termes «résultat» et «aboutissement». La Figure 2 décrit comment ces termes sont utilisés.

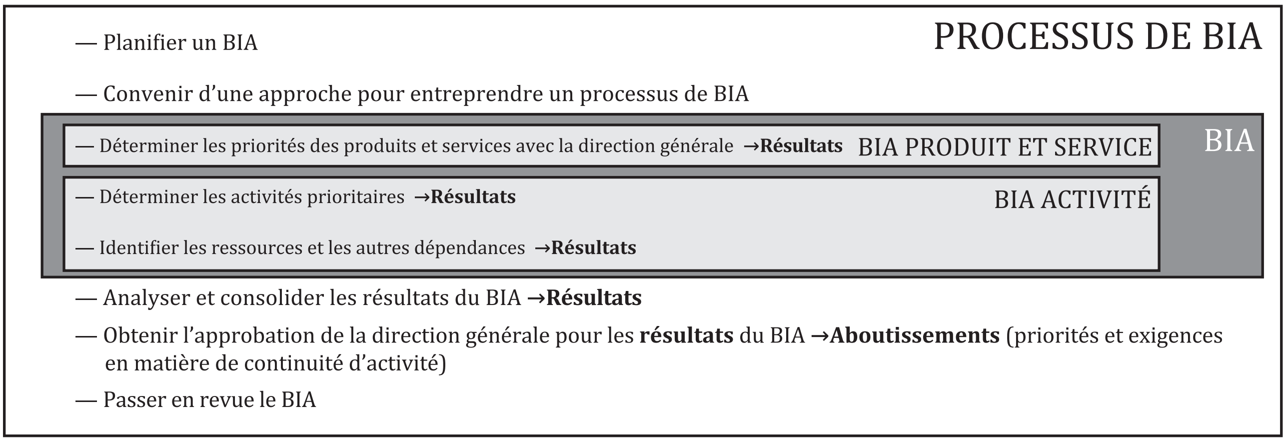


Figure 2 — Comprendre BIA, processus de BIA, résultats et aboutissements

L'objet du présent document est de:

— fournir une base pour la mise en œuvre d'un processus de BIA efficace au sein d'un organisme;

— soutenir l'organisme dans la planification, la conduite et le reporting du processus de BIA de manière cohérente.

Le présent document donne des exemples de réalisation de BIA. Il est important de noter que ces exemples, individuels ou combinés, peuvent aider un organisme à arriver à des aboutissements en matière de BIA. La sélection de la méthode la plus appropriée sera influencée par la taille de l'organisme, son secteur, la géographie ou le contexte.

Les aboutissements du processus de BIA comprennent les éléments suivants:

a) approbation ou modification du domaine d'application du SMCA de l'organisme;

b) identification des exigences (obligations) réglementaires, juridiques et contractuelles et de leur effet sur les priorités et les exigences relatives à la continuité d'activité;

c) évaluation de l'impact d'une perturbation sur l'organisme dans le temps, qui sert de justification aux priorités et exigences relatives à la continuité d'activité;

d) estimation du temps que prendraient les impacts adverses pour rendre les produits et services inacceptables [durée maximale tolérable de perturbation (DMTP)] après une perturbation;

e) identification des exigences [DMTP et objectifs de délai de rétablissement (RTO)] pour les activités prioritaires;

f) identification des ressources nécessaires pour réaliser les activités prioritaires à la suite d'une perturbation, y compris leurs dépendances, et exigences, en spécifiant les RTO et les points de rétablissement des données (RPO);

g) identification des dépendances, y compris les fournisseurs, partenaires et autres parties intéressées;

h) identification des interdépendances des activités prioritaires.

La Figure 3 montre le processus de BIA, ainsi que ses conditions préalables et sa relation avec la sélection de stratégies et de solutions de continuité d'activité. Les chiffres indiqués dans le schéma correspondent aux paragraphes du présent document.

