PROJET FINAL
Norme internationale

ISO/IEC FDIS 27031

Cybersécurité — Préparation des technologies de l'information et de la communication pour la continuité d'activité

Cybersecurity — Information and communication technology readiness for business continuity

ISO/IEC JTC **1**/SC **27**

Secrétariat: **DIN**

Début de vote:
2024-06-26

Vote clos le:
2024-08-21

Numéro de référence
ISO/IEC FDIS 27031:2024(fr)

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

L'ISO (Organisation internationale de normalisation) et l'IEC (Commission électrotechnique internationale) forment le système spécialisé de la normalisation mondiale. Les organismes nationaux membres de l'ISO ou de l'IEC 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 l'IEC collaborent dans des domaines d'intérêt commun. D'autres organisations internationales, gouvernementales et non gouvernementales, en liaison avec l'ISO et l'IEC participent également aux travaux.

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. Le présent document a été rédigé conformément aux règles de rédaction données dans les Directives ISO/IEC, Partie 2 (voir www.iso.org/directives ou www.iec.ch/members_experts/refdocs).

L'ISO et l'IEC attirent l'attention sur le fait que la mise en application du présent document peut entraîner l'utilisation d'un ou de plusieurs brevets. L'ISO et L'IEC ne prennent pas position quant à la preuve, à la validité et à l'applicabilité de tout droit de propriété revendiqué à cet égard. À la date de publication du présent document, l'ISO et l'IEC n'avaient pas reçu notification qu'un ou plusieurs brevets pouvaient être nécessaires à sa mise en application. Toutefois, il y a lieu d'avertir les responsables de la mise en application du présent document que des informations plus récentes sont susceptibles de figurer dans la base de données de brevets, disponible aux adresses www.iso.org/brevets et https://patents.iec.ch. L'ISO et l'IEC ne sauraient être tenues pour responsables de ne pas avoir identifié tout ou partie de tels droits de brevet.

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. Pour l'IEC, voir www.iec.ch/understanding-standards.

Le présent document a été élaboré par le comité technique mixte ISO/IEC JTC 1, *Technologies de l'information*, sous-comité SC 27, *Sécurité de l'information, cybersécurité et protection de la vie privée*.

Cette deuxième édition annule et remplace la première édition (ISO/IEC 27031:2011), qui a fait l'objet d'une révision technique.

Les principales modifications sont les suivantes:

— la structure du document a été modifiée;

— le domaine d'application a été modifié pour clarification;

— un contenu technique a été ajouté en 6.4, 6.5, 6.6, 9.2 et 10.1.5.

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 aux adresses www.iso.org/fr/members.html et www.iec.ch/national-committees.

Introduction

Les technologies de l'information et de la communication (TIC) sont devenues, au fil des années, partie intégrante de nombreuses activités au sein des infrastructures critiques dans tous les secteurs d'activité organisationnels, qu'ils soient publics ou privés. Le développement à grande échelle de l'internet et d'autres services de mise en réseaux électroniques, ainsi que les capacités des systèmes et applications, a également eu pour résultat que les organisations sont plus dépendantes d'infrastructures TIC fiables, sécurisées et protégées.

Entre-temps, la nécessité d'un management de la continuité d'activité (MCA), y compris la préparation aux incidents, la planification de la reprise après un sinistre, et la réponse et la gestion des urgences, a été reconnue et soutenue avec le développement et l'approbation de domaines spécifiques de connaissances, d'expertise, et de normes, y compris l'ISO 22313.

Les défaillances des services TIC, y compris celles provoquées par des problèmes liés à la sécurité, tels que la violation de systèmes et les infections par des logiciels malfaisants, influent sur la continuité des opérations Métier. Ainsi, la gestion des TIC et le management de la continuité associée, ainsi que d'autres aspects liés à la sécurité, constituent un élément clé des exigences en matière de continuité d'activité. De plus, dans la majorité des cas, les processus et activités 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.

