NORME INTERNATIONALE

ISO/CEI 27031

Première édition
2011-03-01

Technologies de l'information — Techniques de sécurité — Lignes directrices pour la préparation des technologies de la communication et de l'information pour la continuité d'activité

Information technology — Security techniques — Guidelines for information and communication technology readiness for business continuity

Numéro de référence
ISO/CEI 27031:2011(F)

Version française parue en 2012

Publié en Suisse

Sommaire

Page

Avant-propos

L'ISO (Organisation internationale de normalisation) et la CEI (Commission électrotechnique internationale) forment le système spécialisé de la normalisation mondiale. Les organismes nationaux membres de l'ISO ou de la CEI participent au développement de Normes internationales par l'intermédiaire des comités techniques créés par l'organisation concernée afin de s'occuper des domaines particuliers de l'activité technique. Les comités techniques de l'ISO et de la CEI collaborent dans des domaines d'intérêt commun. D'autres organisations internationales, gouvernementales et non gouvernementales, en liaison avec l'ISO et la CEI participent également aux travaux. Dans le domaine des technologies de l'information, l'ISO et la CEI ont créé un comité technique mixte, l'ISO/CEI JTC 1.

Les Normes internationales sont rédigées conformément aux règles données dans les Directives ISO/CEI, Partie 2.

La tâche principale du comité technique mixte est d'élaborer les Normes internationales. Les projets de Normes internationales adoptés par le comité technique mixte sont soumis aux organismes nationaux pour vote. Leur publication comme Normes internationales requiert l'approbation de 75 % au moins des organismes nationaux votants.

L'attention est appelée 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 et la CEI ne sauraient être tenues pour responsables de ne pas avoir identifié de tels droits de propriété et averti de leur existence.

L'ISO/CEI 27031 a été élaborée par le comité technique mixte ISO/CEI JTC 1, *Technologies de l'information*, sous-comité SC 27, *Techniques de sécurité des technologies de l'information.*

Introduction

Les technologies de l'information et de la communication (TIC) sont devenues, au fil des années, partie intégrante de nombreuses activités qui constituent les éléments des infrastructures critiques dans tous les secteurs d'activité organisationnels, qu'ils soient publics, privés ou bénévoles. Le développement à grande échelle de l'Internet et d'autres services de mise en réseaux électroniques, ainsi que les capacités actuelles des systèmes et applications, impliquent également que les organisations se fient plus que jamais à des infrastructures TIC fiables, sécurisées et protégées.

Entre-temps, la nécessité d'un processus de management de la continuité d'activité (MCA), y compris la préparation aux incidents, la planification de reprise après un sinistre, et les mesures d'intervention et de gestion des situations d'urgence, a été admise et prise en charge par des domaines spécifiques de connaissances et d'expertise, et des normes ont été élaborées et publiées ces dernières années, dont la norme internationale MCA élaborée par l'ISO/TC 223.

NOTE L'ISO/TC 223 est en cours d'élaboration d'une Norme internationale pertinente de gestion de la continuité d'activité (ISO 22301).

Les défaillances des services TIC, y compris l'occurrence de problèmes liés à la sécurité, tels que la violation de systèmes et les infections par des logiciels malfaisants influent sur la continuité des activités opérationnelles. Ainsi, la gestion des TIC et de la continuité associée, ainsi que des autres aspects liés à la sécurité, constitue un élément clé des exigences de continuité d'activité. De plus, dans la majorité des cas, les fonctions commerciales critiques exigeant une continuité d'activité dépendent habituellement des TIC. Cette dépendance signifie que des perturbations des TIC peuvent représenter des risques stratégiques pour la renommée de l'organisation et sa capacité d'action.

La préparation des TIC est un composant essentiel de la mise en œuvre d'un processus de gestion de la continuité d'activité et de management de la sécurité de l'information pour de nombreuses organisations. Il est essentiel, en tant que partie intégrante de la mise en œuvre et de l'exploitation d'un système de management de la sécurité de l'information (SMSI) spécifié dans l'ISO/CEI 27001 et d'un système de management de la continuité d'activité (SMCA), d'élaborer et de mettre en œuvre un plan d'intervention immédiate à l'intention des services TIC afin de s'assurer de la continuité effective de l'activité.

