Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Département fédéral de la défense,
de la protection de la population et des sports DDPS

Office fédéral de la protection de la population OFPP

Guide pour la protection des infrastructures critiques

Impressum

Editeur

Office fédéral de la protection de la population
Monbijoustrasse 51a
3003 Berne

Vos suggestions et commentaires sont les bienvenus; veuillez les envoyer par courriel à ski@babs.admin.ch. L'Office fédéral de la protection de la population vous en remercie d'avance.

Vous trouverez des informations complémentaires sur le programme de protection des infrastructures critiques sur notre site web: www.infraprotection.ch

Contrôle de version

Version	Date	Description
1.0	30.05.2015	
1.1	17.12.2018	Adaptation de l'échelle de classification des dommages; diverses modifications rédactionnelles (notamment en lien avec la mise à jour de la stratégie PIC)

Clause de non-responsabilité

Table des matières

Condensé

On entend par infrastructures critiques les processus, les systèmes et les installations qui sont essentiels pour le bon fonctionnement de l'économie ou le bien-être de la population. Il s'agit par exemple de l'approvisionnement en énergie, du transport de personnes et de biens ou encore des soins médicaux. Des perturbations graves de l'approvisionnement en électricité, du trafic ferroviaire ou de l'approvisionnement en denrées alimentaires pourraient provoquer des dommages importants. Un des objectifs principaux de la stratégie nationale pour la protection des infrastructures critiques, que le Conseil fédéral a adoptée en 2012 et mise à jour en 2017, est de vérifier et d'améliorer la résilience (capacité de résistance et de rétablissement) des infrastructures critiques. Le présent guide décrit la procédure correspondante.

L'objectif premier de ce guide est d'éviter autant que possible les dérangements graves et, en cas d'événement, d'en réduire la durée. En outre, le guide doit contribuer à améliorer la gestion et la compréhension des risques qu'encourent les infrastructures critiques.

Du point de vue de la méthode, le présent guide reprend les concepts courants et reconnus de la gestion des risques, des crises et de la continuité des activités, dont il combine différents éléments pour obtenir une *protection intégrale*. Il se fonde sur des planifications et des travaux qui existent déjà et sont utilisés en maints endroits au niveau de l'entreprise. Lorsqu'on change d'échelle pour les appliquer au domaine de la protection des infrastructures critiques, la question n'est plus de savoir ce qui est bon *pour l'entreprise* mais dans quelle mesure des défaillances ou des dérangements des infrastructures critiques portent atteinte à *la population et à ses bases d'existence (économiques)*.

Le présent guide aidera à examiner les risques et à identifier les lacunes éventuelles. Il n'a toutefois pas pour but d'offrir une protection absolue et inconditionnelle contre l'ensemble des menaces.

Ce guide entend plutôt proposer une approche fondée sur les risques, dont le but est que le coût des éventuelles mesures supplémentaires reste proportionnel au bénéfice que l'on peut en retirer. Cette approche devra aussi permettre d'éviter toute inégalité de traitement ou toute distorsion du marché au sein d'un secteur ou entre les différents secteurs concernés.

D'une manière générale, la mise en œuvre du guide PIC requiert une étroite collaboration entre les exploitants des infrastructures critiques d'une part et les autorités compétentes et organes de surveillance et de régulation à l'échelon fédéral, cantonal ou communal d'autre part. Ceux-ci sont responsables de la mise en place, dans les domaines concernés, de conditions-cadres permettant le fonctionnement des infrastructures critiques. Dans les différents domaines politiques (politique énergétique, politique des transports, santé publique, etc.), il conviendra également de définir clairement les conditions de la mise en œuvre et du financement des mesures de protection supplémentaires qui peuvent s'avérer nécessaires dans certaines circonstances.

Cependant, les exploitants ont aussi la possibilité de mettre en œuvre le présent guide sans intervention des autorités. Ils peuvent ainsi vérifier si des risques de défaillances susceptibles d'affecter la société ou l'économie pourraient représenter un danger existentiel pour la survie de l'entreprise.

1 Introduction

1.1 Contexte

Infrastructures critiques

Les infrastructures critiques[1] (IC) garantissent la disponibilité de biens et services importants comme l'énergie, la communication ou les transports. Le dérangement, la défaillance ou la destruction des infrastructures critiques peut avoir des conséquences graves sur la population et ses bases d'existence.

Les infrastructures critiques sont subdivisées en secteurs et en sous-secteurs (p. ex. approvisionnement en électricité, en pétrole et en gaz naturel dans le secteur de l'énergie)[2]. A l'intérieur des sous-secteurs critiques, on considère en principe que *tous* les éléments ou objets (p. ex. exploitants, installations, systèmes, etc.) sont des composants d'infrastructures critiques; il est toutefois évident qu'ils n'ont pas tous la même importance (ou criticité)[3].

Stratégie nationale PIC

Le 8 décembre 2017, le Conseil fédéral a approuvé la stratégie nationale pour la protection des infrastructures critiques 2018-2022 (PIC)[4]. Celle-ci remplace la stratégie nationale de 2012. La stratégie nationale 2018-2022 fixe les principes directeurs, les définitions, les objectifs et les mesures permettant d'assurer une protection complète des infrastructures critiques de la Suisse. Elle sert de cadre de référence à toutes les instances aux niveaux de la Confédération, des cantons, des communes et des exploitants travaillant dans le domaine spécifique de la PIC.

Au total, la stratégie englobe 17 mesures, dont la tenue d'un inventaire des infrastructures critiques mis à jour périodiquement (inventaire PIC). D'autres mesures concernent par exemple l'élaboration de planifications préventives des interventions par les partenaires de la protection de la population et l'armée. La vérification et l'amélioration de la résilience des infrastructures critiques constituent l'un des axes principaux de la stratégie. En effet, avec la mesure M1, le Conseil fédéral a chargé les exploitants d'infrastructures critiques d'étudier la résilience (capacité de résistance et de rétablissement) des infrastructures critiques et de l'améliorer au besoin. Le présent guide est conçu comme une aide à la mise en œuvre de cette stratégie, qui montre les points à respecter et la manière de procéder. Outre les tâches attribuées aux exploitants, le Conseil fédéral a également chargé les autorités compétentes, les organes de surveillance et les organes de régulation au sein des différents secteurs de vérifier s'il existe des risques d'incidents graves dans les sous-secteurs et, si besoin, de prendre des mesures en vue de les limiter. Cela implique de mettre en œuvre une procédure qui ressemble beaucoup à celle du guide PIC.

Travaux préliminaires

Dans différents sous-secteurs, il existe déjà des prescriptions et des planifications destinées à la protection des infrastructures critiques; en règle générale, elles ne se rapportent toutefois qu'à certains aspects comme la protection contre les dangers émanant des infrastructures elles-mêmes, la sécurité des produits, la sécurité d'approvisionnement à long terme, la protection contre des menaces particulières, etc.). Poursuivant un objectif de *protection intégrale*, ce guide présente un éventail global des menaces ainsi qu'une liste complète des mesures. Il prend donc en compte l'ensemble des dangers *significatifs* pouvant entraîner des défaillances

---

[1] Pour des explications détaillées de ce terme, cf. → Glossaire.

[2] Vue d'ensemble proposée à l'Annexe 7 – Secteurs et sous-secteurs critique .

[3] Par conséquent, il n'est pas possible de faire de distinction critique/non critique au sein des sous-secteurs. Dans le sous-secteur de l'approvisionnement en électricité par exemple, les quelque 900 entreprises d'approvisionnement doivent en principe être considérées comme des exploitants d'IC, même si leur importance diffère: tandis que certaines jouent un rôle au plan national, d'autres (et c'est le cas de la plupart) n'ont qu'une envergure communale ou locale.

[4] La Stratégie nationale pour la protection des infrastructures critiques 2018-2022 (FF 2018 491-528) est disponible sur le site web de la PIC, à l'adresse www.infraprotection.ch.

ou des dérangements. La liste des mesures contient quant à elle l'ensemble des mesures *adéquates*, du point de vue architectural, technique et organisationnel, visant à empêcher les défaillances ou à en réduire la durée en cas d'événement. Les exploitants d'infrastructures critiques disposent en principe eux aussi de planifications complètes concernant la protection et la sécurité de leur entreprise. Ainsi, le droit des obligations, des sociétés ou des sociétés anonymes contraint par exemple de nombreuses entreprises à mettre en place une gestion efficace des risques ou un système de contrôle interne (SCI). Un grand nombre d'entre elles disposent aussi de planifications destinées à garantir la continuité des activités (Business Continuity Management, BCM). Le présent guide est orienté méthodiquement vers ces processus et permet de prendre en considération les tâches requises (cf. chapitre 2) afin de réduire considérablement l'investissement pour les entreprises. Les prescriptions, conventions, mesures, etc., déjà en vigueur sont relevées précisément dans le cadre des travaux préparatoires (cf. chap. 3.1.3) et prise en compte dans l'analyse des risques. Si un grand nombre de mesures de sécurité ont déjà été prises, les risques seront moindres, et la nécessité de prendre des mesures supplémentaires également.

1.2 Guide PIC

Genèse

Le guide a été rédigé en étroite collaboration avec le groupe de travail interdépartemental PIC (GT PIC)[5], au sein duquel sont représentés 26 organes fédéraux et deux cantons. Un groupe d'experts des domaines de la gestion des risques, des situations d'urgence, des crises et de la continuité des activités a accompagné son élaboration.

En septembre 2011 s'est en outre tenu un atelier avec la participation de l'EPF de Zurich, au cours duquel des experts des domaines cités ci-dessus ainsi que des représentants de l'économie privée, du milieu scientifique et d'associations diverses ont testé et évalué le guide.

En 2012 et 2013, le document a été soumis à d'autres tests pour définir son aptitude à être utilisé dans la pratique, en collaboration avec un exploitant d'IC de chacun des sous-secteurs examinés; le contrôle a porté d'abord sur un objet critique concret, ensuite sur les principaux processus de l'entreprise, le tout sur une période de plusieurs mois.

Au printemps 2014, le guide a enfin été soumis, à titre de consultation technique, aux associations professionnelles, aux exploitants d'IC, aux conférences cantonales, ainsi qu'une nouvelle fois au GT PIC.

Objectif

Le présent *Guide pour la protection des infrastructures critiques* est un outil permettant de vérifier et, si nécessaire, d'améliorer la résilience des infrastructures critiques. Il a plus particulièrement été conçu pour être utilisé au niveau des sous-secteurs critiques et de l'exploitation des objets répertoriés dans l'inventaire PIC[6].

Ce guide doit contribuer à réduire la probabilité de dérangements ou défaillances de grande ampleur et de longue durée touchant les infrastructures critiques et, en cas d'événement, à

---

[5] Organes fédéraux: Chancellerie fédérale (ChF), Division politique de sécurité (DPS - DFAE), Direction du développement et de la coopération (DDC), Office fédéral de la santé publique (OFSP), Office fédéral de météorologie et de climatologie (MétéoSuisse), Office fédéral de la police (fedpol), Politique de sécurité (POLSEC DDPS), Service de renseignement de la Confédération (SRC), Protection des informations et des objets (PIO), Commandement des opérations, armasuisse Immobilier (ar Immo), Office fédéral de la protection de la population (OFPP), Administration fédérale des finances (AFF), Office fédéral des constructions et de la logistique (OFCL), Office fédéral de l'informatique et de la télécommunication (OFIT), Unité de pilotage informatique de la Confédération (UPIC, organe de coordination de la stratégie nationale de protection contre les cyberrisques), Office fédéral pour l'approvisionnement économique du pays (OFAE), Office fédéral des transports (OFT), Office fédéral de l'aviation civile (OFAC), Office fédéral de l'énergie (OFEN), Office fédéral des routes (OFROU), Office fédéral de la communication (OFCOM), Office fédéral de l'environnement (OFEV), Commission fédérale de l'électricité (ElCom), Inspection fédérale de la sécurité nucléaire (IFSN). Cantons: canton de Genève, canton de Bâle-Ville.

[6] L'inventaire PIC répertorie les objets revêtant une importance stratégique pour la Suisse. Il offre entre autres une vue d'ensemble comparative de l'importance des objets et sert de base pour la planification et les décisions relevant de la gestion des risques, des crises et des catastrophes aux niveaux de la Confédération, des cantons et des exploitants. L'inventaire PIC est classé SECRET dans son intégralité. Des extraits de l'inventaire sont en principe classés CONFIDENTIELS.

limiter les dommages et la durée des perturbations. Le but est que toutes les IC soient protégées de manière optimale. Autrement dit, les mesures en œuvre doivent correspondre aux risques que représentent ces IC. On ne vise pas une protection contre tous les risques, ce qui irait à l'encontre des principes de gestion des risques et de proportionnalité exposés dans la stratégie nationale PIC.

Il doit en outre améliorer la gestion et la compréhension des risques qu'encourent les infrastructures critiques.

