
**Sécurité et résilience — Systèmes
de management de la continuité
d'activité — Lignes directrices pour
le développement des plans et
procédures de continuité d'activité**

*Security and resilience — Business continuity management systems
— Guidelines for developing business continuity plans and procedures*
(standards.iteh.ai)

[ISO/TS 22332:2021](https://standards.iteh.ai/catalog/standards/sist/5e16d702-71bc-4f67-b812-303887320e3d/iso-ts-22332-2021)

<https://standards.iteh.ai/catalog/standards/sist/5e16d702-71bc-4f67-b812-303887320e3d/iso-ts-22332-2021>



iTeh STANDARD PREVIEW
(standards.iteh.ai)

[ISO/TS 22332:2021](https://standards.iteh.ai/catalog/standards/sist/5e16d702-71bc-4f67-b812-303887320e3d/iso-ts-22332-2021)

<https://standards.iteh.ai/catalog/standards/sist/5e16d702-71bc-4f67-b812-303887320e3d/iso-ts-22332-2021>



DOCUMENT PROTÉGÉ PAR COPYRIGHT

© ISO 2021

Tous droits réservés. Sauf prescription différente ou nécessité dans le contexte de sa mise en œuvre, aucune partie de cette publication ne peut être reproduite ni utilisée sous quelque forme que ce soit et par aucun procédé, électronique ou mécanique, y compris la photocopie, ou la diffusion sur l'internet ou sur un intranet, sans autorisation écrite préalable. Une autorisation peut être demandée à l'ISO à l'adresse ci-après ou au comité membre de l'ISO dans le pays du demandeur.

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	v
Introduction	vi
1 Domaine d'application	1
2 Références normatives	1
3 Termes et définitions	1
4 Prérequis	1
4.1 Généralités.....	1
4.2 Parties intéressées.....	2
4.3 Identifier les stratégies et solutions de continuité d'activité approuvées.....	2
4.4 Développement du plan de continuité d'activité, rôles et compétences.....	2
4.5 Ressources pour le développement et la maintenance des plans et procédures de continuité d'activité.....	3
5 Réponse	3
5.1 Généralités.....	3
5.2 Structure de réponse.....	3
5.3 Compétence des membres des équipes.....	4
6 Types de plans et procédures des équipes de continuité d'activité	4
6.1 Généralités.....	4
6.2 Plan de l'équipe stratégique.....	5
6.2.1 Objet.....	5
6.2.2 Composition de l'équipe.....	5
6.2.3 Propriétaire.....	5
6.3 Plans des équipes tactiques.....	5
6.3.1 Objet.....	5
6.3.2 Composition de l'équipe.....	6
6.3.3 Propriétaire.....	6
6.4 Plans des équipes opérationnelles.....	6
6.4.1 Objet.....	6
6.4.2 Composition de l'équipe.....	6
6.4.3 Propriétaire.....	6
7 Contenu du plan et des procédures de continuité d'activité	7
7.1 Généralités.....	7
7.2 Sections communes.....	7
7.2.1 Objet.....	7
7.2.2 Objectifs.....	7
7.2.3 Présupposés.....	7
7.2.4 Activation et convocation de l'équipe.....	7
7.2.5 Rôles et responsabilités des membres de l'équipe.....	8
7.2.6 Tâches.....	8
7.2.7 Communications.....	8
7.2.8 Interrelations avec les autres plans.....	8
7.2.9 Démobilisation de l'équipe.....	8
7.2.10 Informations sur les ressources.....	9
7.2.11 Informations de contact.....	9
7.2.12 Annexes.....	9
7.2.13 Contrôle de version.....	9
7.2.14 Contrôle et distribution du plan.....	10
7.3 Procédures spécifiques.....	10
7.3.1 Procédures de réponse d'urgence.....	10
7.3.2 Procédures de communication.....	10
7.3.3 Procédures des technologies de l'information et de la communication (TIC).....	11
7.3.4 Procédures de mise en place d'installations alternatives.....	12

