SwissBanking

Août 2013

Recommandations en matière de Business Continuity Management (BCM)

Sommaire

1 Situation initiale et objectifs

Diverses évolutions constatées ces dernières années, notamment en matière de terrorisme, de pandémies et de catastrophes naturelles, ont souligné la vulnérabilité des acteurs et des systèmes des marchés financiers. La sensibilisation aux événements de ce type et à leurs incidences potentielles s'est fortement accrue.

Aussi existe-t-il au niveau de certaines organisations internationales, mais aussi dans divers pays, des prescriptions et des recommandations en matière de Business Continuity Management (BCM) qui s'imposent à la fois aux acteurs des marchés financiers et aux autorités de surveillance.

L'Autorité fédérale de surveillance des marchés financiers (FINMA) considère qu'un BCM adéquat constitue, pour une banque, une condition préalable à l'autorisation d'exercer son activité au sens de l'art. 3 de la Loi sur les banques. La FINMA soutient l'autorégulation de l'Association suisse des banquiers (ASB).

La présente autorégulation de l'ASB s'adresse aux membres de cette dernière et propose des recommandations (*best practice*) pour la mise en place d'un BCM au sein de chaque Etablissement. A cet égard, il convient de tenir compte des particularités de chaque situation initiale, en particulier en matière de risque, et de l'importance systémique des divers Etablissements.

Trois chapitres des présentes recommandations ont été reconnus par la FINMA conformément à sa circulaire 2008/10 «Normes d'autorégulation reconnues comme standards minimaux» et constituent un standard minimal selon le droit de surveillance, dont le respect est contrôlé par des sociétés d'audit. Sont obligatoires la définition d'une stratégie de Business Continuity Management (chapitre 4.4), l'établissement d'une Business Impact Analysis (chapitre 4.5.1) ainsi que la détermination d'options en matière de Business Recovery (chapitre 4.5.2).

Entrent dans le champ d'application des présentes recommandations les banques et les négociants en valeurs mobilières (ci-après:

Etablissements). Ces recommandations sont réputées sans incidence sur la relation de droit civil entre les Etablissements et leurs clients.

2 Fondements

Les présentes recommandations s'appuient sur diverses normes comparables (cf. également les références complémentaires en Annexe D). Elles reposent notamment sur

- les «High-Level Principles for Business Continuity» du Joint Forum ou du Comité de Bâle sur le contrôle bancaire[1]
- le «British Standard for Business Continuity Management BS 25999»[2] et la norme ISO 22301[3].

Les «High-Level Principles» contiennent les recommandations suivantes:

1. Les acteurs des marchés financiers et les autorités de surveillance doivent disposer d'un BCM complet et efficace. Il appartient au Conseil d'administration (*board of directors*) et à la Direction (*senior management*) de veiller à garantir la Business Continuity.
2. Les acteurs des marchés financiers et les autorités de surveillance devraient intégrer dans leur BCM le risque lié à d'importants dysfonctionnements opérationnels.
3. Les acteurs des marchés financiers devraient développer des objectifs de *recovery* (Recovery Time Objectives, RTO) qui tiennent compte de leur importance systémique, c'est-à-dire du risque qu'ils sont susceptibles de générer pour le système financier.
4. Le Business Continuity Planning des acteurs des marchés financiers comme des autorités de surveillance devrait définir des mesures de communication interne et externe à mettre en œuvre en cas d'interruptions majeures de l'activité.

[1] Comité de Bâle sur le contrôle bancaire, Banque des règlements internationaux, août 2006, www.bis.org.
[2] British Standards Institution, septembre 2008, www.bsigroup.com.
[3] International Organization for Standardization (ISO), mai 2012, www.iso.org.

5. Les plans de communication devraient aussi intégrer la communication avec des autorités de surveillance étrangères, pour le cas où des interruptions de l'activité auraient des répercussions internationales.
6. Les acteurs des marchés financiers et les autorités de surveillance devraient tester leur Business Continuity Planning, évaluer son efficacité et, le cas échéant, adapter leur BCM.
7. Il est recommandé aux autorités de surveillance d'évaluer, dans le cadre de la surveillance courante, le BCM des Etablissements soumis à leur surveillance.