Du fait de la prédominance croissante des services TIC basés sur l'internet (services TIC en nuage), la nature de la capacité de préparation a changé, passant d'une dépendance aux processus internes à une dépendance à la qualité et à la robustesse des services fournis par d'autres organisations et aux relations professionnelles avec ces organisations.

Pour de nombreuses organisations, la préparation des TIC est un composant essentiel de la mise en œuvre d'un processus de management de la continuité d'activité et de management de la sécurité de l'information.

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 pendant les perturbations. Cet élément est particulièrement important dans la mesure où les conséquences de perturbations des TIC présentent souvent l'inconvénient supplémentaire d'être invisibles ou difficiles à déceler.

Pour pouvoir réaliser une préparation des TIC de façon à garantir la continuité de son activité (PTCA), il convient qu'une organisation mette 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. Il est possible d'y parvenir en coordonnant la PTCA avec les processus de sécurité de l'information et de MCA. De cette manière, la PTCA soutient le MCA en s'assurant que les services TIC peuvent être restaurés aux niveaux prédéterminés dans les délais requis et définis par l'organisation.

Lorsqu'une organisation utilise des normes pertinentes en matière de sécurité de l'information et de continuité d'activité, 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.

Le présent document décrit les concepts et principes de préparation des TIC pour la continuité d'activité (PTCA), et fournit un cadre de méthodes et processus destinés à identifier et spécifier les aspects permettant d'améliorer la préparation des TIC, et ce, de manière à assurer la continuité d'activité d'une organisation.

Le présent document complète les mesures de sécurité de l'information relatives à la continuité d'activité dans l'ISO/IEC 27002. Il soutient également le processus de management des risques liés à la sécurité de l'information spécifié dans l'ISO/IEC 27005.

Sur la base des objectifs de préparation des TIC, le présent document étend également les pratiques de gestion des incidents de sécurité de l'information à la planification, à la formation et à l'exploitation de la préparation des TIC.

Cybersécurité — Préparation des technologies de l'information et de la communication pour la continuité d'activité

1 Domaine d'application

Le présent document décrit les concepts et les principes de la préparation des technologies de l'information et de la communication (TIC) pour la continuité d'activité (PTCA). Il fournit un cadre de méthodes et de processus pour identifier et spécifier les aspects permettant d'améliorer la préparation des TIC d'une organisation afin d'assurer la continuité d'activité.

Le présent document sert les objectifs suivants en matière de continuité d'activité pour les TIC:

— objectif minimal de continuité d'activité (OMCA);

— objectif de point de reprise (OPR);

— délai de reprise (DR) dans le cadre de la planification de la continuité d'activité des TIC.

Le présent document s'applique à tous les types et tailles d'organisations.

Le présent document décrit de quelle manière les services TIC planifient et se préparent à contribuer aux objectifs de résilience de l'organisation.

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

ISO/IEC 27002, *Sécurité de l'information, cybersécurité et protection de la vie privée — Mesures de sécurité de l'information*

ISO/IEC 27005, *Sécurité de l'information, cybersécurité et protection de la vie privée — Préconisations pour la gestion des risques liés à la sécurité de l'information*

ISO/IEC 27035-1:2023, *Technologies de l'information — Gestion des incidents de sécurité de l'information — Partie 1: Principes et processus*

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 les définitions de l'ISO/IEC 27000, ISO/IEC 27002, ISO/IEC 27005, ISO/IEC 27035-1, ISO 22300 et ISO 22301, ainsi que les suivants 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/

3.1
mode de défaillance
méthode d'observation d'une défaillance

Note 1 à l'article: Cela décrit généralement le mode d'occurrence de la défaillance et son impact sur le fonctionnement du système.