7.3.5	Procédures d'approvisionnement en ressources alternatives.....	12
8	Plans de réponse aux perturbations spécifiques.....	12
8.1	Généralités.....	12
8.2	Pandémie (mondiale) et épidémie (régionale).....	12
8.3	Cyberattaque.....	13
9	Recommandations sur la rédaction des plans.....	13
9.1	Généralités.....	13
9.2	Clarté.....	14
9.3	Exhaustivité.....	14
10	Contrôles, stockage et disponibilité du plan.....	14
11	Étapes suivant la rédaction des plans et procédures de continuité d'activité.....	15
11.1	Sensibilisation.....	15
11.2	Exercices et tests.....	15
12	Surveillance et revue des plans et procédures de continuité d'activité.....	15
12.1	Revue de performance.....	15
12.2	Maintenance.....	15
12.3	Revue de direction.....	16
Annexe A (informative) Procédures de maintenance de la capacité de continuité d'activité.....		17
Bibliographie.....		21

iTeh STANDARD PREVIEW
(standards.iteh.ai)

[ISO/TS 22332:2021](https://standards.iteh.ai/catalog/standards/sist/5e16d702-71bc-4f67-b812-303887320e3d/iso-ts-22332-2021)

<https://standards.iteh.ai/catalog/standards/sist/5e16d702-71bc-4f67-b812-303887320e3d/iso-ts-22332-2021>

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*.

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.htm.

Introduction

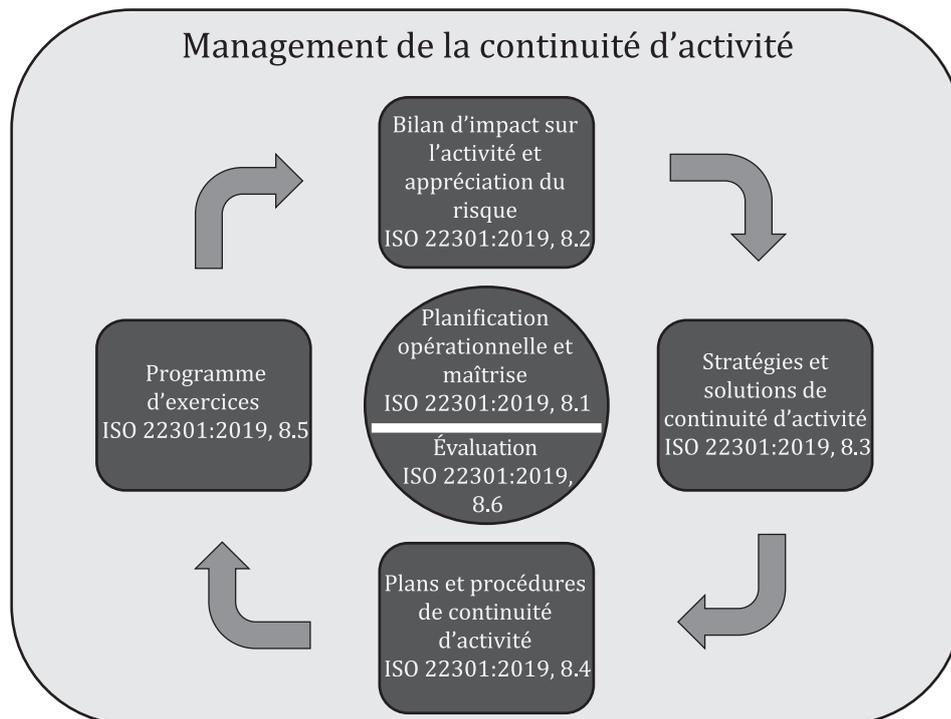
Le présent document fournit des lignes directrices pour le développement et la maintenance des plans et procédures de continuité d'activité. Il est cohérent avec les exigences de la norme ISO 22301 et s'applique au développement de tout plan de continuité d'activité, ou comme partie d'un système de management de la continuité d'activité (SMCA).

