Business continuity management (BCM) pour les compagnies d'assurances en Suisse – standards minimaux et recommandations

Juin 2015

ASA | SVV

Schweizerischer Versicherungsverband
Association Suisse d'Assurances
Associazione Svizzera d'Assicurazioni
Swiss Insurance Association

Destinataires :
Les compagnies d'assurances assujetties à la surveillance de la Finma

Editeur :
Schweizerischer Versicherungsverband SVV | Association Suisse d'Assurances ASA
Conrad-Ferdinand-Meyer-Strasse 14
Case postale
CH-8022 Zurich

Tel. +41 44 208 28 28
Fax +41 44 208 28 00
info@svv.ch
www.svv.ch

Comité compétent :
Comité Finance & régulation

Interlocuteur :
Alex Schönenberger
Département finance et régulation
Schweizerischer Versicherungsverband SVV | Association Suisse d'Assurances ASA
Case postale, CH-8022 Zürich

Pour commander :
alex.schoenenberger@svv.ch

Juin 2015

Exposé de la situation

L'activité d'une compagnie d'assurances peut se retrouver fortement entravée par des événements exceptionnels et des situations de crise. Dans un souci de préservation de la survie de l'entreprise et du maintien de ses activités, des mesures sont nécessaires pour surmonter les situations de crise et garantir la poursuite des processus critiques de l'entreprise (Business continuity management – BCM ou Gestion de la continuité des activités – GCA).

Le présent document s'adresse aux compagnies d'assurances assujetties à la surveillance de l'Autorité fédérale de surveillance des marchés financiers (Finma). Il comprend des standards minimaux et des recommandations permettant d'élaborer une méthode de gestion de la continuité des activités de l'entreprise qui épouse parfaitement les besoins de celle-ci.

Les différentes caractéristiques de l'entreprise, telles sa taille, sa complexité et son profil de risques, sont alors prises en compte.

Entrent dans le champ d'application des présentes recommandations les compagnies d'assurances exerçant en Suisse. Ces standards minimaux et ces recommandations sont réputés sans incidence sur la relation de droit civil entre les compagnies et leurs clients.

Objectifs et responsabilité

Le Business continuity management est censé préserver la survie de l'entreprise et lui permettre de maintenir et de poursuivre ses activités même en cas d'événements exceptionnels et de situations de crise. On entend par là tous les événements pouvant menacer les activités de l'entreprise, comme :

- une défaillance technique ou humaine,
- des cyberattaques,
- une pandémie,
- des catastrophes naturelles,
- des attaques terroristes.

Le Business continuity management vise à minimiser les conséquences de tels événements et situations sur les plans financier et juridique ainsi qu'en termes d'atteinte à l'image de marque.

Le Business continuity management relève de la responsabilité du conseil d'administration de l'entreprise, lequel peut déléguer ses compétences à la direction générale ou à d'autres services.

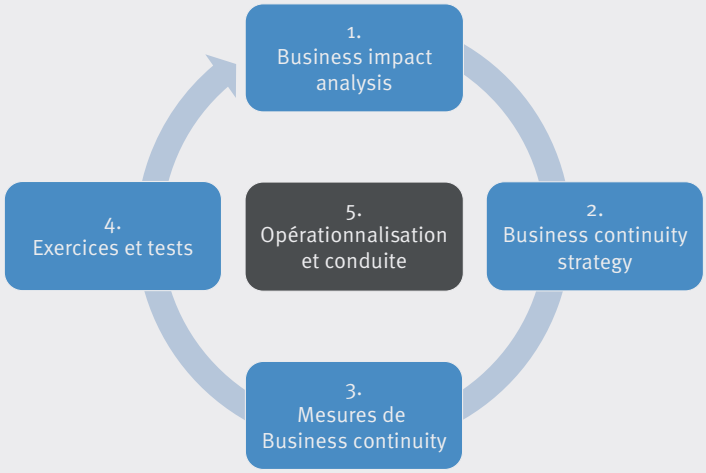
Les standards minimaux précisent les exigences minimales applicables aux compagnies d'assurances exerçant en Suisse.

Les recommandations entendent aider les entreprises à définir le plus précisément possible la manière dont elles souhaitent structurer leur gestion de la continuité des activités.