Un système MCA efficace dépend ainsi fréquemment d'une préparation efficace des TIC afin de s'assurer que les objectifs d'une organisation peuvent continuer à être satisfaits en cas de perturbations. Cet élément est particulièrement important dans la mesure où les conséquences de perturbations des TIC présentent souvent l'inconvénient supplémentaire d'être invisibles et/ou difficiles à déceler.

Pour pouvoir réaliser une préparation des TIC de façon à garantir la continuité de son activité, une organisation doit mettre en place un processus systématique de prévention, prévision et gestion des perturbations et des incidents liés aux TIC, susceptibles de perturber les services qui leur sont associés. L'application des étapes cycliques PDCA (Plan-Do-Check-Act / Planifier-Faire-Vérifier-Agir) comme partie intégrante d'un système de management de la Préparation des TIC pour la Continuité d'Activité (PTCA) constitue le meilleur moyen pour y parvenir. De cette manière, la PTCA soutient le MCA en s'assurant que les services TIC sont les plus résilients possibles et peuvent être restaurés aux niveaux prédéterminés dans les délais requis et définis par l'organisation.

Tableau 1 — Cycle Planifier-Faire-Vérifier-Agir en PTCA

Planifier	Établir une politique, des objectifs, cibles, processus et procédures PTCA adaptés à la gestion des risques et à l'amélioration de la disponibilité des TIC de façon à fournir des résultats conformes aux politiques et objectifs de la continuité d'activité globale d'une organisation.
Faire	Mettre en œuvre et exploiter la politique et les mesures, processus et procédures PTCA.
Vérifier	Évaluer et, le cas échéant, mesurer les performances d'un processus par rapport à la politique, aux objectifs et à l'expérience pratique de la PTCA, et rendre compte des résultats à la direction pour revue.
Agir	Prendre des mesures correctives et préventives, sur la base des résultats de la revue de direction, en vue de l'amélioration continue de la PTCA.

Lorsqu'une organisation utilise l'ISO/CEI 27001 pour établir un SMSI, et/ou utilise des normes correspondantes pour établir un SMCA, il convient que la mise en place d'une PTCA prenne de préférence en considération les processus existants ou prévus associés à ces normes. Cette association peut prendre en charge l'établissement d'une PTCA, et éviter toute redondance éventuelle de processus pour l'organisation. La Figure 1 synthétise l'interaction de la PTCA et du SMCA.

Pour la planification et la mise en œuvre d'une PTCA, une organisation peut se reporter à l'ISO/CEI 24762:2008, dans le cadre de sa planification et de la fourniture de services TIC de reprise après un sinistre, indépendamment du fait que ces services soient délivrés ou non par un fournisseur externe, ou qu'ils soient internes à l'organisation.