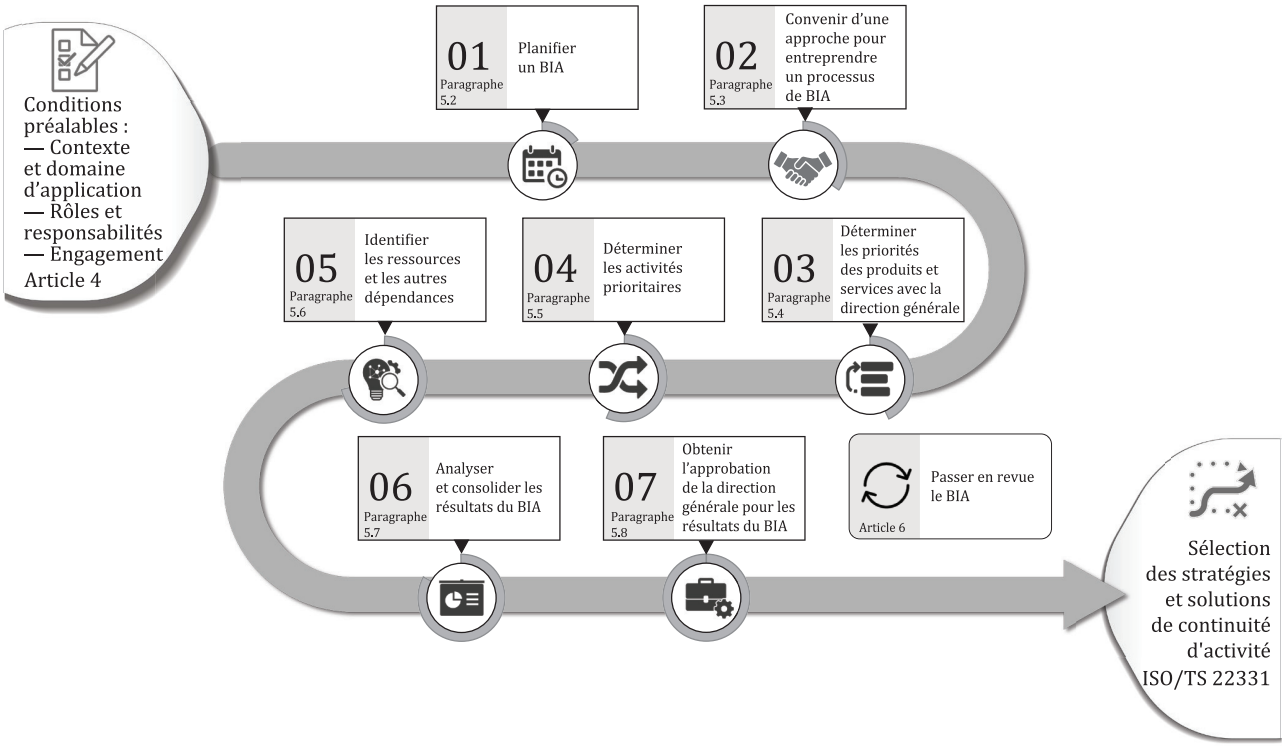


Figure 3 — Processus de BIA

Il convient que l'organisme utilise la déclaration sur les priorités et les exigences de continuité d'activité afin de sélectionner les stratégies et les solutions de continuité d'activité.

Le BIA peut amener l'organisme à reconsidérer la manière dont il livre ses produits et fournit ses services.

Le BIA dépend des informations fournies par de nombreuses personnes à travers l'organisme qui peuvent avoir des perspectives différentes sur la manière dont l'organisme fonctionne, sur ce qui est critique en termes de temps, ou sur les impacts qui peuvent survenir à la suite d'une perturbation. Il est courant que certaines personnes exagèrent leurs exigences alors que d'autres les minorent. Le présent document cherche à définir une approche qui fournisse suffisamment d'objectivité et minimise ces questions dans le but d'arriver à des aboutissements efficaces.