Fondements

Les présents standards minimaux et recommandations s'appuient sur diverses normes reconnues (cf. les sources indiquées en annexe). Ils reposent notamment sur la norme internationale ISO 22313 : « Societal Security – Business continuity management Systems – Guidance » (Sécurité sociétale – Systèmes de management de la continuité d'activité – Lignes directrices). Conformément à la norme ISO, un Business continuity management doit contenir les éléments de l'illustration suivante pour être complet.

Les éléments du Business continuity management



Champ d'application

Par Business continuity management, il faut entendre une méthode de gestion mise en œuvre à l'échelle de toute l'entreprise. Celle-ci vise à assurer la continuité opérationnelle des processus d'exploitation critiques, leur poursuite ou leur rétablissement dans les meilleurs délais en cas d'événements exceptionnels, internes ou externes, ayant une incidence massive et radicale sur l'activité de l'entreprise, et ce pendant ces événements mêmes et après leur survenance.

Les entreprises doivent prendre en compte l'ensemble des risques et des menaces pouvant potentiellement les mettre dans une situation de crise. On entend par là les situations ne pouvant être maîtrisées par les outils de gestion et les instances décisionnelles ordinaires et risquant de mettre en danger la poursuite des activités de l'entreprise. En conséquence, est expressément exclue du champ d'application du Business continuity management la gestion des « dysfonctionnements » qui ne peuvent perturber l'activité de l'entreprise ni de manière importante, ni de manière durable.

Pour la mise en place du Business continuity management, il faut se concentrer principalement sur les conséquences (incidences des risques résiduels dans le temps) et non sur les causes des situations de crise. Après une interruption de l'activité, il est recommandé de tenir compte, pour le rétablissement des processus et des activités critiques, de différentes options en matière de continuité des activités concernant les ressources indispensables à l'entreprise, à savoir :

- le personnel,
- les infrastructures (par exemple locaux, postes de travail, approvisionnement énergétique),
- les outils techniques, les moyens de télécommunication, l'équipement informatique (données, systèmes) ainsi que
- les prestataires externes.

Le Business continuity management doit garantir le respect optimal des dispositions légales, réglementaires, contractuelles et internes, même en situation de crise.

Standards minimaux

Le Business continuity management d'une compagnie d'assurances doit contenir au minimum les normes prudentielles mentionnées ci-après. Par ailleurs, leur bon respect doit être vérifié périodiquement par le service de révision interne de l'entreprise ou par un organisme indépendant. L'étendue et le degré de précision de ces normes doivent tenir compte des exigences de l'entreprise considérée.

1. Business impact analysis

L'analyse des répercussions sur l'activité, ladite Business impact analysis, comprend l'identification et la classification des processus d'exploitation critiques importants et des ressources nécessaires pour leur bon fonctionnement.

Pour ces processus critiques, sont évaluées les incidences d'une défaillance totale ou partielle des ressources nécessaires, ce qui permet de définir les mesures provisoires et durables requises pour leur bon rétablissement. L'analyse prend en considération les incidences notamment en termes
- d'exploitation (opérations),
- de finances,
- de réputation et
- de compliance.

Cette évaluation intègre aussi les interdépendances pertinentes entre les différents processus (dépendances au niveau des processus).

Il faut procéder à une Business impact analysis au moins tous les trois ans et vérifier sa pertinence au cas par cas (par exemple en présence de nouveaux secteurs d'activités ou en cas d'utilisation de nouvelles technologies).

2. Business continuity strategy

La stratégie de continuité des activités ou Business continuity strategy
- précise les durées maximales admissibles des défaillances ;
- désigne, en s'inspirant de la Business impact analysis, les domaines d'activités qui relèvent du Business continuity management ;
- détermine les différentes approches possibles (options) en cas de crise ;
- fixe l'étendue des mesures de continuité des activités en termes de personnel, de locaux, d'outils techniques, de moyens de télécommunication, d'équipement informatique ainsi que de prestataires externes.

L'acceptation de certaines incidences peut aussi constituer une option : aucune mesure transitoire ni durable n'est alors déterminée pour leur correction. Cela doit être documenté en conséquence dans la Business continuity strategy.

3. Mesures de Business continuity

Sur la base de la Business impact analysis et dans le cadre des prescriptions ressortant de la Business continuity strategy, les mesures relatives à la continuité des activités décrivent la manière dont l'entreprise assume la continuité de ses activités opérationnelles.