3.2
reprise après un sinistre des technologies de l'information et de la communication
capacité des éléments de technologies de l'information et de la communication d'une organisation à soutenir ses processus et activités critiques à un niveau acceptable dans un délai prédéterminé à la suite d'une perturbation

3.3
préparation des technologies de l'information et de la communication
état d'une fonction de technologies de l'information et de la communication (TIC) dans lequel elle dispose des connaissances, des compétences, des processus, de l'architecture, de l'infrastructure et des technologies connexes pour la préparation à un événement potentiel qui entraînerait soit une perturbation intolérable des TIC, soit une perte intolérable de données

Note 1 à l'article: Cela ne signifie pas que la fonction de TIC est parfaitement informée et capable de tout faire, mais plutôt qu'elle est adaptée aux objectifs et prête pour la préparation, la réponse et la reprise si une telle situation d'urgence se produit.

3.4
objectif minimal de continuité d'activité
OMCA
niveau minimal de services et/ou produits acceptable par l'organisation pour atteindre ses objectifs d'activité lors d'une perturbation

3.5
objectif de point de reprise
OPR
point à partir duquel les informations utilisées par une activité doivent être restaurées afin de permettre un fonctionnement en reprise

Note 1 à l'article: Il peut également être désigné en tant que «perte maximale de données».

3.6
délai de reprise
DR
durée après un incident pendant laquelle un produit et service ou une activité sont repris, ou des ressources sont rétablies

3.7
restauration
niveau de rétablissement des données, des systèmes TIC et des opérations Métier à leur état normal après une perturbation, avec une perte minimale, le cas échéant

3.8
déclencheur
événement qui provoque la réaction du système

Note 1 à l'article: Également appelé événement déclencheur.

4 Abréviations

AIA Analyse d'impact sur l'activité

CVC Chauffage, ventilation et air conditionné

DR Délai de reprise

OMCA Objectif minimal de continuité d'activité

OPR Objectif de point de reprise

PCA Plan de continuité d'activité

PTCA Préparation des TIC pour la continuité d'activité

TIC Technologies de l'information et de la communication

5 Structure du présent document

5.1 Généralités

L'objectif de chaque article du présent document est le suivant:

— l'Article 6 explique comment la PTCA est liée au MCA et à d'autres processus organisationnels qui sont liés à la PTCA;

— l'Article 7 explique comment la continuité d'activité de l'organisation établit des objectifs qu'il convient d'essayer d'atteindre pour la PTCA;

— l'Article 8 donne des recommandations sur ce qui est nécessaire pour définir les caractéristiques actuelles des TIC qui ont une influence sur la PTCA;

— l'Article 9 donne des recommandations sur différentes stratégies qui peuvent être utilisées et qu'il convient de déterminer pour la PTCA en fonction des objectifs et des caractéristiques actuelles des TIC qu'il convient de suivre pour les plans de continuité des TIC;

— l'Article 10 donne des recommandations sur la manière de concevoir des plans de continuité des TIC fondés sur des stratégies déterminées et sur la manière de traiter différents types de situations défavorables afin d'atteindre les objectifs de continuité pour les TIC;

— l'Article 11 donne des recommandations sur la manière de soumettre à l'essai et de finaliser les plans de continuité des TIC;

— l'Article 12 donne des recommandations sur la manière d'établir les OPR et DR finaux sur la base des plans de continuité des TIC et sur la manière de déterminer la capacité à répondre aux exigences opérationnelles;

— l'Article 13 donne des recommandations sur le retour d'information de la PTCA à la direction au plus haut niveau afin que celle-ci approuve les plans ou les décisions de traitement du risque si les objectifs d'activité n'ont pas été atteints.

Une planification et des vérifications spécifiques des TIC sont essentielles pour construire et assurer que les TIC peuvent faire face à des événements. Sans cette préparation, l'organisation subit des perturbations intolérables des activités prioritaires ou des pertes de données.

Il convient que de tels événements, pouvant résulter de défaillances techniques ou d'incidents de cybersécurité, incitent la fonction de TIC à interfacer sa gouvernance, sa planification et son fonctionnement avec les exigences découlant de l'activité décisionnelle du management de la continuité d'activité et du management de la sécurité de l'information.

6 Intégration de la PTCA dans le MCA

6.1 Généralités

Le risque associé aux perturbations dans le cadre de la sécurité de l'information et des TIC est principalement lié à la disponibilité lorsque survient une situation défavorable qui perturbe la disponibilité des services TIC pour les activités Métier.