Les connaissances acquises grâce aux procédés présentés dans ce guide seront utilisées pour la planification et l'adaptation des mesures de protection lacunaires ou insuffisantes et prises en compte dans les structures de gestion des risques, des situations d'urgence, des crises et de la continuité des activités qui existent déjà au sein de l'entreprise.

Destinataires

La protection des infrastructures critiques est une mission qui incombe à la collectivité et nécessite une étroite collaboration entre les exploitants d'IC d'une part et les autorités compétentes et organes de surveillance et de régulation de chacun des domaines d'autre part. Le guide s'adresse donc aux deux parties, qui peuvent toutes deux être les initiatrices de sa mise en œuvre:

1. les exploitants d'IC, qui sont responsables de garantir un fonctionnement aussi continu que possible de leurs installations et souhaitent mettre en œuvre le guide de leur propre chef;
2. les autorités compétentes à l'échelon fédéral, cantonal ou communal auxquelles la législation attribue un mandat de pilotage ou de surveillance des infrastructures critiques. Le guide peut les aider à déterminer s'il existe des risques pour la société et l'économie qui nécessitent que les autorités prennent des mesures législatives, régulatrices ou autres.

Etant donné que les différentes mesures de protection des infrastructures critiques peuvent être extrêmement onéreuses, il est fortement recommandé de chercher à collaborer avec d'autres exploitants d'IC en vue de la mise en œuvre du guide et plus particulièrement de l'évaluation des mesures envisagées. En renforçant la coopération, c.-à-d. en alliant ses forces pour créer et utiliser des ressources communes ou renforcer la coopération en cas d'événement (p. ex. sous la forme d'une organisation de crise commune), il est possible de réduire les risques à un coût plus raisonnable et avec davantage d'efficacité. Les associations sectorielles peuvent jouer un rôle essentiel dans la coordination des travaux entrepris en ce sens.

Une plus-value pour les exploitants d'IC

Pour les exploitants d'IC, l'utilisation du guide à différents niveaux génère une plus-value en termes de protection des IC:

- Le guide crée des bases décisionnelles pour une affectation efficace des ressources (investissement minimal pour une augmentation maximale de la sécurité).
- Il aide les exploitants à expliciter les prestations qu'ils fournissent à la population et à l'économie et à évaluer les mesures visant à garantir ces prestations de concert avec les autorités compétentes.
- Il favorise l'unité de doctrine et la compatibilité des mesures en matière de protection intégrale au sein des branches professionnelles et entre les différentes branches.
- Grâce à la mise en œuvre du guide à grande échelle, la disponibilité élevée des infrastructures critiques en Suisse est garantie en permanence, ce dont profitent notamment les entreprises (promotion de la place économique).

Positionnement

Le présent guide ne remplace ou n’annule aucune prescription en vigueur concernant la protection des infrastructures critiques. Il fait office de complément aux travaux existants ou en cours d’élaboration dans ce domaine. Il se rapporte méthodiquement aux systèmes de gestion existants (cf. chapitre 2). La mise en place de systèmes et outils supplémentaires en parallèle est à éviter.

2 Conditions préalables

2.1 Points de convergence avec des systèmes de gestion établis

Le présent guide possède des points de convergence avec différents systèmes de gestion généralement établis au niveau de l'entreprise; on relèvera par exemple les éléments suivants:

- gestion de la sécurité
- gestion des risques
- gestion de la continuité des affaires (anglais: *Business Continuity Management,* BCM)
- gestion des crises
- gestion des situations d'urgence
- système de contrôle interne (SCI)

Les systèmes de gestion en question sont définis de diverses manières dans les différents standards, normes et ouvrages existants. Indépendamment de l'organisation, les différents systèmes sont soit traités individuellement, soit considérés comme des parties intégrantes d'un système plus vaste. Il est primordial que chacun des composants aborde différents aspects qui se complètent mutuellement avec pertinence afin d'améliorer la sécurité de l'entreprise, afin de contribuer à réduire la probabilité et l'ampleur des défaillances. Tous les aspects de la sécurité de l'entreprise doivent être pris en compte si l'on veut établir une sécurité globale, mais il est du ressort de l'organisation de déterminer comment les différents systèmes s'articulent entre eux.

Le présent guide n'a ni la volonté ni le droit de donner une définition des systèmes valable à titre général; il n'en fixe pas non plus les frontières. Toutefois, afin de rendre plus compréhensibles le guide et l'interaction des différents composants, une brève explication des systèmes de gestion cités ci-dessus, prenant en considération une sélection de définitions, sera fournie dans le glossaire du présent document.

Systèmes de gestion spécialement importants pour la PIC

Parmi les systèmes de gestion mentionnés ci-dessus, la gestion des risques (aspect « Prévention des événements ») et la gestion de la continuité des activités (aspect « Préparation aux événements ») revêtent une importance toute particulière. Comme il existe des définitions et conceptions différentes de ces systèmes de gestion et de la distinction qu'il convient d'établir entre eux, aucune définition de ces deux termes ne sera proposée dans ce guide. Les principales normes et directives s'y référant sont en revanche mentionnées ci-dessous, à titre de source d'information pour les organes intéressés.

Secteur thématique	Documents de référence
Gestion des risques	*Instructions et remarques pour la mise en place d'un système de gestion des risques:* *- ISO 31000 Management du risque* *- ONR 49001 ss, mise en œuvre de la norme ISO 31000 dans la pratique* *- HB 436:2004 Risk Management Guidelines Companion to AS/NZS 4360:2004* *- Handbuch zum Risikomanagement Bund (manuel de la Confédération pour la gestion des risques, disponible uniquement en allemand)*
Mesures visant à garantir la continuité des activités	*Instructions et remarques pour la mise en place d'un système de gestion de la continuité des activités:* *- ISO 22301: Sécurité sociétale – Systèmes de management de la continuité d'activité – Exigences* *- ISO 22313: Sécurité sociétale – Systèmes de management de la continuité d'activité – Lignes directrices. Première édition, 15 décembre 2012* *- BS 25999-2* *- BCI Good Practice Guidelines 2013* *- Guide BCM de l'Office fédéral pour l'approvisionnement économique (« Ma petite entreprise / connaît pas la crise... »)* *- HB 221/2004 Business Continuity Management (basé sur AS/NZS)*

Tableau 1: Documents de référence par secteur thématique

2.2 L'approche du guide

Avoir un angle plus large

L'utilisation du guide ne doit pas provoquer l'introduction d'un nouveau système de gestion dans l'entreprise mais plutôt s'appuyer sur les systèmes existants et augmenter l'importance accordée à la protection des infrastructures critiques (PIC). Tandis que les systèmes de gestion traditionnels mettent l'accent sur les risques encourus par l'entreprise ou l'organisation, dans le cadre de la PIC, ce sont les risques pour la population et ses bases d'existence qui jouent les premiers rôles.

*Les **bases d'existence** sont l'ensemble des éléments dont la population a besoin pour vivre. Elles rendent possible la vie en commun aux niveaux collectif et individuel. Elles peuvent être réparties en trois catégories:*

- *bases naturelles d'existence:*
  environnement intact (sols, eaux, air, biodiversité);
- *bases économiques d'existence:*
  prospérité économique et infrastructures en état de fonctionnement;
- *bases sociales d'existence:*
  systèmes de droit, de santé publique, de recherche scientifique et de formation qui fonctionnent, confiance de la population dans les institutions étatiques, intégrité territoriale et diversité culturelle.

Lorsque des systèmes de gestion des risques (pour l'entreprise) et de la continuité des activités sont en place, les processus et les risques ayant une importance cruciale pour la santé (généralement financière) de l'entreprise occupent le devant de la scène. Le guide PIC donne par contre la priorité aux processus et risques essentiels pour la collectivité. Il est évidemment possible que ces deux aspects se chevauchent parfois, mais les cas où ils coïncident en tous points restent extrêmement rares.

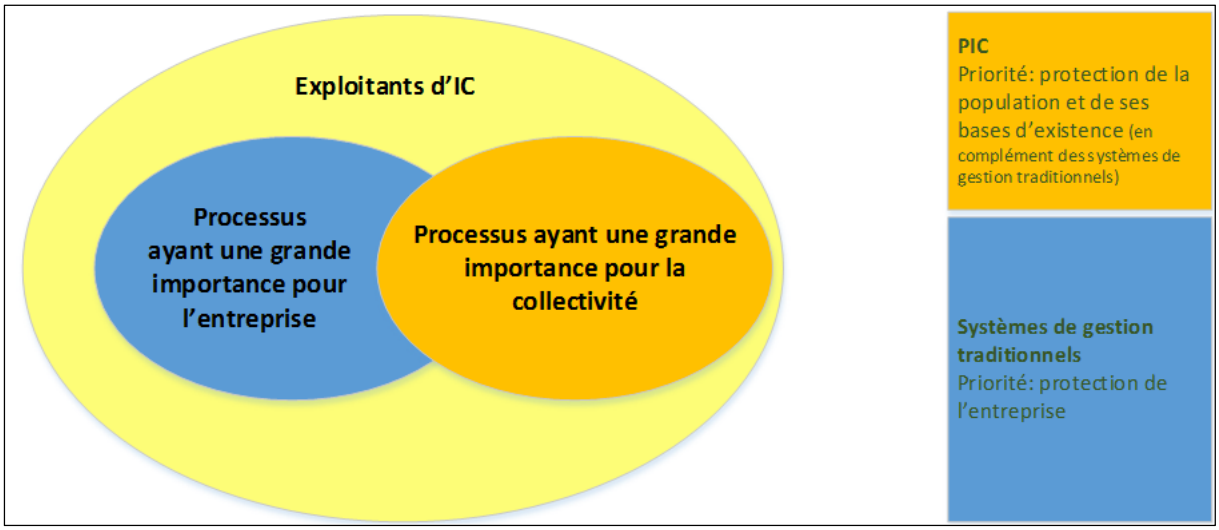


Illustration 1: La PIC en complément aux systèmes de gestion existants au sein de l'entreprise. – Les outils restent les mêmes, le plan de référence est élargi.

Exemple: Pour de nombreuses entreprises, les processus et les risques relatifs à l'encaissement sont de la plus haute importance. En cas de défaillance à ce niveau, la population et l'économie ne sont pas directement touchées. Par contre, un processus du domaine de l'approvisionnement de base (économiquement parlant) insignifiant du point de vue de l'entreprise est essentiel pour l'économie concernée et la population.

Par conséquent, si le guide PIC s'appuie sur les mêmes instruments que la gestion des risques et de la continuité des activités au niveau de la méthode, il ne peut toutefois pas être assimilé à ces systèmes.

2.3 Rôles et collaboration

La mise en œuvre du guide PIC requiert une étroite collaboration entre exploitants et autorités compétentes à l'échelon fédéral, cantonal et éventuellement communal. L'importance des différentes associations sectorielles n'est pas non plus négligeable. On distinguera au minimum les rôles suivants:

Rôle	Fonction
Exploitant d'IC	➢ Responsabilité de la mise en œuvre du guide ➢ Apport de la connaissance de l'entreprise ➢ Mise en œuvre des mesures dans l'exploitation
Associations sectorielles	➢ Coordination et représentation des intérêts des exploitants ➢ Ev. collaboration à la recherche de solutions propres à la branche
Autorités	➢ Recommandation aux exploitants d'IC d'utiliser le guide PIC ➢ Accompagnement / soutien socio-politique du processus ➢ Réglementation de la mise en œuvre et financement des éventuelles mesures supplémentaires

Tableau 2: Rôles et fonctions

Il est opportun que les autorités collaborent et que des échanges se fassent au sein d'une même branche et entre les branches apparentées pour les raisons suivantes:

- En général, dans les différents sous-secteurs critiques, plusieurs exploitants d'IC sont visés par les prescriptions du guide PIC. Les associations sectorielles concernées facilitent la coordination et la représentation des intérêts des exploitants face aux autorités compétentes et aux organes de surveillance et de régulation. En outre, les éventuelles mesures supplémentaires peuvent parfois être réglées dans le cadre des solutions proposées par les branches (p. ex. sous forme de collaboration améliorée ou d'aide mutuelle en cas d'événement) et l'investissement pour chaque entreprise s'en trouve réduit (tant pour ce qui est de la mise en œuvre du guide que pour les éventuelles mesures supplémentaires).
- Des mesures de protection des infrastructures critiques adéquates peuvent rapidement faire voler en éclats le cadre dans lequel travaille l'exploitant d'IC en termes de fonctionnement de l'entreprise ou de gestion. En intégrant les associations sectorielles et les autorités compétentes, on garantit le financement dans le cadre du domaine politique concerné (p. ex. politique énergétique, politique des transports, etc.).