Par ailleurs, il convient de tenir compte des résultats du groupe de travail «PCA au sein de la place financière suisse» qui a identifié, sous l'égide de la Banque nationale suisse (BNS), comme «critiques» les deux processus «traitement des paiements élevés via SIC» et «provision de liquidités via les opérations de pension».[4]

3 Champ d'application et menaces

Les Etablissements doivent envisager toutes les menaces plausibles susceptibles d'entraîner une crise pour l'entreprise. On entend par «crise» une situation de menace nécessitant des décisions critiques et qui ne peut être gérée dans le cadre des processus de gestion et des compétences décisionnelles ordinaires. Dans ce sens, la gestion des «dysfonctionnements» est donc expressément exclue du champ d'application des présentes recommandations (Availability Management, cf. définitions des termes en Annexe A et Annexe B). On peut citer comme exemples de «crises»:

- les événements «à caractère accidentel» (incendies ou explosions p. ex.)
- les attentats terroristes et actes de sabotage
- les catastrophes naturelles (inondations ou tremblements de terre p. ex.).

[4] Banque nationale suisse (BNS), Business Continuity: Situation de la place financière, 2006 et 2009, www.snb.ch.

Or, il est recommandé au sens des *best practice* de se concentrer, pour la mise en place du BCM, principalement sur les conséquences et non sur les causes de crises. Après une interruption de l'activité, il est recommandé, de tenir compte des différentes conséquences pour le rétablissement des processus et des activités critiques selon les objectifs de *recovery* définis dans le cadre des options en matière de Business Recovery (cf. chapitre 4.5.2.).

Dans le cadre du BCM, il appartient aux Etablissements d'identifier, de définir et d'évaluer les types de menaces pertinentes en fonction de leur impact (degré de gravité).

Ces événements peuvent notamment avoir pour conséquence que des collaborateurs et/ou des infrastructures (en particulier locaux ou postes de travail, infrastructures de direction, télécommunications) ne sont plus du tout ou seulement partiellement aptes à remplir des fonctions critiques pour l'entreprise. De même, des problèmes au niveau des services informatiques ou des fournisseurs d'infrastructures peuvent rendre l'exécution de processus d'exploitation critiques impossibles.

S'agissant des pandémies, les scénarios de dommages et les recommandations de l'Office fédéral de la santé publique (OFSP) servent de référence. Les moyens prévus pour faire face à une pandémie doivent tenir compte du fait que les effets d'une maladie infectieuse à large étendue géographique diffèrent significativement, en termes de durée et de prévisibilité du moment de sa survenue, des situations de crise classiques de BCM.

Une situation de crise au sens du BCM

- survient de manière impromptue et entraîne rapidement des conséquences importantes sur l'activité, et
- la stratégie réactive prévue cible le rétablissement de la capacité d'activité dans les meilleurs délais.

Une pandémie, en revanche,

- dure un certain temps en amont avant d'atteindre son point culminant
- et impose une stratégie visant à la continuité des activités critiques et à la suspension de celles moins critiques.

Il est recommandé d'élaborer, au moins au niveau de l'Etablissement, un plan de pandémie. Les informations actuelles à ce sujet sont disponibles sur le site de l'OFSP[5].

De nombreux processus d'exploitation impliquent des prestations par des fournisseurs et des prestataires de service externes 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 BCM Maturity dans un cadre approprié.

Les options en matière de Business Recovery (chapitre 4.5.2) permettent entre autres d'étudier le transfert de prestataires externes vers des prestataires internes. Une autre précaution consiste à prévoir des relations contractuelles avec des fournisseurs redondants ou alternatifs.

En complément à la circulaire de la FINMA 2008/7 «Outsourcing – banques: Externalisation d'activités dans le secteur bancaire», la recommandation au sens de *best practice* stipule de prévoir systématiquement des solutions de rechange pour le cas de défaillance de prestataires ou fournisseurs externes critiques.

Le BCM doit garantir le respect optimal des dispositions légales, règlementaires, contractuelles et internes, même en situation de crise.

[5] Office fédéral de la santé publique (OFSP), Plan suisse de pandémie Influenza, janvier 2009, www.bag.admin.ch.

4 Recommandations

4.1 Définition et étendue

On entend par BCM une méthode de gestion mise en œuvre à l'échelle de l'entreprise, qui vise à assurer la continuité opérationnelle de processus d'exploitation critiques en cas d'événements, internes ou externes, ayant une incidence massive et radicale sur l'activité. Le BCM vise ainsi à minimiser les conséquences de ces événements sur les plans financier et juridique ainsi qu'en termes de réputation.