Un plan de continuité d'activité fournit des recommandations et des informations destinées à aider les équipes à répondre à une perturbation (ISO 22301:2019, 8.4.1) afin de satisfaire aux attentes de livraison des produits et de fourniture des services. Il convient que l'organisme crée des plans et procédures permettant de traiter les communications, la gestion des situations d'urgence, la réponse à incident, la gestion de crise, le rétablissement et la restauration.

Il convient de mettre les plans et procédures de continuité d'activité en cohérence avec les buts et objectifs de l'organisme, ainsi qu'avec ses objectifs de continuité d'activité (voir ISO 22301:2019, 3.4) et de détailler les actions que les équipes vont accomplir pendant une perturbation afin:

- d'activer la réponse;
- de gérer les conséquences immédiates d'une perturbation;
- de continuer ou rétablir les activités prioritaires dans des délais prédéterminés à l'aide des stratégies et solutions de continuité d'activité convenues si celles-ci sont appropriées;
- de surveiller l'impact de la perturbation et la réponse de l'organisme à celle-ci;
- de livrer les produits et fournir les services au niveau de capacité convenu.

La [Figure 1](#) représente les flux entre les différents composants du management de la continuité d'activité. Le processus de la stratégie et des solutions de continuité d'activité (ISO 22301:2019, 8.3) permet d'identifier, de développer et de maintenir les plans et procédures de continuité d'activité (ISO 22301:2019, 8.4). Les plans et procédures de continuité d'activité sont quant à eux indispensables pour coordonner et exécuter les exercices et tests de continuité d'activité (ISO 22301:2019, 8.5).



SOURCE: ISO 22313:2020.

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

<https://standards.iteh.ai/catalog/standards/sist/5e16d702-71bc-4f67-b812-389000000000/iso-ts-22332-2021>

Le présent document a pour but de fournir aux organismes:

- des méthodes détaillées de développement des plans et procédures de continuité d'activité;
- une approche structurée de collecte et d'organisation des informations nécessaires au développement des plans et des procédures;
- des conseils sur la maintenance des plans et procédures dans le temps en vue d'établir un environnement d'amélioration continue.

En suivant ces lignes directrices, il sera possible d'atteindre les résultats suivants:

- établissement d'une structure de management pour répondre à une perturbation, désignation d'un personnel et d'équipes compétentes et responsables disposant de l'autorité nécessaire pour gérer la réponse;
- mise en œuvre et maintenance de processus de réponse concernant la protection de la vie et des actifs;
- établissement d'un commandement et d'un contrôle des opérations dans l'effort de rétablissement engagé après le début de la perturbation;
- mise en œuvre et maintenance de procédures de communication et d'avertissement y compris celles nécessaires pour gérer la réponse aux médias et la coordination avec les autres parties intéressées pendant toute la durée de la perturbation;
- continuité ou rétablissement des activités professionnelles perturbées et des ressources indisponibles dans des délais prédéterminés, y compris les procédures nécessaires au retour des activités professionnelles depuis les mesures temporaires adoptées pendant l'incident jusqu'au fonctionnement normal;

- rétablissement des actifs technologiques perturbés;
- établissement de procédures de maintenance des capacités et de mobilisation de la réponse telles que la formation croisée et les exercices.

iTeh STANDARD PREVIEW
(standards.iteh.ai)

[ISO/TS 22332:2021](https://standards.iteh.ai/catalog/standards/sist/5e16d702-71bc-4f67-b812-303887320e3d/iso-ts-22332-2021)

<https://standards.iteh.ai/catalog/standards/sist/5e16d702-71bc-4f67-b812-303887320e3d/iso-ts-22332-2021>

Sécurité et résilience — Systèmes de management de la continuité d'activité — Lignes directrices pour le développement des plans et procédures de continuité d'activité

1 Domaine d'application

Le présent document fournit des lignes directrices pour le développement et la maintenance des plans et procédures de continuité d'activité. Il s'applique à tous les organismes quels que soient leur type, leur taille et leur nature appartenant au secteur privé, public ou associatif, qui souhaitent développer de façon cohérente des plans et procédures efficaces de continuité d'activité.