3 Protection intégrale des infrastructures critiques

La procédure garantissant une protection intégrale des infrastructures critiques se fonde sur un processus systématique et continu (voir Illustration 2):

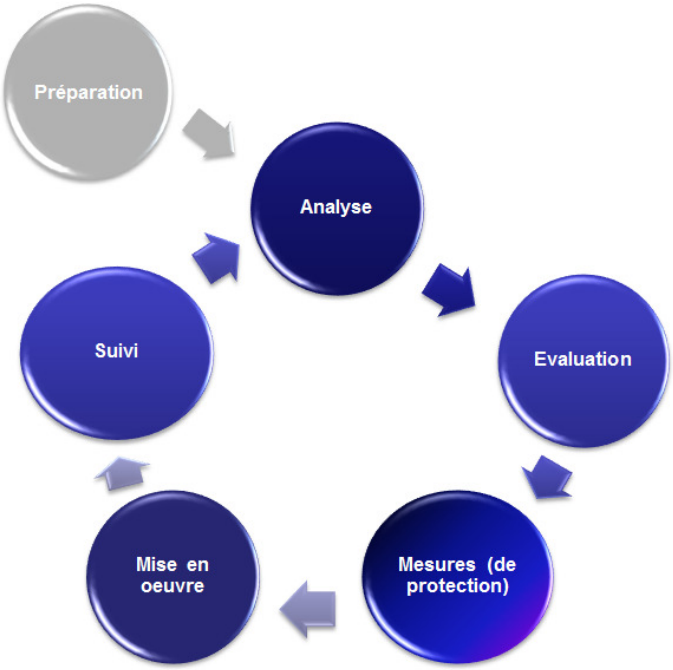


Illustration 2: Processus de protection intégrale des infrastructures critiques

Après une phase de préparation consistant à définir les responsabilités, attribuer les compétences et assigner les mandats, le processus d'amélioration de la protection des infrastructures critiques se répète selon cinq phases:

Durant la phase 1, on identifie les processus critiques et on analyse les menaces pour en déduire les risques de défaillance de ces processus. Les risques sont ensuite relevés et comparés les uns aux autres.

La phase 2 consiste à estimer les risques et les vulnérabilités.

Au cours de la phase 3, on évalue les mesures qui permettent de réduire efficacement les risques.

La phase 4 est celle de la mise en œuvre des mesures. On y démontre comment les mesures peuvent être planifiées, exécutées, accompagnées et surveillées.

La phase 5 (suivi) est consacrée à la vérification, au contrôle et à l'amélioration des mesures. Elle consiste à observer en continu les progrès de la mise en œuvre et l'efficacité des mesures.

3.1 Préparation

Une bonne préparation crée des conditions optimales pour que l'utilisation du guide PIC soit couronnée de succès. Avant de commencer élaborer le guide, des questions fondamentales ont dû être résolues, notamment en ce qui concerne l'attribution des mandats, la composition et l'organisation d'un groupe de travail (GT), la définition des compétences et la mise à disposition des ressources nécessaires pour ces travaux.

3.1.1 Appui des dirigeants et attribution des mandats

Etant donné l'importance et l'étendue des conséquences découlant des décisions à prendre, il est essentiel que l'organe directeur de l'entreprise (comité directeur, conseil d'administration ou autre) soutienne la mise en œuvre du guide. C'est en effet à lui de faire en sorte que toutes les divisions de l'entreprise fonctionnent comme il se doit, en adéquation avec les objectifs poursuivis. Il doit aussi s'assurer que les risques soient identifiés et réduits, et que les répercussions d'un éventuel sinistre sur son entreprise soient minimes.[7]

Même lorsque, dans le cadre de la mise en œuvre du guide, des tâches sont confiées à d'autres personnes ou unités organisationnelles qui assument dès lors la responsabilité de leur mise en œuvre, la responsabilité générale – qui ne saurait être déléguée – reste celle de l'organe directeur. Ce dernier doit faire le nécessaire pour que des ressources suffisantes (personnel, temps, moyens financiers) soient mises à disposition pour la mise en œuvre du guide.

L'organe directeur interne à l'entreprise est chargé d'établir un mandat clair pour la mise en œuvre du guide, qui définira les points suivants:

- l'importance du projet pour l'exploitant d'IC;
- les objectifs du projet;
- le champ d'application du projet;
- la structure du groupe de travail composé pour mener à bien le projet, avec les principaux rôles et leurs compétences;
- les ressources à disposition (temps, personnel, moyens financiers, etc.).

3.1.2 Recensement des travaux existants

Dans le vaste domaine de la protection des infrastructures critiques, il existe une multitude de travaux qui traitent des différents aspects de la PIC. La mise en œuvre du guide PIC s'appuie fortement sur les travaux et planifications disponibles. Voici des exemples de travaux existants:

Travaux existant à l'interne:

- études réalisées dans les domaines de la gestion des risques, gestion des situations d'urgence, gestion de crise et gestion de la continuité des activités,
- systèmes de gestions implémentés, y compris paysage des processus,
- instruments et outils de conduite implémentés,
- prescriptions, directives et normes internes;

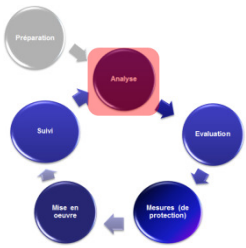
Travaux existants à l'externe:

- bases légales et prescriptions,
- normes et solutions sectorielles,
- normes, directives et guides pour les mettre en œuvre,
- stratégie nationale PIC, inventaire PIC et structures fonctionnelles élaborées dans ce contexte (contient entre autres des indications relatives aux processus et éléments critiques),

[7] Lire à ce sujet l'art. 55 du Code des obligations.

- rapports et études spécifiques au sous-secteur, traitant de la manière d'éviter les défaillances et de réduire les dommages lorsqu'elles se produisent malgré tout.

3.2 Analyse



La phase d'analyse consiste à décrire les processus critiques, à identifier les menaces significatives et les vulnérabilités et à déterminer les risques qui en résultent.

Le schéma suivant présente clairement les différentes étapes de cette phase:

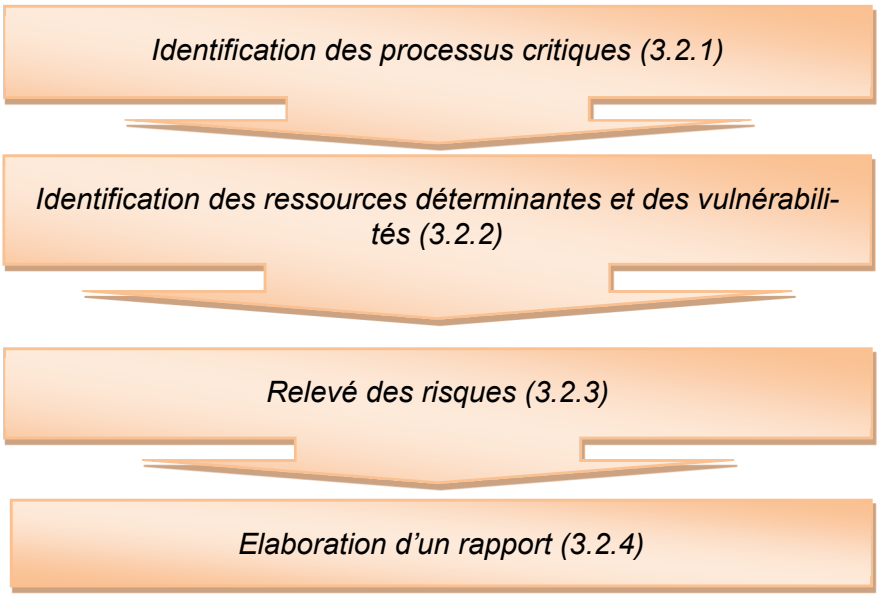


Illustration 3: Schéma des différentes étapes de l'analyse

3.2.1 Identification des processus critiques

La protection globale d'une infrastructure critique présuppose une connaissance détaillée de ses activités et fonctions. Il faut en effet comprendre quels sont les processus absolument indispensables pour garantir une capacité de fonctionnement minimale de l'infrastructure critique.

L'identification des processus critiques se fonde principalement sur l'analyse globale des processus d'exploitation réalisée dans le cadre de la gestion de la continuité des affaires (Business Impact Analyse). Si cette dernière n'a pas encore été faite, les normes et directives en la matière (cf. tableau 1) indiquent comment procéder.

*Dans le contexte de la protection des infrastructures critiques, on entend par **processus critique** un processus essentiel à la capacité de fonctionnement de l'infrastructure critique et dont la défaillance pourrait avoir des répercussions immédiates extrêmement graves pour la population et ses bases d'existence.*

Idéalement, il faudrait prendre en considération un nombre gérable de processus critiques identifiés comme tels. Le tableau 3 ci-dessous donne un exemple **fictif** de processus critiques:

N°	Processus critique
1	Production
2	Conduite et pilotage du système
3	Distribution

Tableau 3: Exemples de processus critiques

3.2.2 Identification des ressources déterminantes et des vulnérabilités

L'étape suivante consiste à évaluer quelles ressources sont absolument nécessaires à l'exécution des processus identifiés comme critiques lors de l'étape précédente. Les ressources des domaines des matières premières, de l'énergie, des TIC, du personnel, de la logistique et des infrastructures méritent une attention particulière.

L'Illustration 4 ci-contre présente cette étape:

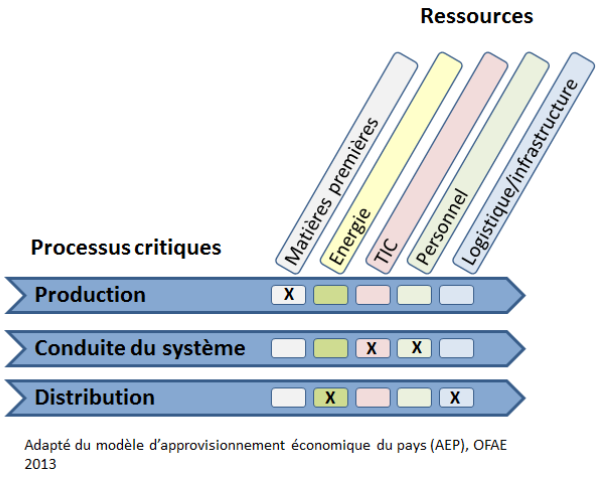


Illustration 4: Diagramme des processus et des ressources

Pour chaque ressource, on décrira ensuite quelles conséquences aurait une défaillance par rapport aux processus critiques et dans quelle mesure une telle défaillance nuirait à l'exécution du processus.

3.2.3 Relevé des risques

Il s'agira ensuite de relever les risques représentant les points faibles déterminés au point 3.2.2 pour la population et ses bases d'existence.

*Le **risque** permet de déterminer l'ampleur d'une mise en danger. Pour le calculer, on multiplie la probabilité ou la plausibilité qu'un événement survienne par l'ampleur des dommages que subiraient la population et ses bases d'existence.*

Dans le contexte de la protection des infrastructures critiques, la notion de risque sert à la fois de modèle pour l'évaluation de questions de sécurité et d'outil permettant de comparer des menaces de nature différente au moyen de critères identiques.

Les deux principaux facteurs qui déterminent le risque sont la probabilité qu'un événement se produise et l'ampleur des dommages qu'il causerait.

*On entend par **probabilité** le nombre, estimé ou déterminé en se basant sur des statistiques, d'événements de ce type survenant dans un laps de temps défini.*

*On appelle **ampleur des dommages** l'estimation des conséquences pour la population et ses bases d'existence lorsqu'une mise en danger se concrétise et provoque une défaillance d'un ou de plusieurs processus critiques. Pour la déterminer, on additionne le montant des dommages au moment où l'événement se produit et celui des dommages susceptibles d'apparaître durant toute la période de remise en état.*

Le relevé des risques se fait en trois étapes: dans un premier temps, on identifie les dangers significatifs. Puis on élabore des scénarios correspondant à chacun, pour évaluer ensuite la probabilité qu'ils se produisent ou leur plausibilité, ainsi que l'ampleur des dommages subis par la population et ses bases d'existence.

Première étape: sélection des dangers significatifs

Les processus et ressources identifiés comme déterminants aux points 3.2.1 et 3.2.2 sont répertoriés dans un tableau et se voient attribuer un numéro. Pour les ressources internes (appartenant **à son propre domaine de responsabilité)**, on retiendra les dangers **significatifs** pouvant entraîner un épuisement de la ressource[8]. Il convient de prendre en considération un éventail complet des dangers: en principe, il ne faut négliger aucun danger potentiel qui pourrait entraîner un épuisement important de la ressource. L'OFPP a établi une liste des dangers possibles, qu'il tient à disposition pour aider à les identifier[9].

- Liste des dangers possibles: cette liste constitue un récapitulatif, à la fois complet et adaptable, des événements et développements de la situation susceptibles de mettre en danger la population et ses bases d'existence, aujourd'hui ou dans le futur. Elle offre une vue d'ensemble aussi complète que possible des événements envisageables, sans toutefois donner priorité à l'un ou l'autre. La liste sera complétée par d'autres dangers propres à chaque ressource qui pourraient entraîner des défaillances.