Globalement, le BCM doit garantir – à un niveau défini en amont – la poursuite ou la reprise rapide de l'activité en situations de crise. Il concerne donc tous les domaines d'activité et toutes les unités organisationnelles d'une entreprise. Il convient de distinguer les mesures de planification au titre du BCM, en amont, et la gestion de crise proprement dite.

4.2 Responsabilités

Le BCM relève de la responsabilité du Conseil d'administration et de la Direction de chaque Etablissement (cf. aussi à cet égard la circulaire de la FINMA 2008/24 «Surveillance et contrôle interne - banques»).

Il incombe au Conseil d'administration de veiller au contrôle du respect de la stratégie de BCM formalisée par écrit. La Direction la met en œuvre et règle les questions liées aux responsabilités, compétences et flux d'informations dans les règlements et les directives internes. La Direction régit notamment (avec l'approbation du Conseil d'administration) les relations entre elle-même et la structure compétente en cas de crise (état-major de crise).

4.3 Analyse des risques

Il est possible, dans le cadre du BCM, d'effectuer une analyse des risques pour les ressources critiques ou de se référer à des analyses des risques existantes d'autres secteurs (p. ex. gestion des risques).

L'analyse des risques dans le contexte du BCM sert à identifier les risques susceptibles d'entraîner une interruption des processus d'exploitation. Le BCM part systématiquement du principe que de tels risques peuvent se produire. Bien que l'identification exhaustive de tous les risques ne soit pas toujours possible, cela permet néanmoins de lister et d'évaluer des risques potentiels. Parfois même, des mesures ciblées permettent d'abaisser la probabilité de survenue d'un scénario de crise à un niveau acceptable.

4.4 Stratégie de Business Continuity Management (standard minimum obligatoire)

Dans sa stratégie de BCM, l'Etablissement définit son approche de principe à ce sujet.

La stratégie de BCM peut faire partie intégrante de la stratégie d'entreprise de l'Etablissement ou être déterminée séparément. Si certains risques résiduels sont sciemment acceptés, la stratégie doit le signaler explicitement. Des décisions à cet égard doivent être consignées par écrit.

La stratégie de BCM doit couvrir et traiter les aspects suivants:

- définition et détermination de la portée du BCM (*scope*)
- ancrage du BCM dans l'organisation de l'entreprise
- création d'une structure de gouvernance adaptée à l'organisation de l'entreprise
- définition des rôles et des responsabilités dans le cadre du BCM
- détermination de menaces potentielles et de leurs incidences sur les ressources de l'entreprise (base de la planification)
- définition de la périodicité d'exécution des reviews et de tests des plans et des mesures
- définition du reporting, de la communication et de la formation.

4.5 Eléments du Business Continuity Management

4.5.1 Business Impact Analysis (standard minimum obligatoire)

La Business Impact Analysis (BIA) fournit les informations nécessaires sur les processus d'exploitation et les ressources critiques pour l'entreprise. Dans le cadre du BCM sont évaluées, pour ces processus critiques, les incidences d'une défaillance totale ou partielle des ressources correspondantes. Il appartient à chaque département des Etablissements de déterminer ses processus et ses ressources critiques.

Cette évaluation intègre aussi les interdépendances entre départements (dites dépendances au niveau des processus) ainsi que les dépendances par rapport à des prestataires et des fournisseurs externes (externalisation).

Cette analyse, qui doit permettre de déterminer les objectifs de *recovery*, devra au moins aboutir à l'identification

- du délai défini jusqu'au rétablissement des processus d'exploitation critiques (Recovery Time Objective, RTO)
- du niveau de rétablissement souhaité pour les processus d'exploitation critiques en fonction du RTO défini
- des ressources (de remplacement) minimales (locaux, collaborateurs, informatique et données informatiques, prestataires et fournisseurs externes) qui doivent être disponibles en cas de crise pour atteindre le niveau de rétablissement souhaité.

La BIA devra faire l'objet d'une révision annuelle en sachant que le type et l'étendue d'une telle révision dépendent notamment de la situation spécifique en matière de risques de l'Etablissement concerné.