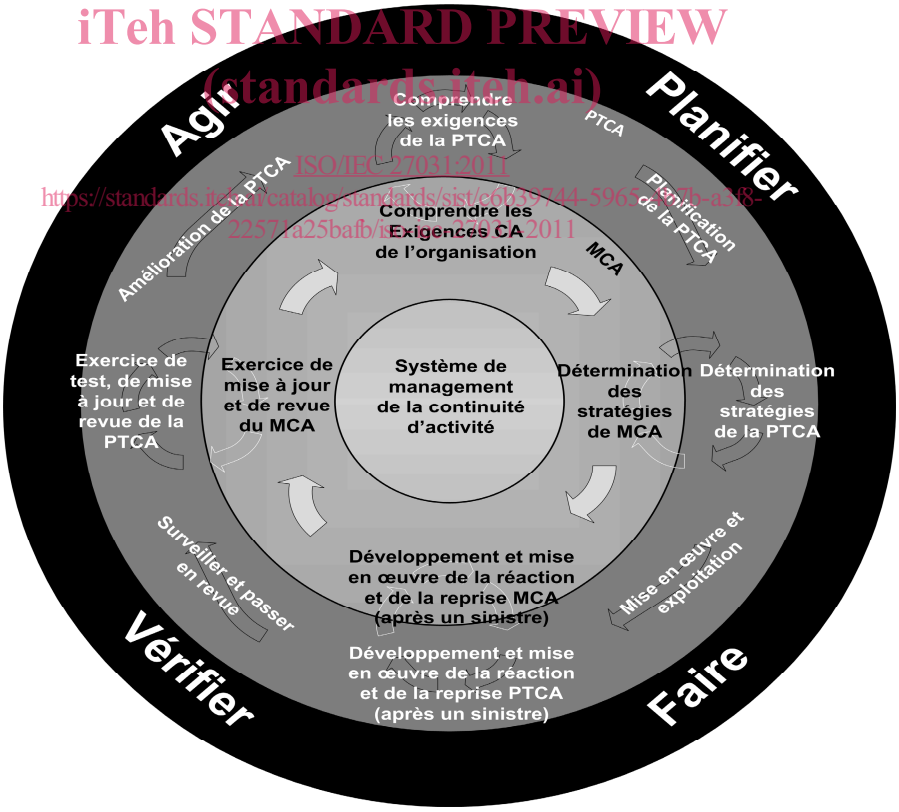

Figure 1 — Intégration des PTCA et SMCA

Technologies de l'information — Techniques de sécurité — Lignes directrices pour la préparation des technologies de la communication et de l'information pour la continuité d'activité

1 Domaine d'application

La présente Norme internationale décrit les concepts et principes de préparation des technologies de l'information et de la communication (TIC) pour la continuité d'activité, et fournit un cadre de méthodes et processus destinés à identifier et spécifier l'ensemble des aspects (tels que les critères de performance, la conception et la mise en œuvre) permettant d'améliorer la préparation des TIC, et ce, de manière à assurer la continuité d'activité d'une organisation. Elle s'applique à toute organisation (privée, gouvernementale et non gouvernementale, quelle que soit sa taille) qui développe son programme de préparation des TIC pour la continuité de son activité (PTCA), et exige de ses services/infrastructures TIC qu'ils soient prêts à prendre en charge les opérations d'activité en cas de survenance d'événements et d'incidents effectifs, ainsi que de perturbations associées, susceptibles d'affecter la continuité (y compris la sécurité) des fonctions métier critiques. Elle permet aussi à une organisation de mesurer les paramètres de performance en corrélation avec sa PTCA d'une manière cohérente et reconnue.

Le domaine d'application de la présente Norme internationale comprend tous les événements et incidents (y compris ceux liés à la sécurité) susceptibles d'influencer l'infrastructure et les systèmes TIC. Il inclut et étend les pratiques de traitement et de gestion des incidents de sécurité de l'information, ainsi que de planification de la préparation des TIC et des services associés.

2 Références normatives

Les documents ci-après, dans leur intégralité ou non, sont des références normatives indispensables à l'application 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/CEI TR 18044:2004[1)], *Technologies de l'information — Techniques de sécurité — Gestion d'incidents de sécurité de l'information.*

ISO/CEI 27000, *Technologies de l'information — Techniques de sécurité — Systèmes de management de la sécurité de l'information — Vue d'ensemble et vocabulaire.*

ISO/CEI 27001, *Technologies de l'information — Techniques de sécurité — Systèmes de management de la sécurité de l'information — Exigences.*

ISO/CEI 27002, *Technologies de l'information — Techniques de sécurité — Code de bonne pratique pour le management de la sécurité de l'information.*

ISO/CEI 27005, *Technologies de l'information — Techniques de sécurité — Gestion des risques liés à la sécurité de l'information.*

1) L'ISO/CEI TR 18044:2004 doit être révisée et renumérotée ISO/CEI 27035.

3 Termes et définitions

Pour les besoins du présent document, les termes et définitions donnés dans l'ISO/CEI TR 18044, l'ISO/CEI 27000, l'ISO/CEI 27001, l'ISO/CEI 27002, l'ISO/CEI 27005 et les suivants s'appliquent.