Sécurité et résilience — Systèmes de management de la continuité d'activité — Lignes directrices pour le bilan d'impact sur l'activité

1 Domaine d'application

Le présent document fournit des lignes directrices visant à permettre à un organisme de mettre en œuvre et de maintenir un processus formel et documenté de bilan d'impact sur l'activité (BIA), adapté à ses besoins. Il n'impose pas de processus unique pour l'exécution d'un BIA.

Le présent document est applicable à tous les organismes, quels que soient leur type, leur taille et leur nature, qu'ils appartiennent au secteur privé ou au secteur public et qu'ils soient à but non lucratif ou non. Les lignes directrices peuvent être adaptées en fonction des besoins, objectifs, ressources et contraintes de l'organisme.

2 Références normatives

Les documents suivants sont cités dans le texte de sorte qu'ils constituent, pour tout ou partie de leur contenu, des exigences du présent document. Pour les références datées, seule l'édition citée s'applique. Pour les références non datées, la dernière édition du document de référence s'applique (y compris les éventuels amendements).

ISO 22300, *Sécurité et résilience — Vocabulaire*

ISO 22301, *Sécurité et résilience — Systèmes de management de la continuité d'activité — Exigences*

3 Termes et définitions

Pour les besoins du présent document, les termes et définitions de l'ISO 22300 et l'ISO 22301 s'appliquent.

L'ISO et l'IEC tiennent à jour des bases de données terminologiques destinées à être utilisées en normalisation, consultables aux adresses suivantes:

— ISO Online browsing platform: disponible à l'adresse https://www.iso.org/obp

— IEC Electropedia: disponible à l'adresse https://www.electropedia.org/

4 Conditions préalables

4.1 Généralités

Bien que le présent document soit en cohérence avec les exigences de l'ISO 22301, il peut être utilisé pour mettre en œuvre et passer en revue tout processus de BIA.

Avant de commencer un processus de BIA, il convient que l'organisme:

— définisse le contexte et le domaine d'application du processus de BIA (voir 4.2);

— définisse et communique les rôles et les responsabilités (voir 4.3);

— obtienne un engagement du leadership et alloue les ressources adéquates (voir 4.4);

NOTE Voir l'Annexe A pour une mise en correspondance de chaque article avec l'ISO 22301.

4.2 Contexte et domaine d'application

4.2.1 Contexte

Les aboutissements du processus de BIA dépendent de la compréhension de l'organisme vis-à-vis des éléments suivants, pour qu'il puisse remplir son objet en livrant ses produits et fournissant ses services à ses clients:

— l'environnement externe (comprenant les fournisseurs, les organes statutaires et réglementaires) dans lequel il fonctionne;

— l'environnement opérationnel interne, y compris les processus métier, activités et ressources, ainsi que l'impact potentiel d'une perturbation sur la livraison des produits et la fourniture des services.

NOTE Pour les organismes opérant dans un environnement non commercial, le «client» peut être le public ou une autorité de tutelle telle que l'administration.

4.2.2 Domaine d'application

Il convient que le processus de BIA couvre l'ensemble du domaine d'application du SMCA. Il convient que l'organisme définisse et documente le domaine d'application du SMCA en termes de produits et de services. Les aboutissements du processus de BIA peuvent requérir de l'organisme qu'il reconsidère le domaine d'application du SMCA par l'ajout ou la suppression de certains produits et services.

Il convient d'abord que l'organisme priorise tous les produits et services du domaine d'application, qui peuvent comprendre des services stratégiques internes (voir 5.4.3). Ceux dont les priorités sont les plus élevées peuvent être traités en premier.

4.3 Rôles et responsabilités

4.3.1 Généralités

Il convient que la direction générale s'assure que:

— les responsabilités et l'autorité des rôles pertinents sont attribuées et communiquées au sein de l'organisme;

— les personnes pilotant le processus de BIA sont compétentes;

— les ressources nécessaires à l'exécution du processus de BIA sont pourvues.