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*

ITeH STANDARD PREVIEW
(standards.iteh.ai)

3 Termes et définitions

ISO/TS 22332:2021

Pour les besoins du présent document, les termes et définitions donnés dans l'ISO 22300 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 Prérequis

4.1 Généralités

Bien que les présentes lignes directrices soient cohérentes avec l'ISO 22301, elles peuvent être utilisées pour développer et maintenir les plans et procédures de continuité d'activité visant à s'aligner sur d'autres normes, obligations ou exigences réglementaires ou à y souscrire. Quelle que soit l'approche retenue, plusieurs prérequis doivent être satisfaits. Il convient que l'organisme:

- comprenne les besoins et les attentes des parties intéressées (4.2);
- détermine et sélectionne une stratégie (4.3);
- définisse et communique les rôles et responsabilités des personnes devant développer les plans (4.4);
- alloue les ressources adéquates au développement et à la maintenance des plans (4.5).

4.2 Parties intéressées

Il convient de traiter les besoins et les attentes des parties intéressées dans le cadre de la continuité d'activité. C'est pourquoi il convient que l'organisme identifie ses parties intéressées et détermine leurs exigences concernant la réponse et l'effort de rétablissement pendant une perturbation.

4.3 Identifier les stratégies et solutions de continuité d'activité approuvées

Avant de développer des plans et procédures de continuité d'activité, il convient que l'organisme ait déterminé, sélectionné et approuvé des stratégies et solutions de continuité d'activité incluant l'identification:

- de modalités de travail alternatives pour faire face à la perte ou à l'inaccessibilité des locaux;
- de dispositions pour faire face à une indisponibilité de personnel;
- des capacités de rétablissement des actifs et services de technologie perturbés, y compris les données et les communications;
- de moyens alternatifs permettant de livrer les produits et fournir les services en cas de perturbation d'un fournisseur.

NOTE Voir ISO 22301 et ISO 22331.

4.4 Développement du plan de continuité d'activité, rôles et compétences

Il convient que la direction affecte une personne dotée de l'autorité appropriée à la supervision d'une équipe chargée d'élaborer les plans et procédures de continuité d'activité englobant le domaine d'application du système de management de la continuité d'activité (SMCA).

Les rôles ou tâches nécessaires à l'élaboration des plans et procédures de continuité d'activité peuvent inclure:

- la gestion des projets de planification de la continuité d'activité;
- la conception d'un modèle de plan permettant d'assurer une cohérence;
- l'apport de contenu aux plans et procédures de continuité d'activité;
- l'approbation des plans et procédures de continuité d'activité.

Il convient que l'organisme s'assure de la compétence des personnes qui dirigent le développement et la maintenance des plans et procédures de continuité d'activité ainsi que de celles qui y participent. Il convient que ces compétences incluent:

- une bonne compréhension de l'organisme;
- la planification, la gestion et la collaboration de projets;
- le rassemblement d'informations;
- la compréhension des processus de l'organisme et des flux;
- une communication orale et écrite efficace;
- les méthodes et techniques nécessaires pour gérer la réponse à une perturbation.

4.5 Ressources pour le développement et la maintenance des plans et procédures de continuité d'activité

Il convient que l'organisme détermine et apporte les ressources nécessaires pour développer et maintenir les plans et procédures de continuité d'activité qui lui permettront:

- de se conformer à sa propre politique de continuité d'activité et d'atteindre ses objectifs de continuité d'activité;
- d'activer au moment opportun ses stratégies et solutions de réponse et de rétablissement;
- de maintenir la mobilisation de la réponse;
- d'assurer l'amélioration continue de ses plans et procédures de continuité d'activité (en effectuant régulièrement des tests, par exemple).

Les ressources incluent le temps de personnel et les ressources financières nécessaires pour documenter et maintenir les plans et procédures de continuité d'activité.