3.1
site alternatif
site d'exploitation alternatif choisi pour être utilisé par une organisation lorsque les opérations d'activité normales ne peuvent être réalisées sur le site normal après une perturbation effective

3.2
management de la continuité d'activité
MCA
processus global de management identifiant les menaces potentielles pour une organisation et les impacts sur les opérations d'activité que ces menaces, si elles se traduisent de manière concrète, peuvent provoquer, et fournissant un cadre pour développer la résilience organisationnelle avec la capacité d'une réaction efficace qui protège les intérêts de ses parties prenantes clés, ainsi que de sa renommée, sa marque et ses activités à création de valeur

3.3
plan de continuité d'activité
PCA
procédures documentées fournissant aux organisations des instructions de réaction, rétablissement, reprise et restauration à un niveau prédéfini de fonctionnement suite à une perturbation

NOTE Cette notion couvre typiquement les ressources, services et activités nécessaires pour assurer la continuité des fonctions commerciales critiques.

3.4
analyse d'impact sur l'activité
AIA
processus d'analyse des fonctions opérationnelles et de l'effet potentiel d'une perturbation sur ces dernières

3.5
critique
description qualitative utilisée pour souligner l'importance d'une ressource, d'un processus ou d'une fonction qui doit être disponible et opérationnel(le) de manière constante, ou disponible et opérationnel(le) le plus rapidement possible après un incident, un cas d'urgence ou un sinistre

3.6
perturbation
incident, prévu (par exemple, ouragan) ou intempestif (par exemple, panne d'alimentation/électricité ; séisme, ou attaque de systèmes/d'une infrastructure TIC) qui perturbe le cours normal des opérations sur le site d'une organisation

3.7
reprise après un sinistre (TIC)
capacité des éléments TIC d'une organisation à soutenir ses activités critiques à un niveau acceptable dans un délai prédéterminé suite à une perturbation

3.8
plan de reprise après un sinistre (TIC)
PRAS
plan défini et documenté de manière claire et permettant de restaurer les capacités TIC lors d'une perturbation

NOTE Ce plan est appelé plan de continuité TIC dans certaines organisations.

3.9
mode de défaillance
méthode d'observation d'une défaillance

NOTE Décrit généralement le mode d'occurrence de la défaillance et son impact sur le fonctionnement du système.

3.10
préparation des TIC pour la continuité d'activité
PTCA
capacité d'une organisation à soutenir ses opérations d'activité par la prévention, la détection, la réaction à une perturbation et la reprise des services TIC

3.11
objectif minimum de continuité d'activité
OMCA
niveau minimum de services et/ou produits acceptable par l'organisation pour atteindre ses objectifs d'activité lors d'une perturbation

3.12
objectif de point de reprise
OPR
moment auquel les données doivent être rétablies suite à une perturbation

3.13
délai de reprise
DR
période au cours de laquelle les niveaux minimum de services et/ou produits, ainsi que les systèmes, applications ou fonctions de soutien, doivent être rétablis suite à une interruption

3.14
résilience
capacité d'une organisation à résister aux perturbations qui l'affectent

3.15
déclencheur
événement qui provoque la réaction du système

NOTE Également appelé événement déclencheur.

3.16
document essentiel
document électronique ou au format papier essentiel pour la préservation, la poursuite ou le rétablissement des opérations d'une organisation, ainsi que pour la protection des droits de cette même organisation, de ses employés, clients et parties prenantes

4 Abréviations

PTCA Préparation des TIC pour la continuité d'activité (en anglais ICT Readiness for Business Continuity)

SMSI Système de management de la sécurité de l'information (en anglais Information Security Management System).

5 Généralités

5.1 Rôle de la PTCA dans le management de la continuité d'activité

Le management de la continuité d'activité (MCA) est un processus de gestion globale qui identifie les impacts potentiels constituant une menace pour la continuité des activités commerciales d'une organisation, et fournit un cadre de mise en place d'une résilience et d'une capacité nécessaires à une réaction efficace préservant les intérêts de l'organisation contre les perturbations.