4.5.2 Options en matière de Business Recovery (standard minimum obligatoire)

Les options en matière de Business Recovery définissent, au niveau opérationnel, la procédure selon laquelle l'entreprise entend atteindre les objectifs de *recovery* fixés dans la BIA – pour les secteurs d'activité sélectionnés conformément au chapitre 4.5.1 – au regard des scénarios

de menace envisagés et de leurs incidences sur les ressources. Les objectifs de *recovery* doivent faire l'objet d'une documentation écrite et comprendre les options de *recovery* pour les ressources critiques qui y sont définies. Ceci permet de présenter quelles options en matière de Business Recovery sont en principe disponibles à un niveau minimum en cas de défaillances

- du personnel
- des locaux
- de systèmes informatiques ou de l'infrastructure informatique (y compris les systèmes de communication)
- ou de prestataires et fournisseurs externes (externalisation), par exemple dans le domaine des fournisseurs d'information.

Ces options en matière de Business Recovery devront par la suite être formulées concrètement dans le Business Recovery Planning correspondant. Une option en matière de Business Recovery peut consister en l'acceptation d'un risque résiduel, qui devra alors faire l'objet d'une démarche analogue et d'une documentation écrite.

4.5.3 Business Recovery Planning

Le Business Recovery Planning décrit les procédures à suivre, les solutions de remplacement et les ressources de remplacement minimales nécessaires pour maintenir (*continuity*) ou rétablir (*recovery*) les processus d'exploitation critiques (en assurant le respect des prescriptions légales, réglementaires, contractuelles et internes). Ce Planning devra comprendre au minimum les éléments suivants: descriptif du cas (scénario déclencheur), procédure à suivre ou catalogue de mesures précisant les priorités ainsi que les ressources de remplacement nécessaires.

Le Business Recovery Planning devra faire au moins une fois par an l'objet d'une vérification en termes d'actualité et être mis à jour le cas échéant. Des changements importants dans le fonctionnement de l'entreprise (réorganisations, mise en place d'un nouveau domaine d'activité, etc.) peuvent également nécessiter une révision de ce Planning.

4.5.4 Business Continuity Reviews

Les Business Continuity Reviews recensent la documentation BCM établie par les différentes unités organisationnelles et vérifient sa conformité par rapport aux critères définis. Il est recommandé de fixer des critères cohérents et de mettre en place un processus clair de surveillance et de suppression des lacunes.

4.5.5 Business Continuity Tests

Les Business Continuity Tests permettent de tester et de vérifier la mise en œuvre de la planification en matière de Business et IT Disaster Recovery ainsi que la capacité de réaction de l'organisation de gestion de crise. Des éléments clés tels que la cadence des différents tests doivent être définis en fonction de l'évaluation des risques (cf. BIA). La simultanéité des tests de différentes unités organisationnelles permet d'évaluer la capacité d'un Etablissement dans son ensemble à maîtriser des situations de crise.

Il est recommandé de coordonner les différents tests en établissant une planification systématique, de prévoir un reporting des résultats uniforme et de définir un processus de surveillance et de suppression des points faibles.

La planification doit être organisée de manière à vérifier ou à tester au moins une fois par an les mesures les plus importantes (y compris l'organisation de crise).

4.6 Gestion de crise

L'objectif consiste à mettre en place un système de gestion de crise qui permette à l'entreprise de maîtriser efficacement et rapidement les situations de crise. 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, l'état-major de crise est convoqué. Celui-ci prend en charge la gestion de la crise jusqu'au rétablissement d'une situation normale.

Il est recommandé de régler clairement au préalable les modalités de convocation de l'état-major de crise, ses responsabilités et ses compétences ainsi que de préciser l'organisation de crise en tenant compte de l'activité et de la structure géographique de l'Etablissement concerné. Il convient de veiller tout particulièrement et autant que possible à ce que les personnes responsables soient également joignables lorsqu'une situation de crise survient.

4.7 Reporting, communication et formation

4.7.1 Reporting

Les actions menées en matière de BCM ainsi que l'état des mesures préparatoires de gestion de crise, doivent faire l'objet de comptes-rendus réguliers, par échelon hiérarchique, à l'intention du Conseil d'administration et de la Direction. Ces comptes-rendus doivent notamment indiquer les résultats des Business Continuity Reviews et des Business Continuity Tests.

4.7.2 Communication

La communication joue un rôle capital dans la gestion de crise. Il convient donc de veiller à préparer systématiquement et soigneusement des concepts et plans de communication de crise (communication tant interne qu'externe). L'enjeu est notamment de maintenir un niveau élevé de professionnalisme, mais aussi de préserver la crédibilité de l'Etablissement et la confiance des différentes parties prenantes envers ce dernier.