Pour les ressources externes (prestataires externes, services, etc.), il convient de toujours examiner la défaillance de la ressource, quelle qu'en soit la cause. Le Tableau 4 ci-dessous donne un exemple fictif de liste:

---

[8] Il s'agit de ressources pour lesquelles des mesures préventives peuvent empêcher un épuisement de la ressource. Il faut donc les distinguer des mesures de préparation, qui empêchent que l'épuisement de la ressource ne conduise à une défaillance du processus.

[9] www.risk-ch.ch -> Liste des dangers possibles

N°	Processus critique selon le chap. 3.2.1	Ressources déterminantes selon le chap. 3.2.2	Défaillance de ressources externes / Danger significatif pour les ressources relevant du propre domaine de responsabilité
1	Production	*Matières premières (externe)*	*Epuisement des matières premières*
2	Production	Ouvrages et constructions (usine X)	Séisme
3	Production	Ouvrages et constructions (usine X)	Attaque conventionnelle
3	Conduite et pilotage du système	*TIC (externe)*	*Défaillance de la télécommunication publique*
4	Conduite et pilotage du système	TIC (réseau d'entreprise)	Cyberattaque
5	Conduite et pilotage du système	Personnel (gestionnaire du système)	Pandémie
7	Distribution	*Energie (externe)*	*Défaillance de l'approvisionnement en électricité*
8	Distribution	Ouvrages et constructions (centrale de distribution Z)	Incendie

Tableau 4: Exemple de mise en regard des processus, ressources et dangers

Deuxième étape: élaboration des scénarios

La deuxième étape consiste à créer des scénarios illustrant sous quelle forme la défaillance d'une ressource déterminante se manifeste ou comment le danger significatif porte atteinte à cette ressource et quelles en sont les conséquences pour la population et ses bases d'existence. Des exemples de scénarios et d'informations relatifs aux différentes menaces sont notamment disponibles dans les travaux réalisés dans le cadre de l'analyse nationale des dangers représentés par les catastrophes et situations d'urgence en Suisse.[10]

Pour ce qui est de la protection des infrastructures critiques, on part du principe que les événements du quotidien et leurs répercussions sont maîtrisés par les exploitants et ne posent donc pas de problème pour la collectivité; par conséquent, ce sont les événements d'une intensité importante voire extrême qui doivent être au centre de l'attention. De plus, les travaux se fondent en principe sur le pire scénario envisageable: celui où le danger se manifeste de la manière la plus défavorable possible et a les effets les plus négatifs sur la ressource analysée[11]. Concernant la durée maximale de la panne des installations, on partira d'hypothèses réalistes quant au temps nécessaire aux réparations ou à la mise en place de solutions d'approvisionnement de remplacement (jusqu'au rétablissement de la disponibilité opérationnelle). On prendra en outre en considération les conditions-cadres applicables à chaque danger (p. ex. lorsqu'un événement entraîne des dommages de grande ampleur et qu'il en résulte une disponibilité réduite de pièces de rechange ou de personnel spécialisé).

[10] www.risk-ch.ch

[11] Par exemple, si l'on prend le scénario du séisme et son effet sur la ressource «ouvrages et constructions», on prendra en compte un séisme touchant deux emplacements redondants (p. ex. centres de calcul), simultanément et avec la plus grande intensité possible.

Troisième étape: appréciation des scénarios

Il faut ensuite relever les dommages correspondant aux différents scénarios. Contrairement aux approches traditionnelles de gestion des risques et de la continuité des activités, ce ne sont pas les conséquences pour l'entreprise qui sont ici étudiées en priorité, mais celles qui toucheront la population et ses bases d'existence.

On ne saurait évaluer l'ampleur des dommages sans fixer des indicateurs adéquats. De tels indicateurs sont proposés ci-après: ils permettent d'évaluer les dommages pouvant résulter de défaillances ou de dérangements des infrastructures critiques dont souffriraient la population et ses bases d'existence. Il est évidemment possible que certains indicateurs ne puissent pas être pris en compte pour l'une ou l'autre infrastructure critique, ou que des indicateurs supplémentaires soient définis. Le choix des indicateurs sera documenté et justifié lors de l'établissement du rapport.

Domaine concerné	Sous-secteur	Indicateur	Base Cst.	Unité
Population	Vie et santé	**Victimes décédées**	Art. 10, 57, 58, 61,118	Nombre
		Blessés/malades		Nombre
	Aide en situation d'urgence	**Personnes ayant besoin d'assistance**	Art. 12, 115	Jours-personnes
Environnement	Ecosystème	**Ecosystèmes dégradés**	Art. 74, 76, 77, 78, 104	Surface x ans
Economie	Patrimoine	**Dommages patrimoniaux et coûts de maîtrise (biens réels et fonds)**	Art. 61	CHF
	Capacité économique	**Réduction de la capacité économique**	Art. 100	CHF
Société	Approvisionnement en biens et services essentiels à la survie	**Dégradation de la qualité de vie**	Art. 102	Personnes x jours
	Ordre public constitutionnel, sécurité intérieure	**Restrictions touchant l'ordre public et la sécurité intérieure**	Art. 52, 185	Jours-personnes
	Réputation et confiance en l'Etat	**Atteinte à la réputation**	Art. 54	Intensité x durée
		Perte de confiance en l'Etat/les institutions	Préambule, art. 2, 5	Intensité x durée
	Intégrité territoriale	**Restrictions de l'intégrité territoriale**	Art. 58	Intensité x durée
	Biens culturels	**Endommagement/perte de biens culturels**	Art. 2, 69, (78)	Nombre x importance

Tableau 5: Proposition d'indicateurs de dommages

Des informations détaillées au sujet des différents indicateurs de dommages et des propositions concernant les classes correspondantes figurent à l'Annexe 2 – .

I M P O R T A N T !

Lors du relevé de l'ampleur des dommages, l'accent est mis sur les dommages portant atteinte à la population et à ses bases d'existence engendrés par la défaillance, le dérangement ou la destruction d'une infrastructure critique. On prendra tout particulièrement en considération les dommages consécutifs indirects (parfois difficiles à quantifier) dus à la défaillance des processus critiques, jusqu'à ce que ceux-ci soient rétablis. Il convient notamment d'évaluer s'il existe des redondances suffisantes ou d'autres solutions permettant de remplacer temporairement une prestation (p. ex. transport routier au lieu du transport ferroviaire).

Après avoir relevé l'ampleur des dommages, on s'intéressera à la probabilité d'occurrence et à la plausibilité des scénarios. Pour ce faire, il faudra à nouveau définir des indicateurs et des classes; des exemples sont proposés à l'annexe 3[12]. Le choix des indicateurs retenus pour évaluer la probabilité d'occurrence devra également être documenté et justifié. Ces indicateurs permettront ensuite d'évaluer la probabilité et la plausibilité de chaque scénario[13].

Les valeurs indiquant l'ampleur des dommages et la probabilité d'occurrence sont ensuite reportées dans le tableau répertoriant les processus critiques et les dangers. Concernant les différents indicateurs utilisés pour évaluer l'ampleur des dommages, il est recommandé d'indiquer la valeur de la classe la plus élevée.

N°	Processus critique selon le chap. 3.2.1	Ressource déterminante selon le chap. 3.2.2	Défaillance de ressources pertinentes ou danger pour des ressources du propre domaine de responsabilité	Risque
1	Production	*Matières premières (externe)*	*Epuisement des matières premières*	A3 / P3
2	Production	Ouvrages et constructions (usine X)	Séisme	A5 / P5
3	Production	Ouvrages et constructions (usine X)	Attaque conventionnelle	A6 / P2
4	…	…	…	…
5	…	…	…	…

Tableau 6: Mise en regard des processus critiques, des ressources et des dangers (tableau 4) complétée par les valeurs de probabilité et d'ampleur des dommages

Au terme de cette étape, les valeurs obtenues peuvent être reportées sur un graphique qui permettra de saisir les différents risques en un coup d'œil. L'Illustration 5 présente un diagramme de la probabilité et des risques qui résume les trois étapes expliquées ci-dessus (l'axe vertical peut aussi être utilisé pour indiquer la plausibilité au lieu de la probabilité, ou en complément).

[12] Pour davantage d'informations concernant cette méthode, cf. *Methode zur Risikoanalyse von Katastrophen und Notlagen für die Schweiz*, Version 1.03 (méthode pour l'analyse des risques découlant de catastrophes et de situations d'urgence en Suisse, document disponible uniquement en allemand).

[13] L'OFPP met à disposition des documents de référence destinés à l'évaluation de la plausibilité et de la probabilité d'occurrence des scénarios, ainsi que de leur impact.

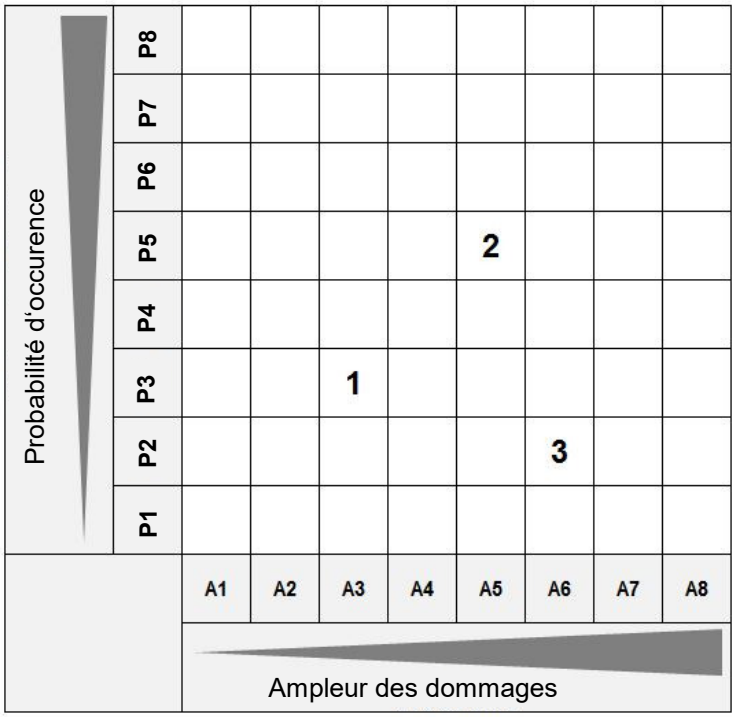


Illustration 5: Exemple de matrice des risques

3.2.4 Etablissement d'un rapport d'analyse

Le rapport d'analyse devrait contenir toutes les informations essentielles recueillies dans la phase de préparation et d'analyse. La définition de la situation de fait doit toutefois se limiter aux processus critiques.

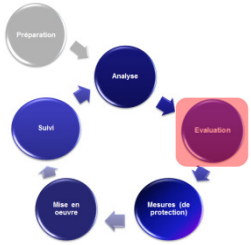
Si l'analyse devait révéler d'importantes lacunes en matière de sécurité des processus critiques (p. ex. *Single Point of Failure*, non-respect de conditions légales, etc.), le rapport proposera également des mesures à mettre en œuvre sans délai pour remédier aux lacunes de sécurité.

Le rapport d'analyse comporte les points suivants:

- Brève description du système
- Données concernant les travaux préliminaires existants (bases de la gestion des risques et de la continuité des activités)
- Données concernant les processus critiques
- Données relatives aux ressources déterminantes et aux vulnérabilités
- Dangers significatifs
  - Indicateurs pertinents pour déterminer l'ampleur de chaque danger, y compris brève justification s'appliquant aux indicateurs jugés non pertinents
  - Ampleur des dommages et probabilité des scénarios
  - Mesures de sécurité déjà mises en œuvre, ou planifiées et prises en considération dans l'analyse
- Matrice des risques
- Lacunes découvertes / mesures immédiates requises (lorsqu'elles sont connues)

Au cours des travaux suivants, les résultats des phases d'évaluation et de définition des mesures (de protection) viendront compléter le rapport d'analyse pour obtenir un rapport général. L'*Annexe 6 – Concept de protection intégrale. Proposition de structure d'un rapport général* montre comment un tel rapport peut être structuré. Le rapport d'analyse couvrira les chap. 1 à 3 du rapport général.

3.3 Evaluation



Après l'analyse des dangers et de la vulnérabilité, on déterminera le degré de sécurité visé dans le cadre de la phase d'évaluation. On se fondera notamment sur les objectifs stratégiques définis dans la stratégie nationale PIC (cf. chap. 1.2).

Au cours de cette phase, les questions essentielles qui se posent sont les suivantes:

- *Quelle est la sécurité minimale acceptable?*
- *Que sommes-nous prêts à accepter si un événement survient?*
- *Combien sommes-nous prêts à investir pour augmenter la sécurité?*

Ce sont en premier lieu les objectifs stratégiques relatifs au niveau de sécurité visé qui donnent à cette phase du processus son orientation.

Le niveau de sécurité se définit comme la situation en matière de sécurité que tous les responsables souhaitent établir ensemble.