Il convient que la direction générale s'assure que les rôles suivants (d'autres rôles peuvent être concernés) relatifs à l'exécution du processus de BIA sont attribués:

a) le pilote du BIA (cela peut être la même personne que le responsable SMCA) (voir 4.3.2);

b) les propriétaires d'activité (voir 4.3.3).

4.3.2 Pilote du BIA

Le pilote du BIA est responsable du processus de BIA et il convient qu'il:

— s'assure que des personnes ayant les compétences requises sont disponibles pour réaliser le processus de BIA;

— prépare et fournisse la méthodologie du BIA;

— planifie et gère le processus de BIA;

— s'assure que les informations fournies par les propriétaires d'activité sont cohérentes au sein de l'organisme;

— entreprenne la consolidation et l'analyse des informations fournies par les propriétaires d'activité;

— présente les aboutissements à la direction générale pour approbation.

4.3.3 Propriétaires d'activité

Il convient que les propriétaires d'activité:

— fournissent une compréhension approfondie de l'activité dont ils sont responsables, y compris de l'ensemble des ressources qui permettent à l'activité d'être réalisée;

— fournissent des informations concernant les solutions de contournement, les processus métier et les ressources existants, qui influent sur les priorités et exigences relatives à la continuité d'activité;

— appliquent la méthodologie du BIA et fournissent les informations pertinentes au pilote du BIA.

4.4 Engagement

L'engagement de la direction générale en faveur du processus de BIA est nécessaire pour assurer une participation efficace. Il convient que la direction générale:

a) communique la valeur du processus de BIA;

b) apporte un soutien continu au processus de BIA;

c) fournisse suffisamment de ressources pour le processus de BIA afin de:

   1) remplir les rôles et responsabilités spécifiques au processus de BIA, ainsi que les exigences relatives à la formation et à la sensibilisation (prise de conscience), en temps opportun;

   2) répondre à l'évolution des exigences de l'organisme;

d) donne son accord sur les méthodes, priorités et délais relatifs au BIA;

e) s'assure que l'environnement permet de réaliser des améliorations continues au sein de l'organisme;

f) approuvent les aboutissements du BIA qui assurent:

   1) que les priorités et les exigences relatives à la continuité d'activité sont alignées sur les objectifs et la direction stratégique de l'organisme;

   2) que l'organisme respecte ses obligations juridiques et contractuelles et les exigences des clients en cas de perturbation;

   3) que les produits et services, les processus métier, les activités et ressources sont alignés de façon appropriée;

g) assure que les aboutissements du BIA sont disponibles lors de la sélection des stratégies et solutions de continuité d'activité.

5 Le processus de BIA

5.1 Fondamentaux

Le processus de BIA priorise les activités et les ressources, de sorte que, à la suite d'une perturbation, la livraison de produits et la fourniture de services puissent reprendre dans un délai prédéterminé et avec une capacité prédéfinie, de façon satisfaisante pour les parties intéressées. Les aboutissements en sont les priorités et les exigences relatives à la continuité d'activité.

La qualité du processus de BIA et de ses aboutissements est essentielle pour sélectionner les stratégies et solutions appropriées de continuité d'activité.

La rapidité pour obtenir des aboutissements de qualité pour le BIA est essentielle pour minimiser les impacts en cas de perturbation. Si certaines informations sont incomplètes, indisponibles, confidentielles ou retenues, il convient que ces difficultés ne retardent pas la progression et l'achèvement du processus de BIA. Il convient de trouver un équilibre entre la qualité et la rapidité.