La PTCA, comme partie intégrante du processus MCA, se rapporte à un système de management qui complète et soutient le programme MCA et/ou SMSI d'une organisation, afin d'améliorer la préparation immédiate de l'organisation pour :

a) réagir à un environnement de risque en constante évolution ;

b) assurer la continuité des activités opérationnelles critiques prises en charge par les services TIC associés ;

c) pouvoir réagir bien avant la perturbation d'un service TIC, dès la détection d'un ou d'une série d'événements associés qui deviennent des incidents ; et

d) réagir et reprendre l'activité suite à des incidents/sinistres et des défaillances.

La Figure 2 illustre le résultat TIC souhaité venant à l'appui des activités de gestion de la continuité d'activité.

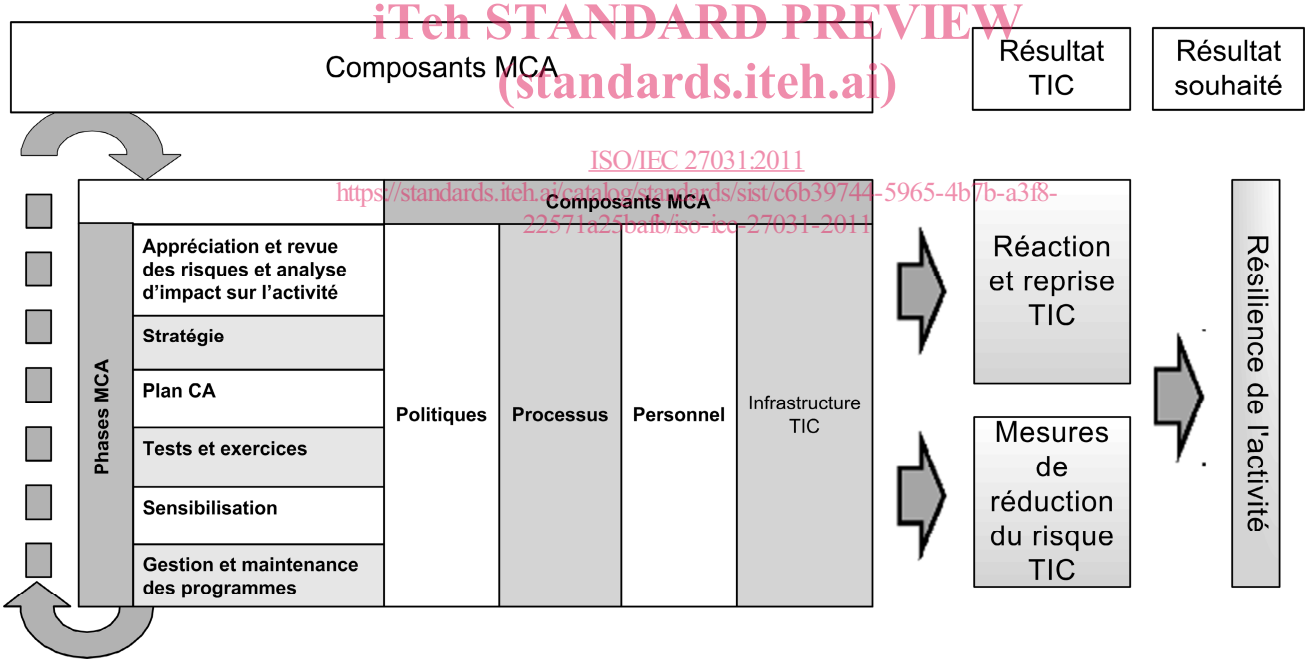

Figure 2 — Cadre pour la continuité d'activité, et produit et résultat souhaité TIC associés

La Norme internationale MCA développée par l'ISO/TC 223 résume l'approche MCA de prévention, réaction et reprise après des incidents. Les activités internes au processus MCA incluent la préparation aux incidents, la gestion de la continuité opérationnelle, la planification de la reprise après un sinistre (PRAS), et l'atténuation du risque dont l'objectif est le renforcement de la résilience de l'organisation et sa préparation à une réaction efficace aux incidents et à une reprise de l'activité dans les délais prédéterminés.

Une organisation fixe par conséquent ses priorités MCA, ces dernières menant aux activités PTCA. A son tour, la MCA dépend de la PTCA afin de s'assurer que l'organisation peut satisfaire de façon permanente à ses objectifs généraux de continuité d'activité, et notamment pendant des périodes de perturbation.