Selon la stratégie nationale PIC, le niveau de sécurité visé dans le domaine des infrastructures critiques répond aux conditions suivantes: *«La capacité de fonctionnement de ses infrastructures critiques assure à la Suisse une résilience permettant d'éviter dans la mesure du possible des défaillances graves et de grande ampleur géographique des infrastructures critiques et de façon qu'en cas d'incident, l'étendue des dommages reste limitée.»*[14]

Concernant les dangers d'origine naturelle, la plate-forme nationale « Dangers naturels » PLANAT prescrit quant à elle le niveau de sécurité suivant: « *Les risques (...) sont si faibles que la pérennité de la collectivité est assurée, aujourd'hui comme pour les générations à venir. Des biens et des services d'une importance vitale ne peuvent faire défaut dans une grande partie de la Suisse que pendant un court laps de temps.*»[15]

Enfin, en fixant des objectifs de protection, les responsables apportent une contribution concrète pour atteindre le niveau de sécurité visé.

Un objectif de protection indique le niveau de sécurité auquel aspire chaque responsable dans le domaine dont il a la charge.

Dans plusieurs domaines de la protection des infrastructures critiques (p. ex. dans les différents sous-secteurs ou pour certains dangers), des objectifs de protection sont déjà définis et doivent absolument être respectés dans le cadre de la mise en œuvre du guide PIC. Il s'agit notamment des objectifs liés aux risques individuels (p. ex. risque de décès).

En ce qui concerne les risques collectifs (avant tout dans les domaines où l'on n'a **pas** encore défini d'objectifs de protection), on évaluera lesdits risques et les mesures visant à les réduire dans le cadre d'une planification des mesures, notamment selon l'approche des coûts marginaux[16]. Ceux-ci représentent la limite de ce que la société est prête à payer pour éviter *une*

[14] Stratégie nationale pour la protection des infrastructures critiques 2018 – 2022, FF 2018 503.
[15] Plate-forme nationale «Dangers naturels» (2013): *Niveau de sécurité face aux dangers naturels*, août 2013, p. 11.
[16] Indépendamment de l'approche choisie, les objectifs de protection ont une autre fonction: dans le domaine des dangers naturels par exemple, ils constituent un critère de contrôle déterminant la nécessité d'agir. Il est notamment nécessaire d'agir lorsque certains seuils se rapportant au risque global ou à des facteurs de risque isolés (probabilité d'occurrence ou ampleur des dommages) sont dépassés. En revanche, l'approche basée sur les coûts marginaux, qui est utilisée pour compléter d'autres approches, ne définit pas de tels seuils se rapportant aux risques. Le guide PIC est conçu de telle sorte qu'il est compatible avec les deux types d'approches.

unité de dommage (p. ex. combien la société est disposée à payer pour éviter *un* mort ou *un* franc de dommages économiques ou *une* atteinte précise à l'environnement, etc.).

3.3.1 Procédure relative à l'évaluation des risques et des vulnérabilités

Concrètement, la phase d'évaluation se déroule en quatre étapes:

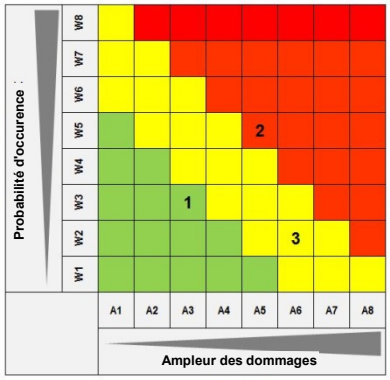
Première étape: évaluation des prescriptions existantes

Le point de départ consiste à remplir les exigences posées par les prescriptions existantes (legal compliance). Ces prescriptions englobent toutes les mesures ayant un caractère obligatoire pour les exploitants d'IC pour des raisons légales (respect de prescriptions légales, de normes, best practices, etc.), ainsi que les exigences relatives à d'autres objectifs de protection définis. Si des prescriptions applicables aux risques dont il est question ne sont pas respectées, il convient de prendre sans délai des mesures pour y remédier (cf. chap. 3.4).

Deuxième étape: définition des risques prioritaires

Si l'on dispose de plusieurs scénarios de dangers et processus, l'analyse des risques peut donner un nombre élevé de facteurs contribuant aux risques, de diverse importance. Pour simplifier la quantification des risques et la planification des mesures qui en découle, on peut commencer par classer ces facteurs en fonction de leur envergure et fixer des limites provisoires afin de pouvoir formuler des objectifs.

Les risques sont ensuite insérés dans la matrice, où ils sont répartis selon trois degrés de priorité:



rouge = mesures à planifier en priorité
jaune = mesures à planifier en second lieu
vert = mesures pouvant être planifiées ultérieurement

Illustration 6: Proposition d'affectation des degrés de priorité

Pour simplifier le travail, on peut également définir une limite en-deçà de laquelle on renonce à quantifier les risques et à planifier des mesures. La définition de cette limite devra être motivée et consignée dans le rapport subséquent.

Troisième étape: établissement des coûts marginaux pertinents et de l'aversion

Pour pouvoir quantifier les risques, les différents indicateurs de l'ampleur des dommages (cf. chap. 3.2.3, 3^{e} étape) doivent être convertis en valeur monétaire. Il s'agit en fait d'établir quel montant la société est prête à payer pour réduire d'une unité l'ampleur des dommages.

On se fondera pour ce faire sur un indicateur clé, pour lequel il existe à la fois des bases fiables et un consensus de « monétarisation » (obtenu à partir de la disposition de la collectivité à payer). Il s'agit généralement des victimes décédées: des documents complets sont aujourd'hui disponibles pour leur monétarisation. Les autres indicateurs sont ensuite étalonnés sur cet indicateur clé. L'annexe *Annexe 4.1* – fournit un exemple.

Pour prendre en compte le fait que la société essaie principalement d'éviter les risques majeurs, on peut fixer un facteur d'aversion[17]. L'annexe *Annexe 4.2* – fournit une proposition de facteur d'aversion.

Les coûts marginaux et la fonction d'aversion sont fixés en accord avec les autorités compétentes.

Les risques seront considérés avec ET sans le facteur d'aversion afin de pouvoir établir des comparaisons avec d'autres analyses.

Quatrième étape: quantification des risques

Pour les risques à traiter en priorité selon la matrice des risques, on procèdera à une analyse quantitative détaillée à l'aide des indicateurs de dommages monétarisés et éventuellement de la fonction d'aversion. Pour la suite des travaux, il est préférable de convertir les risques en valeurs annuelles de dommages prévus et de les additionner par type de processus ou par type de danger afin d'obtenir une vue d'ensemble (cf. Illustration 7). Cette étape permet en outre de connaître le risque global concernant les infrastructures (valeur annuelle des dommages auxquels il faut s'attendre).

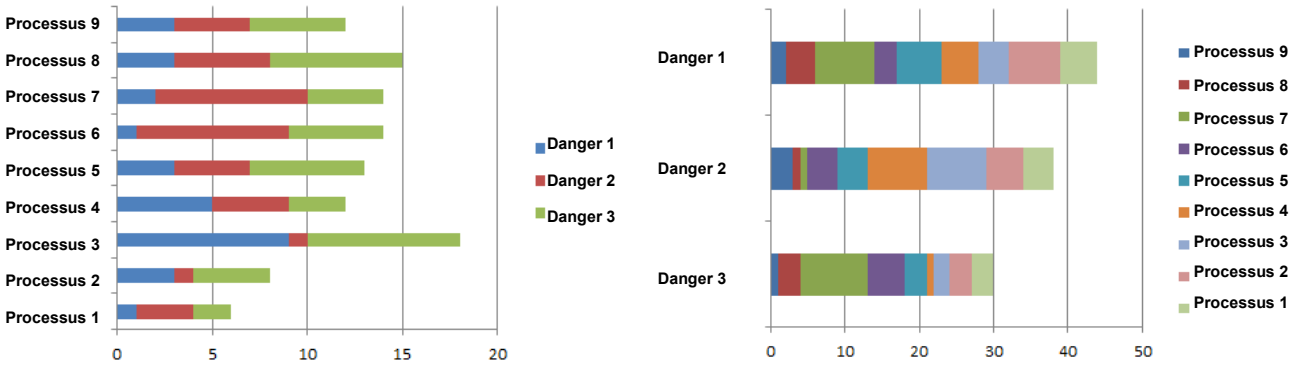


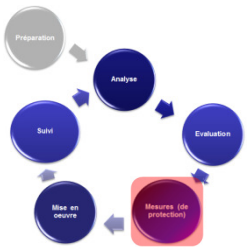
Illustration 7: Vue d'ensemble des risques pour un exemple fictif comprenant 9 processus et 3 types de dangers

A gauche: risques résultant des différents dangers pour chacun des processus; à droite: risques menaçant les différents processus pour chacun des dangers.

Les risques ainsi monétarisés servent de base à la planification des mesures. A partir de là, il faudra vérifier quelles sont les mesures – et les coûts qui les accompagnent – permettant de réduire les risques à un niveau acceptable. La décision finale concernant la réalisation des mesures (et donc, en fin de compte, le niveau de sécurité à atteindre concrètement) sera prise après la mise au point d'une combinaison optimale tenant compte des intérêts, politiques et autres, pesant dans la balance (cf. chapitre 3.4.4). Le rapport établi à l'issue de la phase d'analyse doit être complété par les résultats de la phase d'évaluation. On y consignera notamment, pour chaque indice, les coûts marginaux afin de déterminer ce que la société est disposée à payer.

[17] Par exemple, un accident de la route dans lequel 20 personnes perdent la vie n'aura pas le même impact sur la population que 20 accidents faisant chacun une victime, bien que la valeur de risque soit la même.

3.4 Mesures (de protection)



Lors de l'élaboration de la planification des mesures, on évaluera les mesures qui pourraient réduire les risques identifiés et analysés au préalable. L'évaluation reposera sur les questions fondamentales suivantes:

- *Comment les répercussions peuvent-elles être minimisées?*
- *Quelles sont les lacunes (quelles sont les mesures de protection qui font défaut)?*
- *Quelles sont les mesures de protection qui existent mais doivent être complétées ou adaptées?*
- *Combien sommes-nous prêts à investir pour des mesures destinées à augmenter la sécurité?*

Le processus visant à répondre à ces questions est décrit dans les sous-chapitres qui suivent.

Il existe en principe trois options à choix pour traiter les risques: éviter les risques, les réduire ou les répercuter sur d'autres acteurs. Etant donné que le fonctionnement des infrastructures critiques est indispensable pour la société et l'économie et que les risques qu'elles encourent ne peuvent ni être totalement évités ni suffisamment assurés, les explications ci-après se concentreront sur les aspects relevant de la réduction des risques.

3.4.1 Répertorier les mesures possibles

Dans un premier temps, il convient de répertorier les mesures qui pourraient permettre de réduire les risques. Il y a tout un éventail de mesures possibles à prendre en compte à cet égard, notamment:

- les mesures architecturales (passif, isolement du danger)
- les mesures techniques (actif, «si... alors...»)
- les mesures personnelles (vêtements de protection, etc.)
- les mesures administratives et organisationnelles (règles et interdictions)
- les mesures légales (contrats, accords de prestation, collaboration en cas de catastrophe, etc.)

Des exemples de telles mesures de protection figurent à l'*Annexe 5 – .* Elles sont donc données à titre purement informatif et servent à compléter les mesures de protection qui existent peut-être déjà. Il faut bien comprendre que cette liste ne prétend en aucune façon être exhaustive. Par ailleurs, il faudra déterminer pour chaque infrastructure critique quelles sont les mesures de protection déjà en place ou qui sont déjà planifiées.

Etant donné que certaines mesures de protection des infrastructures critiques peuvent être extrêmement onéreuses, il est fortement recommandé de chercher à collaborer avec d'autres exploitants concernés lors de l'élaboration des mesures. Suivant les circonstances, il peut être judicieux de mettre en place des mesures sous forme de solutions sectorielles (p. ex. collaboration accrue en cas d'événement, acquisition groupée de matériel de remplacement, etc.).

Il faut en outre tenir compte du fait que, selon les circonstances, les seules mesures de protection des infrastructures critiques ne suffisent pas à parer certaines menaces d'une intensité extrême. Dans de tels cas, on examinera avec les services spécialisés (p. ex. les services chargés des dangers naturels ou de la protection de la population) si les pouvoir publics peuvent agir à la source du danger.

Les étapes décrites ci-après, concernant la planification et la mise en œuvre, se réfèrent exclusivement aux mesures visant à renforcer la résilience des infrastructures critiques.
En matière de résilience, on peut opter pour des mesures préventives, mais aussi pour des mesures de préparation. Dans le cadre de la planification des mesures, on prendra en considération des mesures des deux types.

- **Mesures préventives**

  Mesures dont le but premier est de réduire la vulnérabilité d'une infrastructure critique, soit en évitant le danger, soit en limitant ses effets. Les mesures relevant de la prévention déploient leur effet avant que l'événement ne se produise.

- **Mesures de préparation**

  Mesures destinées à minimiser la durée de la défaillance d'une infrastructure critique ou à aider à la maîtrise d'un événement de sorte qu'il ne prenne pas des proportions plus importantes. Les mesures relevant de la préparation déploient leur effet au moment où l'événement se produit ou peu après.