5.2 Planifier le BIA

Les tâches de planification peuvent inclure:

a) l'allocation des ressources nécessaires, y compris les personnes compétentes pour piloter le processus de BIA ou y prendre part;

b) le regroupement des produits et services lorsque leurs caractéristiques sont similaires, il est possible par exemple de les regrouper par type, par zone géographique ou par secteur d'activité;

c) l'identification de la structure de l'organisme et des équipes ou individus pouvant fournir des informations sur les produits et services, les activités et les ressources;

d) la communication des attentes à tous les participants du processus de BIA;

e) l'établissement du plan, incluant les activités menées pour:

   1) obtenir l'accord de la direction générale quant à l'approche utilisée pour entreprendre le processus de BIA (voir 5.3);

   2) organiser une ou des réunion(s) avec la direction générale pour déterminer les priorités relatives aux produits et services (voir 5.4);

   3) identifier et sélectionner des méthodes de collecte des informations (voir Annexe B);

   4) définir un modèle ou un outil pour enregistrer les informations collectées (voir 5.5);

   5) rassembler les informations provenant des propriétaires d'activité (voir 5.5 et 5.6);

   6) analyser et consolider les informations reçues (voir 5.7);

   7) obtenir l'approbation de la direction générale concernant les résultats (voir 5.8);

f) l'obtention d'une approbation concernant le processus de BIA planifié.

5.3 Convenir de l'approche pour engager le processus de BIA

5.3.1 Comprendre les impacts

Le processus de BIA explore, de manière cohérente, les impacts sur l'organisme résultant d'une perturbation dans la livraison des produits et la fourniture des services. La perturbation peut venir de l'intérieur, de la chaîne d'approvisionnement ou d'autres sources externes – de chacun de ces éléments peut résulter une perturbation dans la livraison d'un ou plusieurs produits et services aux clients et aux autres parties intéressées.

Les impacts sur l'organisme résultant des réactions des parties intéressées peuvent inclure les exemples donnés au Tableau 1.

Tableau 1 — Impacts dus aux parties intéressées

Partie intéressée	Exemples d'impacts
Consommateurs et clients existants	Perte de revenus et de parts de marché Plaintes accrues Pénalités contractuelles ou contentieux
Communauté	Perte de confiance
Consommateurs et clients potentiels	Perte d'opportunités commerciales potentielles
Organismes partenaires	Volonté et capacité réduites de poursuivre la coopération
Média et société	Effet négatif sur la réputation, l'image de marque et l'opinion publique
Parties prenantes	Effet négatif sur le cours actuel de l'action et les investissements futurs
Créancier	Effet négatif sur les paiements des dettes et les exigences financières futures
Concurrents	Perte de parts de marché si les concurrents profitent de la situation
Personnel	Perte de personnel clé (temporaire ou permanente)
Régulateurs et gouvernement	Pénalités et modifications des règles Perte de licence d'exploitation

5.3.2 Définir les types d'impacts et les critères

L'organisme peut expérimenter différents types d'impact tels que les atteintes à la réputation ou aux objectifs métiers, les pertes financières et les litiges. Les types d'impact ne sont pas les mêmes que les types ou catégories de conséquences utilisés en management des risques. L'impact est le résultat d'une perturbation sur l'organisme. Pour comparer et apprécier de manière cohérente des impacts qui sont très différents, il convient que l'organisme définisse des types d'impacts et des critères.

Il convient que l'organisme définisse les types d'impact afin de comprendre les impacts dans le temps à la suite d'une perturbation dans la livraison des produits ou la fourniture des services. Il convient que la direction générale approuve les types d'impact proposés et les critères.

Le choix des types d'impact et des critères est influencé par le secteur, le contexte et la nature des activités de l'organisme, ainsi que par la culture organisationnelle. Il convient que la sélection d'un ou plusieurs types d'impact et de critères, y compris le besoin d'avoir des informations quantitatives et qualitatives concernant l'impact, ainsi que le niveau de détails recueillis, conviennent à l'organisme pour sélectionner ou justifier les priorités et les exigences en matière de continuité d'activité.

Les types d'impact à prendre en compte peuvent comprendre:

— les objectifs métiers;

— les aspects environnementaux;

— les aspects financiers;

— la santé et la sécurité des personnes;

— les aspects réglementaires, juridiques et contractuels;

— les parts de marché;

— les aspects opérationnels;

— les aspects de réputation.

Un organisme peut consolider les types d'impact, par exemple:

— les objectifs métiers;