Les plans de communication doivent notamment indiquer les personnes à informer en cas de crise (liste des noms et numéros de téléphone des autorités de surveillance, collaborateurs, médias, clients, contreparties, prestataires de services, etc.). Une communication spécifique doit être prévue en cas de crise d'envergure potentiellement internationale.

En cas de crise et de convocation de l'état-major de crise, l'autorité de surveillance doit être dûment informée.

4.7.3 Formation et sensibilisation

Il convient de veiller à ce que les collaborateurs bénéficient d'une formation suffisante quant à leurs tâches, responsabilités et compétences au titre du BCM. A cet égard, il convient de prendre en compte non seulement la formation des nouveaux collaborateurs, mais aussi la mise à jour régulière des connaissances du personnel en place. La formation des membres de l'état-major de crise doit faire l'objet d'une attention particulière.

En outre, à l'aide d'un programme d'information continue, il convient de faire en sorte que les nouveaux collaborateurs et ceux déjà en place soient sensibilisés en permanence à l'importance du BCM.

5 Entrée en vigueur

Les présentes recommandations ont été adoptées par le Conseil d'administration de l'ASB en date du 24 juin 2013 et approuvées par la FINMA le 12 juillet 2013. Elles entrent en vigueur le 1er octobre 2013 et doivent être mises en œuvre par les Etablissements au plus tard le 30 septembre 2014. Elles remplacent la précédente version des recommandations entrées en vigueur le 1er janvier 2008.

Bâle, le 29 août 2013

Annexe A - Glossaire

Availability Management

Processus intégrant la définition, l'analyse, la planification, la mesure et l'optimisation de tous les aspects influant sur la disponibilité des services informatiques. L'Availability Management fait en sorte que l'ensemble de l'infrastructure informatique (processus, outils, tâches informatiques et autres) soient conformes aux exigences définies dans les Service Level Agreements en termes de disponibilité. Les événements compromettant la disponibilité peuvent être maîtrisés au moyen des processus de gestion et des compétences décisionnelles habituels.

Business Continuity Management (BCM)

Méthode de gestion à l'échelle de l'entreprise (directives et standards) visant à garantir qu'en cas d'événements (internes ou externes), les processus d'exploitation critiques restent opérationnels ou le redeviennent dans les plus brefs délais. Le BCM intègre donc les phases de planification, de mise en œuvre et de contrôles ainsi que l'ensemble de l'environnement requis (services, processus, techniques) pour assurer une disponibilité ininterrompue des processus d'exploitation critiques ou pour pouvoir la rétablir dans un laps de temps prédéfini, après un événement.

Business Continuity Reporting

Fait de rendre compte (y compris au Conseil d'administration et à la Direction) des actions menées en matière de BCM, notamment de l'état des mesures préparatoires de gestion de crise. Le Business Continuity Reporting doit rendre compte en particulier des Business Continuity Reviews et des Business Continuity Tests.

Business Continuity Testing

Contrôle systématique et à intervalles réguliers du Business Continuity Planning, notamment en termes de mise en œuvre, d'efficacité et de mise à jour.

Au cas où l'Etablissement dispose d'une organisation en matière informatique, la planification en matière d'IT Disaster Recovery doit également faire l'objet de tests réguliers.

Business Impact Analysis (BIA)

Processus d'identification et de mesure (quantitative et qualitative) des répercussions que peuvent avoir les interruptions de l'activité ou les défaillances de certains processus et ressources. La BIA comprend notamment l'identification des processus d'exploitation critiques et des ressources nécessaires pour le Business Recovery, effectuée sur la base d'une analyse des dépendances et incidences, ainsi qu'une évaluation et une classification des dommages potentiels.

Business Recovery

Rétablissement de processus ou d'activités spécifiques à la suite d'une interruption à un niveau préalablement défini ou, le cas échéant, mesures à prendre à la suite d'un événement dommageable (cf. Business Recovery Planning). Ceci peut se faire en plusieurs étapes avant la reprise de l'activité régulière ou la restauration de la capacité intégrale.

Business Recovery Planning

Plans exhaustifs de mesures (y compris listes de vérification et outils) préparés à l'avance en vue de permettre la continuité de l'activité ou une reprise structurée et, dans les meilleurs délais, des processus d'exploitation critiques en cas de situation de crise.

Crise

Situation de menace nécessitant des décisions critiques et qui ne peut être gérée dans le cadre de la gestion (outils de gestion, instances décisionnelles) ordinaire de l'Etablissement.