  Les mesures visent principalement à garantir la continuité des activités, la gestion des situations d'urgence et la gestion de crise, ainsi qu'à compléter les résultats des travaux entrepris lors des étapes décrites aux chapitres 3.2 et 3.3.

  Le tableau ci-dessous fait office de récapitulatif et sert de base aux différentes mesures.

Mesures	Explications
Mesures visant à garantir la continuité des activités	Dans le cadre de la protection des infrastructures critiques, les mesures destinées à garantir le fonctionnement des éléments d'infrastructures critiques peuvent tout à fait être intégrées au système de *Business Continuity Management* (système BCM) existant. Le BCM devra éventuellement être adapté à cet effet. S'il n'existe aucune mesure de garantie de la continuité des activités interne à l'entreprise, il faudra en planifier en élaborant un BCM et le documenter. *On trouvera des instructions et autres indications concernant les mesures destinées à garantir la continuité des activités notamment dans les documents suivants:* *- ISO 22301: Sécurité sociétale – Systèmes de management de la continuité d'activité – Exigences* *- ISO 22313: Sécurité sociétale – Systèmes de management de la continuité d'activité – Lignes directrices. Première édition, 15 décembre 2012* *- Norme BSI 100-4 Notfallmanagement, version 1.0, 2008 (gestion des cas d'urgence, porte principalement sur la gestion de la continuité des services informatiques)* *- Umsetzungsrahmenwerk zum Notfallmanagement nach BSI-Standard 100-4, 2013 (cadre pour la mise en œuvre de la gestion des cas d'urgence selon la norme BSI 100-4, porte principalement sur la gestion de la continuité des services informatiques)* *- BS 25999-2* *- BCI Good Practice Guidelines 2013* *- Guide BCM de l'Office fédéral pour l'approvisionnement économique (« Ma petite entreprise / connaît pas la crise... »)* *- HB 221/2004 Business Continuity Management (basé sur AS/NZS)*
Mesures de gestion des cas d'urgence	Dans le cadre de la protection des infrastructures critiques, ces dernières peuvent tout à fait être intégrées au système de gestion des cas d'urgence interne à l'entreprise. Les concepts internes d'alarme, d'alerte et d'évacuation peuvent être appliqués aux infrastructures critiques. La gestion des cas d'urgence pour les infrastructures critiques comprend la planification, la préparation et l'adaptation des mesures immédiates pour les cas d'urgence. Les organisations de premiers secours doivent avoir une bonne connaissance de la gestion d'urgence des infrastructures critiques et les mesures immédiates dans ce domaine doivent avoir fait l'objet d'exercices. S'il n'existe pas de système de gestion des cas d'urgence à l'interne, il faut en mettre un en place. *On trouvera des instructions et autres indications concernant la création d'un système de gestion des cas d'urgence notamment dans les documents suivants:* *- Norme BSI 100-4* *- ISO / PAS 22399*

Mesures de gestion de crise	Dans le cadre de la protection des infrastructures critiques, ces dernières peuvent tout à fait être intégrées au système de gestion de crise interne à l'entreprise. La gestion de crise doit être conçue ou adaptée de sorte qu'en cas d'événement perturbant le fonctionnement d'une infrastructure critique, l'état-major de crise soit toujours engagé. S'il n'existe pas de système de gestion de crise à l'interne, il faut en mettre un en place. *On trouvera des instructions et autres indications concernant la gestion de crise notamment dans les documents suivants:* *- Manuel pour les membres des organes civils de conduite (édité par l'Office fédéral de la protection de la population OFPP)* *On trouvera des indications concernant la mise en place d'un système de gestion de crise entre autres dans les documents suivants:* *- British Standards Institute - PAS 200:2011 –* *Crisis management. Guidance and good practice* *- «Präventive Schadenbewältigung: Mehr gewinnen als verlieren»,* *Société suisse de réassurance Swiss Re, 2001.* *- ISO 22320:2011 Sécurité sociétale – Gestion des urgences – Exigences des opérations de secours*

Tableau 7: Domaines de mesures avec indications d'aides et autres documents

3.4.2 Définition de la combinaison de mesures optimale sur le plan économique

Il s'agit dans la prochaine étape de définir, parmi les mesures compilées, celles qui représentent la combinaison de mesures optimale sur le plan économique.

L'approche basée sur les coûts marginaux vise un rapport optimal entre les dommages résultant des défaillances ou des dérangements des IC et les coûts des mesures à mettre en œuvre. La combinaison de mesures optimale est celle qui donne le total des coûts le plus bas selon le schéma ci-dessous:

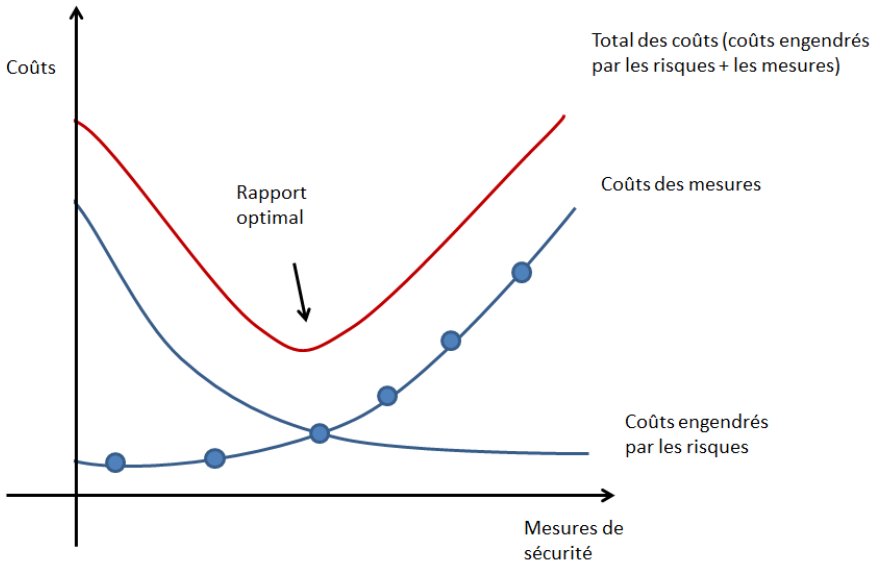


Illustration 8: Principe des coûts marginaux.

Les points bleus représentent les différentes mesures. Chaque mesure implémentée réduit le coût des dommages résultant d'une défaillance ou d'une perturbation d'une IC. La combinaison est optimale lorsque les coûts totaux (c.-à-d. la somme des coûts des mesures et des dommages résultant de défaillances ou de dérangements des IC) sont au point le plus bas.

En partant de la liste de toutes les mesures possibles, on considérera comme prioritaires celles dont on peut supposer qu'elles auront un rapport coût-utilité positif. On analyse ensuite en détail les coûts annuels de ces mesures (coûts d'investissement et coûts périodiques). On

évalue en outre à quel point la mesure permettra de réduire les risques. On peut ainsi établir une liste décroissante de l'ensemble des mesures, se fondant sur le rapport entre la réduction du risque et les coûts de la mesure. Les différentes mesures sont ensuite reportées dans un diagramme dont l'abscisse indique les coûts et l'ordonnée la réduction du risque. Les points reliés forment un polygone (cf. Illustration 9); on trace ensuite une droite d'une inclinaison de -1 (critère des coûts marginaux) tangente à ce polygone. Au point de contact, le critère des coûts marginaux est encore rempli. A droite de ce point, les coûts engendrés par les mesures de protection sont supérieurs à ceux de la réduction potentielle des dommages. A gauche de ce point, chaque mesure coûte moins cher que les dommages qu'elle permet d'empêcher.

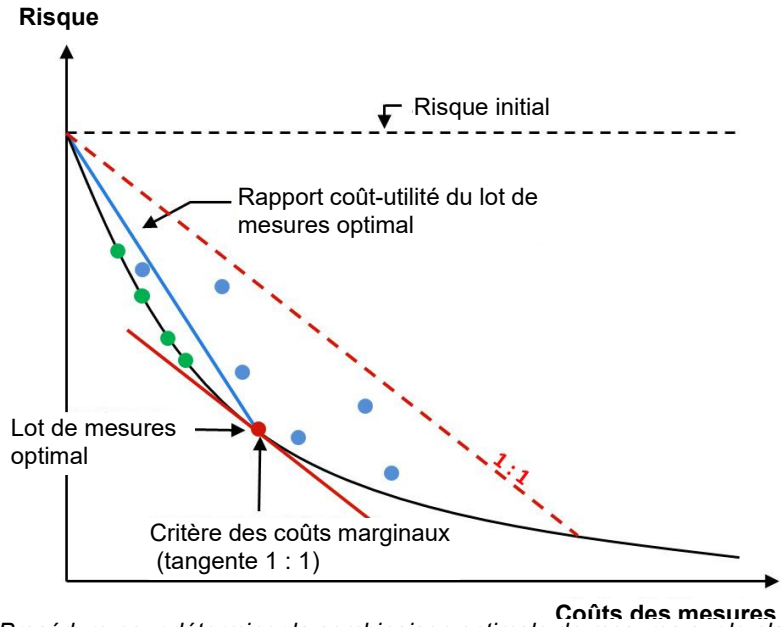


Illustration 9: Procédure pour déterminer la combinaison optimale de mesures sur le plan économique

La courbe noire représente la limite inférieure de l'ensemble des mesures. Sur cette courbe, les mesures atteignent une utilité maximale (réduction des risques) avec des coûts minimaux. Toutes les mesures situées au-dessous de la ligne rouge en pointillé (points bleus) ont bien un rapport coût-utilité supérieur à 1 mais elles ne sont efficaces ou optimales que si elles se trouvent sur la ligne noire avant le point de tangente (point rouge) = coûts marginaux des mesures (points verts).

Il est théoriquement possible que l'on ne trouve aucune mesure présentant un rapport coût-utilité positif. Cela peut par exemple se produire si l'on n'a pas planifié les mesures adéquates. Dans un tel cas, il faut alors examiner des mesures alternatives de réduction des risques (cf. chap. 3.4.1). Il est également possible qu'il n'existe, face à certains risques, aucune mesure efficace et rentable. Il convient alors d'élaborer des stratégies pour gérer les risques existants (cf. chap. suivant).

3.4.3 Évaluation des risques résiduels et pesée générale des intérêts

La combinaison de mesures élaborée après la pesée générale des intérêts doit ensuite être évaluée en lien avec le risque résiduel. Il faudra en particulier vérifier si elle respecte toutes les prescriptions (lois, directives, normes, objectifs, etc.). Si ce n'est pas le cas, il convient de choisir la combinaison de mesures qui s'approche le plus de la version optimale.

Comme le montre l'Illustration 9, un risque résiduel considérable subsiste lorsque l'on atteint les coûts marginaux, qui ne peut être couvert au moyen de mesures rentables. Il est donc important de prévoir avant tout événement une stratégie pour gérer ce risque résiduel au cas où ce dernier devait se concrétiser et se traduire, du moins partiellement, en dommages réels. Pour les risques relatifs à l'entreprise, il existe des assurances. L'État en particulier est appelé à assumer les risques sociétaux et économiques (p. ex. dans le cadre de la prévention des dangers, en accordant un soutien subsidiaire en cas d'évènement, en créant un fonds de solidarité, etc.). Les mesures correspondantes peuvent entre autres être prévues dans la stratégie nationale PIC.

Il faut en outre attribuer une grande importance à la communication sur les risques résiduels. Le dialogue entre tous les acteurs concernés améliore la conscience commune des risques, augmente la connaissance de ceux-ci et permet d'y sensibiliser la population et les acteurs économiques. Dans de nombreux cas, ces derniers peuvent prendre eux-mêmes des mesures de précaution et contribuer ainsi dans une large mesure à la réduction des risques.

Les mesures ne doivent pas simplement être optimales au niveau économique, mais aussi prendre en compte les autres aspects de la durabilité générale. A cet effet, il convient d'examiner les conséquences qu'implique la combinaison de mesures choisie pour les exploitants concernés, l'environnement, l'économie et la société.

On déterminera également comment se déroulera le financement des mesures; on s'assurera ainsi qu'il n'y a ni distorsion de la concurrence, ni inégalité de traitement entre les exploitants d'IC (également dans un contexte de concurrence internationale). La protection des infrastructures critiques mettant l'accent sur les prestations au profit de la collectivité, on veillera aussi, en ce qui a trait au financement des mesures, à ce que la société apporte une participation financière adéquate à la réduction des risques (p. ex. par une facturation aux clients ou via les pouvoirs publics).

De plus, on présentera le déroulement de la mise en œuvre des mesures. Dans certains cas, il sera nécessaire de créer des bases légales à cet effet ou de compléter celles qui existent. Les conditions-cadres à remplir seront précisées.