Ces activités de préparation, comme l'illustre la Figure 3, visent à :

a) améliorer les capacités de détection d'un incident ;

b) éviter toute défaillance subite ou sévère ;

c) permettre une dégradation acceptable de l'état opérationnel pour le cas où la défaillance ne peut pas être supprimée ;

d) réduire davantage le temps de reprise ; et

e) réduire l'impact sur l'occurrence éventuelle de l'incident.

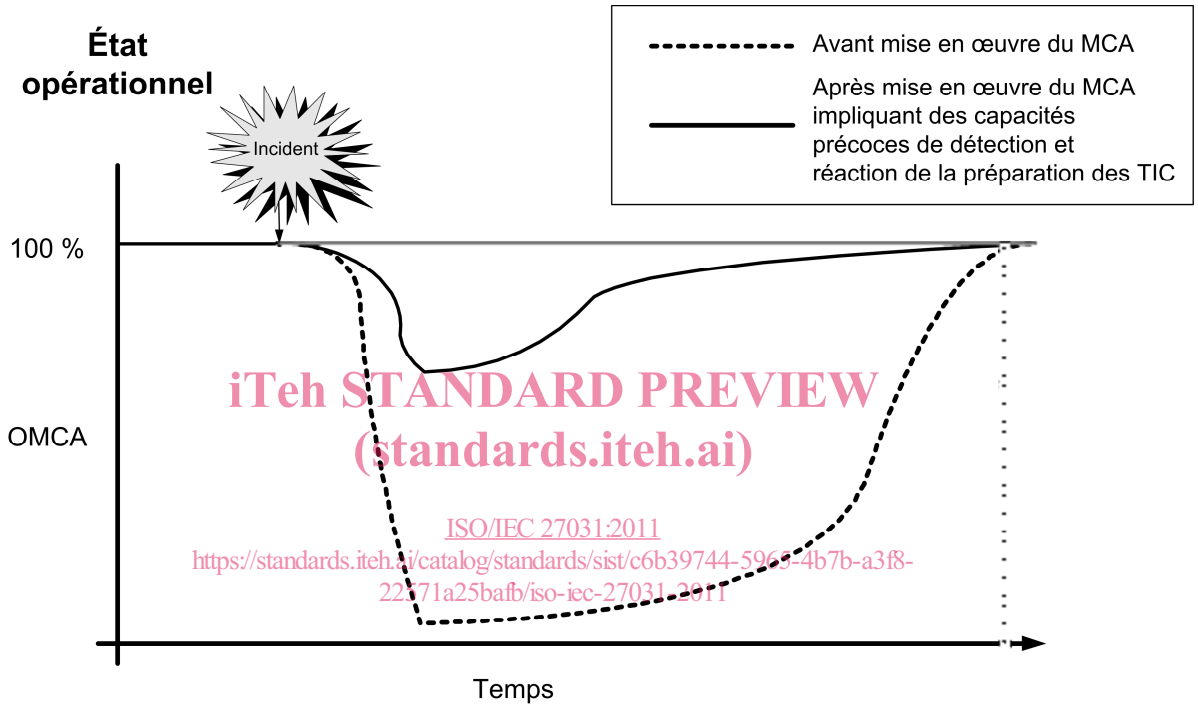

Figure 3 — Concept de préparation des TIC pour la continuité d'activité

5.2 Principes de la PTCA

La PTCA repose sur les principes clés suivants :

a) prévention des incidents - La protection des services TIC contre les menaces, telles que les défaillances liées à l'environnement et matérielles, les erreurs de fonctionnement, les attaques malfaisantes et les catastrophes naturelles, est critique pour le maintien des niveaux souhaités de disponibilité des systèmes pour une organisation ;

b) détection des incidents - La détection des incidents le plus tôt possible réduit l'impact sur les services, réduit l'effort de reprise et préserve la qualité de service ;

c) réaction - La réaction à un incident de la manière la plus appropriée engendre une reprise plus efficace et minimise de durée d'indisponibilité. Une mauvaise réaction peut transformer un incident mineur en un incident bien plus grave ;