Etat-major de crise (aussi: Crisis Management Team, CMT ou organisation en cas d'urgence)

Equipe responsable de la gestion des situations de crise jusqu'au rétablissement d'une situation normale (minimisation des dommages économiques et des risques de réputation).

Incident

Evènement qui entraîne une interruption des activités, une perte ou une limitation de la qualité des services, mais qui peut être géré dans le cadre de l'Availability Management (contrairement à une crise).

Options en matière de Business Recovery

Définition de la procédure afin d'assurer la continuité de l'activité ou de réagir à la défaillance de ressources critiques (y compris la détermination des risques acceptables, l'analyse d'options d'action et décisions de principe sur la mise à disposition de ressources de remplacement). Les options en matière de Business Recovery s'appuient sur la BIA et constituent la base du Business Recovery Planning.

Processus critiques

Processus d'une entreprise dont l'arrêt est susceptible d'empêcher ou de compromettre notablement le service à la clientèle, le respect des obligations réglementaires de l'entreprise et/ou la gestion des positions à risques, et qui peuvent dès lors entraîner un dommage critique (direct ou indirect).

Recovery Point Objective (RPO)

Perte de données définie comme étant acceptable (au maximum) en cas de crise.

Recovery Time Objective (RTO)

Période définie au cours de laquelle les processus d'exploitation critiques et les systèmes informatiques doivent être rétablis.

Ressources critiques

Ressources d'une entreprise (personnel, locaux, systèmes/données informatiques, prestataires et fournisseurs externes, etc.) qui, en cas de défaillance, entraînent des interruptions ou arrêts de processus d'exploitation (critiques). Les ressources critiques sont identifiées dans le cadre de la BIA.

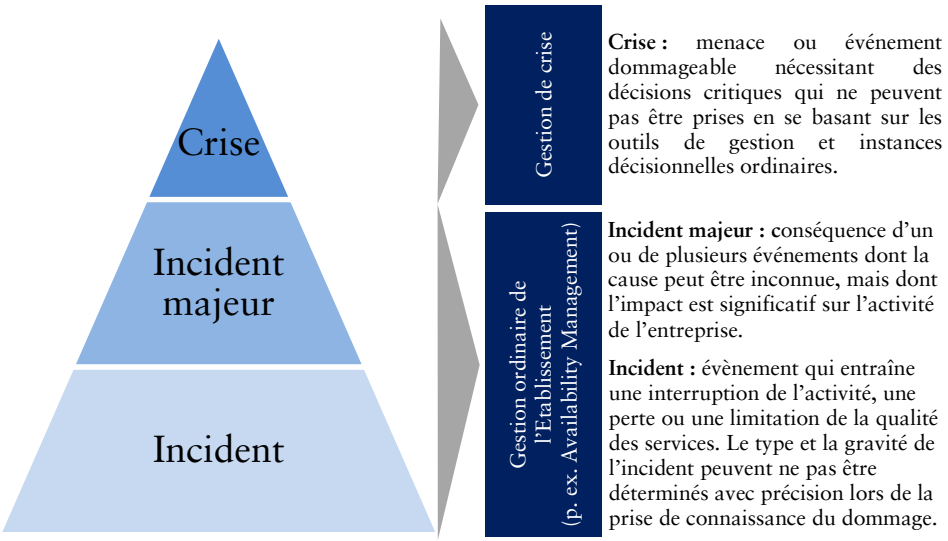
Stratégie de Business Continuity Management

Définition de l'approche de principe en matière de BCM. La détermination de l'entité responsable en matière de BCM, la définition des rôles et responsabilités ainsi que la définition de l'étendue des activités (*scope*) de BCM en font partie.

Toute décision qui s'y rapporte doit être formalisée par écrit.

Annexe B – Degrés de gravité des événements

Selon la gravité des conséquences résultant d'un ou de plusieurs événements, on parle d'incident, d'incident majeur ou de crise. Le BCM ne concerne que la prévention des crises ainsi que la gestion de crise.