Si l'autorité compétente émet des réserves quant à la combinaison de mesures proposées après la pesée générale des intérêts ou l'évaluation des risques résiduels, il conviendra de procéder aux évaluations de la combinaison de mesures qui se rapproche le plus de la combinaison optimale. S'il s'avère impossible de définir des mesures satisfaisant aux différentes exigences de la pesée générale des intérêts, il conviendra le cas échéant de revoir les objectifs stratégiques et les évaluations effectuées (objectifs de protection et coûts marginaux éventuellement disponibles, cf. chap. 3.3).

3.4.4 Adoption des mesures

Les organes de conduite compétents à l'échelon le plus élevé (direction, conseil d'administration, autorités compétentes de surveillance et de régulation, Conseil d'Etat, Conseil fédéral, etc.) décideront quelles mesures seront effectivement réalisées en tenant compte de tous les intérêts pesant dans la balance (notamment les effets écologiques, économiques et sociaux à long terme, la proportionnalité, le besoin de sécurité, etc.). Il est donc tout à fait possible que le niveau de sécurité finalement atteint soit plus élevé ou plus bas que celui que l'approche des coûts marginaux donnait comme optimal.

Si la mise en œuvre des mesures exige une modification des bases légales, la décision finale de les réaliser est prise au niveau socio-politique. Les acteurs concernés (notamment les associations) peuvent mettre en avant leurs intérêts (lors d'une procédure de consultation ou d'audition) dans le cadre du processus législatif.

3.5 Mise en œuvre des mesures

La planification, la réalisation et le contrôle de la mise en œuvre des mesures relèvent généralement de la responsabilité des exploitants d'IC.

Lorsque le budget ou le personnel à disposition sont insuffisants pour implémenter simultanément l'ensemble des mesures, on procédera selon un ordre défini à partir des réflexions suivantes:

- Si un processus critique contient ce qui s'appelle un *Single-Point-of-Failure*, c'est-à-dire un élément dont la défaillance entraînerait la panne complète de l'infrastructure critique, la sécurisation de ce processus (et donc la suppression de cette vulnérabilité) est prioritaire.
- Pour certaines mesures, des liens logiques imposent un ordre chronologique qu'il est obligatoire de respecter dans le cadre de la mise en œuvre.
- Certaines mesures agissent à grande échelle, d'autres ont un effet plus local. Lorsqu'il s'agit de la protection d'infrastructures critiques, il est judicieux de s'occuper d'abord des mesures ayant l'effet le plus important.

3.6 Vérification, contrôle et amélioration des mesures

Pour pouvoir améliorer en permanence la protection intégrale des infrastructures critiques, il faut non seulement mettre en œuvre les mesures adéquates et tenir à jour les documents en continu, mais aussi vérifier régulièrement l'efficacité de la protection intégrale. L'organe de l'entreprise compétent procédera donc à des contrôles et évaluations périodiques de la protection intégrale (évaluation de la gestion).

Tous les résultats obtenus et toutes les décisions rendues seront documentés de manière compréhensible. Le contrôle et l'amélioration de la protection intégrale portent sur toutes les phases, et donc aussi bien sur l'examen des points établis dans la planification préalable que sur celui de l'actualité des risques existants ou encore sur la vérification de l'efficacité des mesures mises en œuvres ou des mesures préparatoires. De tels examens doivent avoir lieu régulièrement, p. ex. chaque année. On procédera à des contrôles supplémentaires aux échéances suivantes:

- après la mise en œuvre des mesures;
- après un événement (crise);
- après un agrandissement ou une transformation de l'infrastructure critique;
- après une modification significative de la situation en matière de danger.

3.6.1 Exercices/tests

Si des processus de travail comme la mise en service et l'utilisation d'installations techniques ne sont que sporadiquement mis en œuvre, ils risquent de se dérouler trop lentement ou de manière lacunaire lorsqu'un événement survient. Les structures et les procédures des différentes mesures, en particulier celles prévues pour parer à des événements dont la probabilité d'occurrence est faible mais dont l'ampleur des dommages est importante, doivent donc faire l'objet d'exercices à intervalles réguliers. Le but de ces exercices est[18]:

- de contrôler l'aptitude à fonctionner et la praticabilité des mesures;
- d'exercer la coordination et la communication en cas de crise;
- de tester les processus de crise et de les optimiser en se fondant sur des expériences pratiques;
- de créer des directives en vue du développement des structures et procédures nécessaires.

Ils permettront également d'entraîner le retour à une exploitation normale après une période d'exploitation de crise.

Les exercices peuvent être de divers types et recourir à diverses méthodes, qui se distinguent par le degré d'abstraction et l'investissement requis[19].

3.6.2 Entretien du processus de PIC

L'entretien du processus de protection intégrale requiert l'élaboration de critères de mesure et d'évaluation pour chaque infrastructure critique. Il est nécessaire d'effectuer régulièrement des mesures afin de pouvoir observer l'évolution des valeurs. Si celle-ci est négative, il faudra en rechercher les causes et définir des mesures d'amélioration, désigner des responsables pour mettre en œuvre ces mesures et procéder aux adaptations nécessaires.

---

[18] GUSTIN, Joseph F. *Disaster & Recovery Planning: A Guide for Facility Managers,* The Fairmont Press, Lilburn GA, 2004, p. 226.

[19] Des instructions et indications concernant les différents types et méthodes d'exercices sont notamment fournies dans: British Standards Institute – Published Document 25666:2010 – *Business Continuity Management – Guidance on Exercising and Testing for Continuity and Contingency Programmes.*

3.6.3 Contrôle

Seuls des contrôles réguliers de la protection intégrale permettent d'évaluer l'aptitude d'une infrastructure critique à maîtriser les urgences et les crises. Il s'agit de relever les lacunes et les possibilités d'amélioration et de faire des recommandations dans le but de garantir la capacité à fonctionner, l'efficacité, l'adéquation et l'efficience de la protection intégrale.

L'examen de la protection intégrale devrait être réalisé à plusieurs niveaux différents, p. ex. par le biais d'auto-évaluations ou de révisions internes ou externes. Les contrôles réguliers aux différents échelons doivent être planifiés puis exécutés, et leurs résultats doivent être documentés. On résoudra sans délai les problèmes révélés à l'occasion de ces contrôles.

Liste des abréviations

Abrévia-tion	*Terme*
BCI	*The Business Continuity Institute* → www.thebci.org
BCM	*Business Continuity Management* → Glossaire
BIA	Business Impact Analysis → Glossaire
BS	British Standard
BSI	Bundesamt für Sicherheit in der Informationstechnik (Office fédéral allemand pour la sécurité des techniques de l'information) → https://www.bsi.bund.de
FF	Feuille fédérale
IC	Infrastructures critiques → Glossaire
ISO	International Organization for Standardization → www.iso.org
PIC	Protection des infrastructures critiques → Glossaire
SCI	Système de contrôle interne → Glossaire

Illustrations

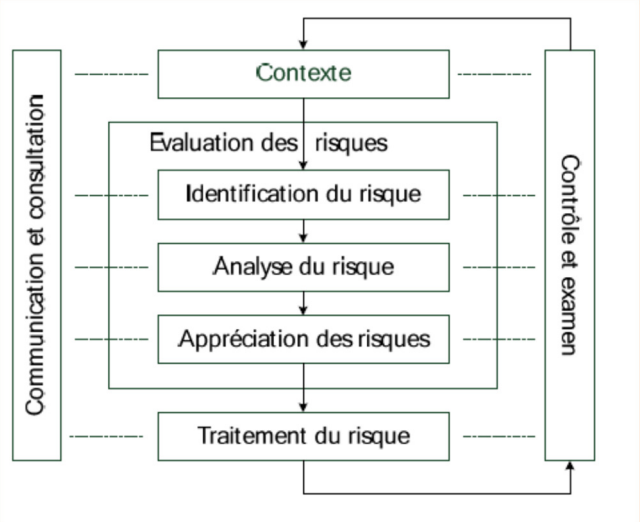
Tableaux

Glossaire

Les définitions ci-dessous donnent la signification des termes selon l'utilisation qui en est faite dans le présent guide et qui peut différer de leur utilisation dans d'autres publications. La flèche → renvoie toujours à une autre entrée de ce même glossaire.

Terme	*Définition*
Ampleur des dommages	L'ampleur des dommages désigne l'estimation des conséquences pour la population et ses → bases d'existence lorsqu'une → mise en danger se concrétise et provoque une défaillance d'un ou de plusieurs → processus critiques. Elle correspond au montant des dommages au moment où l'événement se produit et des dommages susceptibles d'apparaître durant toute la période de remise en état.
Analyse des risques	L'analyse des risques recense et décrit de manière systématique les → risques dans un système donné. L'appréciation du niveau des risques, souvent sous forme d'une classification des scénarios considérés en fonction de leur → probabilité d'occurrence et de → l'ampleur des dommages envisagés en fait partie. L'analyse des risques traite de la question «que peut-il arriver?». *Source: Glossaire des risques, Office fédéral de la protection de la population, 29.4.2013* L'analyse des risques est la base de la → gestion des risques. Elle sert à décrire la nature du → risque (→ mise en danger) et à en déterminer l'importance (ÖNORM ISO:3100). L'analyse des risques permet de déterminer une situation de départ aussi concrète et transparente que possible en vue de la planification des mesures de protection. La première étape consiste à identifier et recenser tous les risques potentiels qui pourraient nuire à l'organisation. Les répercussions (généralement financières) à chaque niveau (p. ex. commune ou entreprise) qu'entraîneraient les risques retenus ainsi que leur probabilité d'occurrence sont ensuite analysées. Tant les répercussions que la probabilité d'occurrence des risques dépendent des hypothèses relatives à leur intensité sur lesquelles se fonde l'appréciation. C'est la raison pour laquelle il est nécessaire de définir un scénario pour les différents risques avant de pouvoir procéder à une appréciation. Pour simplifier, on adopte en général le scénario du «pire cas possible» qui reste toutefois «crédible» (*worst credible case*). L'importance du risque est définie en multipliant l'ampleur des dommages par la probabilité d'occurrence. Les résultats sont reportés dans une matrice des risques, utilisée comme base de la planification dans la → gestion des risques.
Bases d'existence	Ensemble des éléments dont la population a besoin pour vivre. Les bases d'existence rendent possible la vie en commun aux niveaux collectif et individuel. Elles peuvent être réparties en trois catégories: - <u>bases naturelles d'existence:</u> environnement intact (sols, eaux, air, biodiversité); - <u>bases économiques d'existence:</u> prospérité économique et infrastructures en état de fonctionnement; - <u>bases sociales d'existence:</u> système de droit et ordre constitutionnel intacts, confiance réciproque, intégrité territoriale et diversité culturelle. *Source: Glossaire des risques, Office fédéral de la protection de la population, 29.4.2013*
Business Continuity Management (BCM)	Le *Business Continuity Management* (fr. gestion de la continuité des activités) est une tâche de conduite globale, consistant à identifier les risques (et leurs effets sur les processus commerciaux), à planifier des mesures correctives et à les appliquer en cas d'accident majeur. C'est un processus destiné à assurer la continuité de l'exploitation après une défaillance des ressources stratégiques.

	Traduit à partir du glossaire BCMnet.CH, avril 2013
Business Impact Analysis (BIA)	La *Business Impact Analysis* (fr. analyse d'impact commercial) est l'analyse des répercussions (financières et matérielles) que peut avoir un accident majeur sur une entreprise ordinaire. Elle consiste à identifier les ressources critiques et ce qu'exige une relance du système, ainsi que les conséquences d'interruptions inopinées du fonctionnement. *Traduit à partir du glossaire BCMnet.CH, avril 2013*
Coûts marginaux	Les coûts marginaux permettent de mesurer la capacité de paiement pour prendre les mesures visant à réduire les risques. Concrètement, il s'agit des coûts par unité de dommage empêchée que la société est prête au maximum à dépenser pour prendre des mesures visant à réduire les → risques. *Source: Glossaire des risques, Office fédéral de la protection de la population, 29.4.2013*
Défaillance grave	Une défaillance est considérée comme grave lorsque des biens et services importants ne sont plus disponibles pendant une certaine durée sur le territoire dépendant de l'IC concernée (commune, canton, région, pays, etc.)
Efficacité	L'efficacité se réfère aux mesures prises et indique dans quelle mesure le → risque est réduit par celles-ci. *Source: Glossaire des risques, Office fédéral de la protection de la population, 29.4.2013*
Gestion de crise	Préparation systématique aux crises ainsi qu'à la maîtrise de telles situations. Cette notion englobe l'organisation de crise, l'identification et l'analyse de situations de crise, la mise au point de stratégies visant à maîtriser les crises ainsi que la mise en marche et le suivi de contre-mesures. La gestion de crise englobe tant les dispositions prises pour affronter la situation de crise que la gestion de la situation en elle-même. *Source: Glossaire des risques, Office fédéral de la protection de la population, 29.4.2013*
Gestion de la continuité	Voir Business Continuity Management
Gestion de la sécurité	La gestion de la sécurité comprend la planification, le pilotage et le contrôle de la sécurité au sein d'une organisation. Elle englobe les aspects sécuritaires des systèmes techniques ainsi que des aspects non techniques tels que la sécurité au travail ou la sécurité d'exploitation, ou encore la sécurité des locaux et des bâtiments. La gestion de la sécurité s'entend parfois comme un processus global dans lequel sont intégrés des éléments tels que la → gestion des risques, la → gestion de la continuité des activités (BCM), etc. Il existe cependant aussi des formes d'organisation dans lesquelles c'est au contraire la gestion de la sécurité qui est une mesure faisant partie intégrante de la → gestion des risques.
Gestion des risques	On entend par gestion des risques l'ensemble des activités coordonnées dans le but de diriger et d'orienter une organisation par rapport aux risques, c.-à-d. par rapport aux conséquences que peuvent avoir les incertitudes sur les objectifs de l'organisation. *Traduit à partir de la norme ÖNORM ISO 31000:2010* La gestion des risques est un processus systématique pour traiter les risques de manière intégrale. La gestion des risques est un processus établi dans la société et l'économie pour le traitement des risques. Selon le contexte, la gestion des risques est structurée et organisée de manière diverse (éléments et pondérations). Le modèle général est le processus selon ISO 31000 présenté ci-après.