Les mesures de continuité des activités spécifient
- les processus et
- les moyens

permettant de surmonter les défaillances temporaires de processus critiques et les ressources alors nécessaires (personnel, locaux, outils techniques, moyens de télécommunication, équipement informatique, prestataires externes) en vue du rétablissement de la situation normale.

Les secteurs concernés et leurs collaborateurs doivent avoir connaissance des mesures de continuité des activités qui ont été définies (par exemple processus critiques surmontés grâce à des changements de postes de travail) et, si nécessaire, avoir reçu les formations correspondantes (par exemple utilisation de systèmes de secours).

4. Exercices et tests

Des exercices et des tests permettent de contrôler et de vérifier la mise en œuvre des mesures indiquées et leur capacité à aider l'entreprise à surmonter les situations de crise.

Il faut spécifier en amont la périodicité des exercices et des tests permettant de mettre à l'épreuve et de vérifier l'efficacité des mesures définies pour la continuité des activités (par exemple redémarrage des systèmes informatiques critiques).

Les résultats des tests doivent être consignés dans des comptes rendus, et les enseignements tirés pris en compte pour ajuster les mesures de continuité des activités.

5. Opérationnalisation et conduite

Le Business continuity management doit être ancré dans l'entreprise (par exemple dans la stratégie ou la politique de l'entreprise) et pris en compte de manière correspondante dans la structure de gouvernance de l'entreprise.

Il faut spécifier une organisation appropriée pour les fonctions et les instances assurant la continuité des activités et œuvrant à la gestion des situations de crise (par exemple organisation de gestion de crise ou état-major de crise). Les rôles, les responsabilités et les compétences de ces différentes fonctions et instances doivent également être indiqués avec précision. Il faut planifier les ressources nécessaires et veiller à ce que les personnes concernées aient suivi les formations appropriées.

La périodicité et le contenu des rapports internes doivent être précisés (par exemple rapports à l'intention de la direction).

Recommandations

Les présentes recommandations s'entendent comme des conseils et des aides pour l'organisation du Business continuity management. Leur application et leur mise en œuvre dépendent notamment de la structure et de la situation de l'entreprise en termes de risques. Elles obéissent aux dispositions précisées dans la Business continuity strategy.

Prescriptions en matière de Business continuity management

Les prescriptions en matière de Business continuity management dans le domaine des outils techniques, des moyens de télécommunication et de l'équipement informatique peuvent être définies par les attentes suivantes (avec précision de leur contenu et des délais impartis) visant le bon rétablissement des processus d'exploitation :

- délai nécessaire jusqu'au rétablissement des processus d'exploitation critiques (Recovery time objective RTO) ;
- niveau de rétablissement souhaité pour les processus d'exploitation critiques en fonction du RTO ;
- perte de données maximale acceptable en cas de crise (Recovery point objective RPO).

Prestations externes

De nombreux processus d'exploitation reposent sur des prestations fournies par des prestataires de services et des fournisseurs externes (outsourcing ou externalisation) qui peuvent, eux aussi, défaillir à court terme. Si des processus d'exploitation critiques impliquent le recours à des prestataires de service et à des fournisseurs externes, il est conseillé d'évaluer leur maturité en termes de Business continuity management dans un cadre approprié.

Il est recommandé de prévoir des solutions de rechange en cas de défaillance de prestataires de services et de fournisseurs externes revêtant une importance critique. Dans le cadre de la planification de la continuité des activités, il est également envisageable de prévoir le transfert de prestataires externes vers des prestataires internes et inversement.

Gestion de crise

Il est recommandé de définir un système de gestion de crise adapté ainsi qu'une communication correspondante qui permettent à l'entreprise de maîtriser efficacement et rapidement des événements exceptionnels. Dans des situations de crise qui exigent des décisions critiques et ne peuvent être maîtrisées à l'aide des mesures et des compétences décisionnelles ordinaires, il faut alors convoquer un collège approprié (par exemple l'état-major de crise ou l'organisation pour les cas d'urgence). Celui-ci prend en charge la gestion de la crise jusqu'au rétablissement d'une situation normale.