5 Réponse

5.1 Généralités

Pendant une perturbation, il convient que les plans et procédures de continuité d'activité:

- permettent à l'organisme de prendre des décisions en temps utile;
- soient suffisamment flexibles pour s'adapter à des situations imprévues et évolutives;
- se focalisent sur l'objectif de minimiser les effets anticipés des perturbations;
- fassent usage, dans les cas appropriés, des stratégies et solutions de continuité d'activité préparées pour réduire le plus possible les impacts;
- identifient les rôles et attribuent les responsabilités pour toutes les activités de réponse;
- disposent des ressources disponibles nécessaires pour soutenir les activités de réponse.

5.2 Structure de réponse

Il convient que l'organisme établisse une structure de réponse consistant en une ou plusieurs équipes, chacune soutenue par un ensemble de plans et procédures documentés. En collaborant entre elles pendant une perturbation, ces équipes permettront à l'organisme:

- d'identifier, de faire remonter et de gérer l'incident;
- de gérer les besoins de toutes les parties intéressées;
- de reprendre la livraison des produits et la fourniture des services dans des délais prédéterminés à un niveau acceptable.

Si la nature de l'incident menace des vies ou des actifs, des actions immédiates peuvent être engagées pour les protéger.

Une structure hiérarchique d'équipes peut être créée, comprenant:

- Une équipe stratégique: équipe de la direction, qui, si nécessaire, gère les problèmes stratégiques de l'incident, notamment ceux extérieurs à l'organisme, tels que la communication, l'aspect réglementaire et la réputation. La direction peut choisir de déléguer à une équipe de communication séparée l'envoi des messages internes et externes.

- Une ou plusieurs équipes tactiques: une équipe de management, ou plusieurs équipes, qui gèrent la réponse interne à l'incident et le rétablissement des activités. La ou les équipes tactiques analysent l'impact de l'incident et dirigent les équipes opérationnelles dans la mise en œuvre des solutions appropriées parmi celles disponibles, assurent la reprise en temps utile de la livraison des produits et de la fourniture des services et rendent compte à l'équipe stratégique de leur progression.
- Équipes opérationnelles: chaque service ou unité fonctionnelle peut disposer de plans qui, selon sa fonction, décrivent la manière dont l'équipe répondra aux perturbations. Elles fonctionnent sous la direction d'une équipe tactique, à qui elles rendent compte de leur progression.

Dans un organisme de petite taille, une équipe unique peut suffire à gérer tous les aspects de la réponse.

5.3 Compétence des membres des équipes

Pour satisfaire aux objectifs des équipes, il convient d'accorder une grande attention à la sélection de leurs membres. Le [Tableau 1](#) souligne les qualités nécessaires aux membres de chaque équipe.

Tableau 1 — Caractéristiques des membres des équipes

Niveau	Compétence des membres
Équipe stratégique	<ul style="list-style-type: none"> — comprendre les buts stratégiques de l'organisme; — connaître leurs responsabilités et être aptes à les exercer; — assurer la supervision des équipes; — être capable de prendre des décisions sous la pression; — être apte à anticiper le ou les impacts possibles sur l'organisme.
Équipe tactique	<ul style="list-style-type: none"> — connaître leurs responsabilités et être aptes à les exercer; — comprendre les relations entre les équipes et les plans; — savoir coordonner des activités multiples au même moment et communiquer avec les équipes stratégiques, tactiques et opérationnelles; — comprendre les complexités de l'organisme et les conséquences des décisions; — être apte à travailler et prendre des décisions sous la pression; — démontrer une capacité de résolution pragmatique des problèmes; — savoir remettre en question les décisions.
Équipe opérationnelle	<ul style="list-style-type: none"> — connaître leurs responsabilités et être aptes à les exercer; — être apte à travailler avec précision et méthode sous la pression; — suivre les instructions avec discipline; — être aptes à faire remonter les préoccupations ou les problèmes.

6 Types de plans et procédures des équipes de continuité d'activité

6.1 Généralités

Les procédures sont documentées dans des plans.

Chaque équipe a besoin d'un plan pour s'assurer qu'elle:

- comprend son domaine d'action, ses objectifs et ses responsabilités;