Les risques associés ont les caractéristiques d'une très faible vraisemblance, ce qui signifie qu'ils peuvent se produire très rarement, voire jamais, mais qu'ils ont des conséquences et un impact sur l'activité considérables s'ils se produisent. Il convient de noter que la continuité d'activité est l'activité censée réduire le plus fortement possible les conséquences si de tels risques se produisent, car, dans la plupart des cas, la vraisemblance de ces risques ne peut jamais être totalement éliminée.

La détermination des risques pour les processus d'activité peut résulter du processus de management du risque et des mesures de sécurité visant à les atténuer pour maintenir la continuité d'activité.

Les activités prioritaires sont identifiées au moyen d'une analyse d'impact sur l'activité (AIA) portant sur les processus d'activité et les fonctions, qui permet de déterminer les dépendances des TIC et d'établir des délais critiques.

Les événements réels ou les scénarios de risque concernant la manière dont les services TIC sont interrompus peuvent être difficiles à déterminer pour les entreprises et sont généralement situés à un niveau élevé, sur la base de différentes menaces. Ces menaces et ces sources peuvent inclure:

— sources environnementales — incendies, inondations, etc.;

— défaillances techniques matérielles et logicielles, ou les insuffisances ou pannes de l'alimentation et de la climatisation (CVC);

— source de risque humain involontaire — erreurs dans la gestion des modifications, sauvegarde mal configurée, etc.;

— source de risque humain intentionnelle — piratage, logiciels malfaisants, sabotage;

— sociétales — pandémie, grèves, troubles sociaux, etc.;

— cyberattaques — DOS, DDOS;

— spécifiques à la chaîne d'approvisionnement des TIC:

  — perturbation du canal de communication avec un fournisseur de données/services;

  — perturbation d'un fournisseur de services en nuage;

  — exigences peu claires en matière de sécurité de l'information dans les conditions contractuelles couvrant les services TIC fournis par des parties externes.

Ces menaces ou événements peuvent considérablement perturber les services TIC et déclencher des stratégies de continuité d'activité, avec les conséquences suivantes:

— perte de matériels et logiciels de TIC critiques;

— perte de service de TIC critique;

— perte d'installations;

— perte de service de TIC critique d'un fournisseur;

— perte de personnel clé.

Il convient que ces scénarios soient pris en compte dans le cadre de la planification de la continuité d'activité pour les TIC s'ils sont pertinents pour les TIC fournies à l'activité. Il convient de déterminer des stratégies

globales et d'élaborer et de soumettre à l'essai le PCA afin de déterminer les risques résiduels à traiter dans le cadre du processus de management du risque. Les vulnérabilités ou les autres faiblesses qui provoquent de graves perturbations pour les TIC peuvent être déterminées au moyen d'un management des risques. C'est au moyen d'une évaluation des risques et d'un traitement des risques que les risques peuvent être atténués. Cependant, cette atténuation n'élimine pas la nécessité de mettre en place une PTCA, car il existe toujours un risque qu'un événement imprévu se produise.

6.2 Facilitation de la gouvernance

Il convient que les organisations aient une connaissance générale de la préparation des différents éléments des TIC, y compris les suivants:

— les services TIC;

— les installations TIC;

— la technologie (matériel, logiciels, architecture);

— les données;

— les processus;

— les fournisseurs, ainsi que leurs composantes critiques; et

— les compétences du personnel.

La connaissance de la structure des TIC est un élément crucial pour assurer le soutien nécessaire à la gouvernance de la continuité d'activité, y compris la préparation des TIC. Il convient par conséquent que l'organisation:

a) suscite, améliore et maintienne la sensibilité par le biais d'un programme permanent de formation, d'études et d'information destiné au personnel compétent, et établisse un processus d'évaluation de l'efficacité de la prestation de sensibilisation; et

b) s'assure que le personnel est conscient de sa contribution à la réalisation des objectifs de préparation des TIC pour la continuité d'activité (PTCA).