Dans un tel cas, les modalités de convocation de l'état-major de crise ou de l'organisation pour les cas d'urgence devraient être réglées en amont et de manière claire, avec précision des responsabilités et des compétences de chacun ainsi que des critères en cas d'aggravation de la situation de crise. L'organisation de crise doit être déterminée en tenant compte de l'activité et de la structure géographique de l'entreprise considérée.

Communication de crise

La communication interne et la communication externe jouent un rôle capital dans la gestion de crise. Il convient donc de veiller à préparer avec soin les concepts et les plans de communication de crise. L'enjeu consiste en particulier à préserver la crédibilité des différentes parties prenantes de l'entreprise et la confiance dont elles bénéficient.

Les plans de communication contribuent essentiellement à garantir l'accessibilité des différents intervenants en cas de crise (liste de noms et coordonnées des clients, médias, collaborateurs, autorités de surveillance, contreparties, prestataires de services, etc.). Ces plans facilitent l'instauration d'une communication régulière et préventive avec les différents groupes d'intérêts (clients, collaborateurs, actionnaires, investisseurs, etc.). Des mesures de communication spécifiques doivent être spécifiées en cas de crise d'envergure potentiellement internationale.

Bilan du Business continuity management

Les Business continuity reviews recensent la documentation relative au Business continuity management et vérifient sa conformité par rapport aux prescriptions définies en matière de continuité des activités. Il est recommandé de fixer des critères de vérification cohérents et de mettre en place un processus clair de surveillance et de suppression des lacunes.

Exercices et tests

Les éléments clés ainsi que la fréquence des différents exercices et tests devraient être déterminés en fonction de l'évaluation du caractère critique des risques conformément à la Business impact analysis ou aux directives internes.

La définition d'un processus de surveillance et de suppression des points faibles peut s'avérer précieuse.

Etablissement des rapports

Les actions menées en matière de Business continuity management ainsi que l'état des mesures préparatoires de gestion de crise devraient faire l'objet de comptes rendus réguliers, par échelon hiérarchique, à l'intention des personnes exerçant des responsabilités. Ces comptes rendus doivent notamment indiquer les résultats des Business continuity reviews ainsi que ceux des exercices et des tests portant sur la continuité des activités.

Les principaux enseignements tirés de ces comptes rendus peuvent être communiqués en interne et en externe (externalisation).

Entrée en vigueur

Les présents standards minimaux et recommandations ont été adoptés par le comité Finances & Régulation de l'Association Suisse d'Assurances ASA en date du 9 juin 2015. Ils entrent en vigueur le 1er octobre 2015 et doivent être mis en œuvre avant le 31 juillet 2017 au plus tard.

La Finma reconnaît les standards minimaux au sens de l'art. 7 al. 3 LFINMA au 23 septembre 2015.

En cas de divergence entre l'original allemand et la traduction française, la version allemande fait foi.

Sources

International Organization for Standardization (ISO, Organisation internationale de normalisation), ISO 22313:2012 : Societal security – Business Continuity Management Systems – Guidance (Sécurité sociétale – Systèmes de management de la continuité d'activité – Exigences)
http://www.iso.org/iso/fr/home/store/catalogue_tc/catalogue_detail.htm?csnumber=50038

International Organization for Standardization (ISO, Organisation internationale de normalisation), ISO/IEC 27031:2011 : Information technology – Security Techniques – Guidelines for Information and Communication Technology Readiness for Business Continuity (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)
http://www.iso.org/iso/fr/home/store/catalogue_tc/catalogue_detail.htm?csnumber=44374

Bundesamt für Sicherheit in der Informationstechnik (BSI, Ministère allemand de la sécurité des techniques de l'information), BSI-Standard 100-4 (Norme BSI 100-4) – Notfallmanagement (Gestion de crise), 2008
www.bsi.bund.de/cae/servlet/contentblob/471456/publicationFile/30746/standard_1004.pdf

Glossaire

Pour les définitions des différentes notions abordées dans le présent document, l'ASA recommande de consulter la norme ISO 22301:2012 Societal security – Business Continuity Management Systems – Requirements (Sécurité sociétale – Systèmes de management de la continuité d'activité – Exigences), chapitre 3 « Termes et définitions ».

ASA | SVV

Association Suisse d'Assurances ASA
Conrad-Ferdinand-Meyer-Strasse 14
Case Postale
CH-8022 Zurich

Tel. +41 44 208 28 28
Fax +41 44 208 28 00
info@svv.ch
www.svv.ch