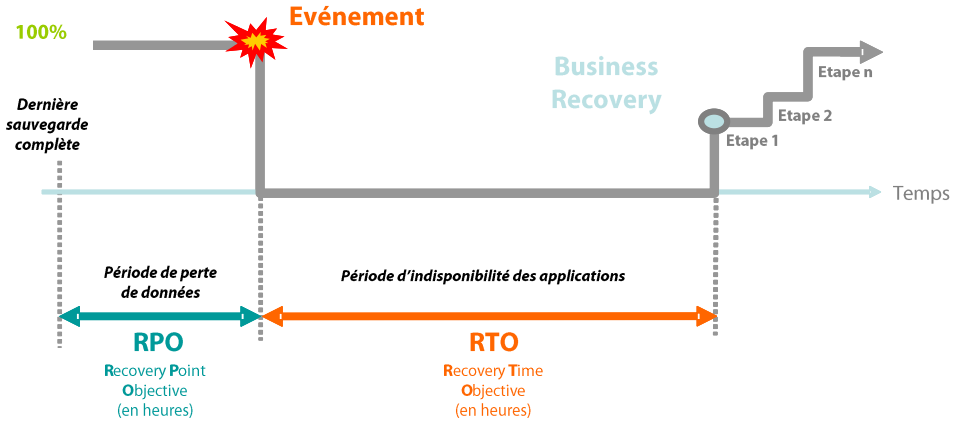
Crise : menace ou événement dommageable nécessitant des décisions critiques qui ne peuvent pas être prises en se basant sur les outils de gestion et instances décisionnelles ordinaires.

Incident majeur : conséquence d'un ou de plusieurs événements dont la cause peut être inconnue, mais dont l'impact est significatif sur l'activité de l'entreprise.

Incident : évènement qui entraîne une interruption de l'activité, une perte ou une limitation de la qualité des services. Le type et la gravité de l'incident peuvent ne pas être déterminés avec précision lors de la prise de connaissance du dommage.

Annexe C – Déroulement d'une crise

Déroulement d'une crise illustré, à titre d'exemple, par un impact du type «Perte de données informatiques»



Annexe D – Sources complémentaires

Dans le cadre de la mise en œuvre d'un BCM, on peut se référer entre autres aux standards suivants (sélection non exhaustive).

Australian Prudential Regulatory Authority (APRA), Prudential Standard APS 232 «Business Continuity Management» et Guidance Note 232,
www.apra.gov.au

Banque nationale suisse (BNS), Business Continuity pour le secteur bancaire suisse, janvier 2006 et septembre 2009,
www.snb.ch/fr/iabout/finstab/id/finstab_bcp

Basel Committee on Banking Supervision (BCBS), High-Level Principles for Business Continuity, Bank for International Settlements, août 2006,
www.bis.org/publ/joint17.htm

British Standards Organisation, Business Continuity Management Standard, BS 25999-2:2007,
www.bsigroup.com/en/Standards-and-Publications/

Bundesamt für Sicherheit in der Informationstechnik, BSI), BSI-Standard 100-4 – Notfallmanagement, 2008,
www.bsi.bund.de/cae/servlet/contentblob/471456/publicationFile/30746/standard_1004.pdf

Business Continuity Institute, The BCI Good Practice Guidelines 2008 ou 2010,
www.thebci.org/

Federal Reserve System (Fed), Interagency Paper on Sound Practices to Strengthen the Resilience of the U.S. Financial System, 2003,
www.federalreserve.gov

Financial Services Authority (FSA), Business Continuity Management Practice Guide, novembre 2006,
www.fsa.gov.uk/pubs/other/bcm_guide.pdf

Information Security Forum, Aligning Business Continuity and Information Security, mars 2006,
www.securityforum.org

International Organization for Standardization (ISO), ISO/IEC 27031:2011: Information technology – Security techniques – Guidelines for information and communication technology readiness for business continuity,
www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=44374

International Organization for Standardization (ISO), ISO 22301:2012: Societal security – Business continuity management systems – Requirements,
www.iso.org/iso/catalogue_detail?csnumber=50038

Office fédéral de la santé publique (OFSP), Plan de pandémie – Manuel pour la préparation des entreprises, novembre 2007,
www.bag.admin.ch/influenza/01120/01134/03058/04319/index.html?lang=fr

Office fédéral de protection de la population (OFPP), Analyses des risques et des dangers et protection de la population – une étude sur les travaux en cours dans les cantons, mars 2011,
www.bevoelkerungsschutz.admin.ch/internet/bs/fr/home/dokumente/Unterlagen_Risiken.html

Association suisse des banquiers
Aeschenplatz 7
Case postale 4182
CH-4002 Bâle
T +41 61 295 93 93
F +41 61 272 53 82
office@sba.ch
www.swissbanking.org