Il convient que l'organisation s'assure que l'ensemble du personnel auquel il a confié des responsabilités PTCA dispose des compétences nécessaires pour exécuter les tâches requises, et ce en:

c) déterminant les compétences nécessaires dudit personnel;

d) effectuant une analyse des besoins en formation de ce même personnel;

e) assurant une formation;

f) s'assurant de l'acquisition effective des compétences nécessaires; et

g) tenant des registres dédiés aux études, à la formation, aux compétences, à l'expérience et aux qualifications.

Il convient que la direction au plus haut niveau ou ses délégués s'assurent qu'une répartition claire et complète des rôles a été établie avec une granularité suffisante pour identifier chaque rôle individuel dans la PTCA. Il convient de documenter l'identification des responsabilités liées à chaque rôle attribué.

Il convient de planifier, d'élaborer et de mettre en œuvre un programme de formation à la PTCA afin de s'assurer que le personnel concerné ayant un rôle dans la PTCA puisse remplir ses responsabilités lorsqu'un événement se produit.

NOTE Pour plus de détails concernant la sensibilisation et la formation à la gestion des incidents de sécurité de l'information, voir l'ISO/IEC 27035-2.

6.3 Objectifs du management de la continuité d'activité

Le management de la continuité d'activité est le processus permettant de mettre en œuvre et de maintenir la capacité d'une organisation à continuer la fourniture de produits et de services dans des délais acceptables avec une capacité prédéfinie pendant une perturbation.

La PTCA, comme partie intégrante du processus MCA, se rapporte à un processus visant à améliorer la préparation immédiate de l'organisation pour:

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

b) assurer la continuité des services TIC liés qui soutiennent les activités prioritaires;

c) anticiper et être prêt à 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 à la suite d'incidents et des défaillances affectant les TIC.

Une organisation fixe par conséquent ses priorités MCA, qui orientent les activités PTCA. À son tour, le MCA dépend de la PTCA afin de s'assurer que l'organisation peut satisfaire de façon permanente à ses objectifs généraux de continuité du service TIC, et notamment pendant des périodes de perturbation.

Ces objectifs de préparation incluent notamment:

e) l'amélioration des capacités de détection d'un incident;

f) la prévention de toute défaillance subite ou sévère;

g) la possibilité d'une dégradation acceptable du service opérationnel si la défaillance ne peut pas être empêchée;

h) une réduction supplémentaire du temps de reprise; et

i) la réduction la plus forte possible des conséquences sur l'occurrence éventuelle de l'incident.

6.4 Management du risque et mesures de sécurité applicables pour la PTCA

Le processus de management du risque inclut les risques liés à la sécurité de l'information lorsque le risque lié à la perte de disponibilité des services TIC dans des situations défavorables s'applique à la préparation des TIC et à la continuité d'activité. Ces risques sont caractérisés par une très faible vraisemblance et un très fort impact.

Il convient que le traitement du risque comporte des mesures de sécurité liées à la continuité de l'activité.

Ces mesures sont essentielles pour modifier et diminuer le risque et réduire l'impact sur l'activité grâce à une PTCA. Il convient alors de déterminer l'étendue et la capacité de la PTCA par le biais du processus de management du risque, en fonction de la propension à prendre des risques et de l'analyse d'impact sur l'activité.

Le management du risque et les rapports sur l'état du risque aident l'entreprise à déterminer le risque et l'éventuelle acceptation du risque selon une perspective stratégique et à long terme.

La PTCA soutient la mise en œuvre réelle de la mesure de sécurité spécifiée dans l'ISO/IEC 27002:2022, 5.30.

Pour des informations supplémentaires sur le management des risques liés à la sécurité de l'information, voir l'ISO/IEC 27005.

6.5 Gestion des incidents et relation avec la PTCA

Les incidents applicables à la PTCA se situent au niveau de classification le plus élevé de la classification des incidents de l'organisation subissant ces incidents.