	 *Source: Glossaire des risques, Office fédéral de la protection de la population, 29.4.2013*
Gestion des situations d'urgence	Un plan de gestion des situations d'urgence (aussi appelé mesures de précaution) prépare une organisation à réagir et à maîtriser rapidement une situation d'urgence. La gestion des situations d'urgence fixe notamment les organisations d'urgence, la transmission de l'alarme, la réaction schématique (mesures immédiates) face à certaines situations d'urgence et indique le comportement à adopter. Elle établit aussi comment se déroule la coopération avec les organisations de premiers secours. Son but est qu'en cas d'urgence, on ne perde pas de temps à prendre des décisions inutiles, à donner des directives ou à attribuer des compétences. La gestion des situations d'urgence vise avant tout à protéger la vie et l'intégrité corporelle. Cependant, puisqu'elle sert à maîtriser les événements, elle peut aussi être conçue comme une partie du système de → *gestion de la continuité des activités* (BCM) ou de la → gestion de crise, étant donné que des situations d'urgence peuvent être à l'origine de crises.
Infrastructures critiques (IC)	On entend par infrastructures critiques les processus, systèmes et installations revêtant une importance capitale pour le fonctionnement de l'économie et le bien-être de la population.
Inventaire PIC	L'inventaire PIC est une liste des objets critiques dont la défaillance, le dérangement ou la destruction pourraient avoir des conséquences graves sur la population et ses bases d'existence. Il s'agit, d'une part, d'objets jouant un rôle essentiel dans l'approvisionnement de certains biens et services et, d'autre part, d'objets présentant un potentiel de danger élevé. L'inventaire PIC comprend notamment des objets d'importance nationale. Il remplace la liste des ouvrages GBE (garantie des besoins existentiels), qui avait été établie et mise à jour dans le cadre de la défense générale. L'inventaire PIC a été élaboré sous la direction de l'Office fédéral de la protection de la population (OFPP), en étroite collaboration avec les organes compétents de la Confédération et des cantons et les exploitants d'IC. Il est régulièrement mis à jour. Son but premier est de servir de base aux processus de planification et de décision aux différents échelons (Confédération, cantons et exploitants d'IC).
Mise en danger	Par «mise en danger», on entend un danger concret existant pour un bien digne de protection concret. La mise en danger correspond par conséquent à un événement ou développement potentiel pouvant avoir des conséquences sur un bien digne de protection. *Source: Glossaire des risques, Office fédéral de la protection de la population, 29.4.2013*
Niveau de sécurité visé	Etat de sécurité visé conjointement par toutes les entités assumant une responsabilité. *Source: Niveau de sécurité face aux dangers naturels, PLANAT 2013*

Objectif de protection	Niveau de sécurité visé par certaines entités assumant une responsabilité dans leur domaine de compétence. *Source: Niveau de sécurité face aux dangers naturels, PLANAT 2013*
Politique de sécurité de l'entreprise	Pour assurer une sécurité uniforme au sein de l'entreprise, il est essentiel de formuler une politique de sécurité valable pour l'ensemble de la société (angl.: *Corporate Security Policy*). La notion de politique de sécurité n'est pas définie de la même manière dans les différents documents, normes et standards existants. D'une manière générale, la politique de sécurité fixe l'orientation et la culture choisies dans le domaine de la sécurité, ainsi que les standards et réglementations applicables au sein de l'organisation. Elle permet de définir des objectifs de protection en établissant le niveau de sécurité visé (ISO/IEC TR 13335-1). La politique de sécurité de l'entreprise se doit de refléter la politique de l'entreprise. C'est à la direction qu'incombe l'élaboration de cette politique, par laquelle elle s'engage à assumer la responsabilité de la sécurité de l'entreprise (Müller, 2005). La politique de sécurité de l'entreprise doit être publiée dans les locaux; tous les collaborateurs doivent en avoir connaissance. Le texte doit être bref, clair et compréhensible. Il doit tenir en quelques pages. La politique de sécurité d'une entreprise comprend notamment les aspects suivants: - importance de la sécurité dans l'entreprise; - références aux exigences des niveaux supérieurs et aux lois en vigueur; - objectifs de sécurité et éléments stratégiques nécessaires pour les atteindre, ainsi que méthodes et standards à utiliser; - éléments de l'organisation de la sécurité; - déclarations relatives au contrôle de la mise en œuvre de la politique de sécurité de l'entreprise; déclarations relatives aux sanctions en cas de non-respect de la politique de sécurité de l'entreprise.
Prévention des risques	Il est possible de parer les risques soit en évitant les régions menacées, soit en mettant en œuvre des mesures destinées à empêcher l'apparition de dangers. Face aux aléas naturels et à l'environnement des dispositifs à haut risque (songeons aux itinéraires de transport des marchandises dangereuses), les zones exposées – autrement dit menacées – peuvent souvent être identifiées. Une révision de la conception des sites, des bâtiments et des dispositifs concernés permettra d'éviter ces zones. La prévention totale des risques est toutefois impossible, aucun site n'en étant exempt. *Source: Ministère fédéral de l'Intérieur, Protection des infrastructures critiques – gestion des risques et des crises – Manuel destiné aux entreprises et aux administrations, Berlin, janvier 2008, p. 22*
Probabilité d'occurrence	On appelle probabilité d'occurrence la probabilité estimée ou calculée sur la base de statistiques qu'un événement se produise au cours d'une période donnée (p. ex. dans les 10 ans).
Processus	Un processus peut être considéré comme une suite de (sous-)processus au cours desquels des actes sont réalisés et des décisions sont prises. En principe, un processus comprend un élément entrant (input), qui provient d'autres processus commerciaux, et fournit un élément sortant, c.-à-d. un résultat (output), par exemple sous forme de produit, d'information ou de prestation. Les éléments entrants et sortants établissent le lien entre les différents processus. Les processus commerciaux peuvent être répartis en deux catégories, en fonction de leur type, les → processus clés et les → processus de support.

Processus clé	Les → processus clés sont ceux qui contribuent de manière directe à remplir la mission de l'infrastructure critique. Ils peuvent par exemple permettre aux autorités d'accomplir des tâches étatiques qui leur sont déléguées ou aux exploitants de fournir des prestations ou de fabriquer un produit.
Processus critique	Dans le contexte de la protection des infrastructures critiques, on entend par processus critique tout processus indispensable au fonctionnement de l'infrastructure critique et dont la défaillance aurait des répercussions graves sur la population et ses bases d'existence.
Processus de support	Les processus de support ne contribuent pas directement à l'accomplissement des tâches d'une infrastructure critique mais peuvent néanmoins jouer un rôle indirect très important et donc critique, puisqu'ils permettent le maintien de → processus clés. L'alimentation en électricité et la télécommunication sont des exemples de processus de support d'infrastructures critiques.
Protection des infrastructures critiques (PIC)	La protection des infrastructures critiques englobe des mesures qui réduisent la → probabilité d'occurrence et/ou → l'ampleur des dommages d'un dérangement, d'une défaillance ou d'une destruction d'→ infrastructures critiques ou qui réduisent le plus possible la durée de non-disponibilité.
Rapport coût-efficacité	Le rapport coût-efficacité est une grandeur permettant de déterminer la proportionnalité des mesures à prendre. Il constitue donc une caractéristique des mesures et met en parallèle → l'efficacité des mesures (→ réduction des risques) et les coûts générés. *Source: Glossaire des risques, Office fédéral de la protection de la population, 29.4.2013*
Réduction des risques	Les mesures de réduction des risques sont de deux ordres: soit elles diminuent la vulnérabilité des éléments de risque face aux incidences de certains aléas, soit elles visent à garantir la continuité opérationnelle des processus critiques en instaurant des systèmes redondants et/ou des systèmes de remplacement: même s'ils peuvent perturber certains éléments critiques, ces systèmes ont l'avantage d'assurer une continuité opérationnelle dans le cadre de la gestion de la reprise sur incident. *Source: Ministère fédéral de l'Intérieur, Protection des infrastructures critiques – gestion des risques et des crises – Manuel destiné aux entreprises et aux administrations, Berlin, janvier 2008, p. 21*
Résilience	La «résilience» décrit la capacité d'un système, d'une organisation ou d'une société, à surmonter des dysfonctionnements d'origine interne ou externe et à maintenir autant que possible ou à retrouver toute sa fonctionnalité. La résilience se compose de quatre éléments: 1) la robustesse des systèmes (p. ex. → infrastructures critiques, Etat, économie et société); 2) les redondances disponibles; 3) la capacité à mobiliser des mesures auxiliaires efficaces; 4) la rapidité et l'efficience des mesures auxiliaires. *Source: Glossaire des risques, Office fédéral de la protection de la population, 29.4.2013*
Risque	Le risque permet de déterminer l'étendue d'une → mise en danger et englobe la fréquence ou → probabilité et → l'ampleur des dommages d'un événement indésirable. *Source: Glossaire des risques, Office fédéral de la protection de la population, 29.4.2013* Dans le domaine de la → protection des infrastructures critiques, la notion de risque sert à la fois à évaluer des questions de sécurité et à comparer différents types de → mises en danger en utilisant les mêmes critères. Le modèle des risques s'appuie en principe sur deux facteurs: → la probabilité d'occurrence d'un événement; → l'ampleur des dommages pour la population et ses → bases d'existence.

	Le risque correspond donc à un produit qui se définit par la probabilité d'occurrence d'un événement et par l'ampleur des dommages qu'il engendre.
Risque résiduel	On entend par «risque résiduel» le risque qui subsiste une fois que toutes les mesures de sécurité prévues ont été mises en œuvre. *Source: Glossaire des risques, Office fédéral de la protection de la population, 29.4.2013*
Single Point of Failure	Source de problème grave: élément dont la défaillance entraînerait la panne complète de l'infrastructure critique ou de ses processus critiques. Ces points vulnérables doivent être supprimés ou sécurisés en priorité.
Sous-secteur	Les → infrastructures critiques suisses ont été réparties en 28 sous-secteurs couvrant l'ensemble des branches, industries, secteurs économiques et autres divisions économiques. En Suisse, les infrastructures critiques appartiennent aux sous-secteurs suivants: déchets, eaux usées, armée, soins médicaux et hôpitaux, représentations diplomatiques et organisations internationales, banques, services d'urgence, industrie chimique et pharmaceutique, approvisionnement en gaz naturel, approvisionnement en pétrole, recherche et enseignement, technologies de l'information, biens culturels, laboratoires, approvisionnement en denrées alimentaires, trafic aérien, industrie mécanique, électrique et métallurgique, médias, Parlement, gouvernement, justice et administration, trafic postal, trafic ferroviaire, trafic fluvial, trafic routier, approvisionnement en électricité, télécommunication, assurances, approvisionnement en eau et protection civile.
Système de contrôle interne (SCI)	Il s'agit d'un système de contrôle comprenant l'ensemble des processus, méthodes et mesures servant à assurer le bon déroulement des activités. Dans le cas des entreprises de droit privé, le système de contrôle interne se fonde sur le code des obligations (art. 716a). Pour ce qui concerne l'administration fédérale, le système de contrôle interne est décrit dans la loi sur les finances (LFC, art. 39) ainsi que dans l'ordonnance sur les finances (OFC, art. 36). Le SCI traite des risques opérationnels (→ risque) dans le domaine des risques financiers et économiques ainsi que des risques juridiques (conformité aux règles à appliquer («Compliance»)). - *Source: Glossaire des risques, Office fédéral de la protection de la population, 29.4.2013*

Annexe 1 – Bases méthodologiques

Australie/Nouvelle-Zélande:

- AS/NZS 4360:2004 *Risk management* (replaced by AS/NZS ISO 31000:2009).
- HB 436:2004 *Risk Management Guidelines Companion to AS/NZS 4360:2004.*
- AS/NZS 5050:2010 *Business Continuity – Managing Disruption Related Risks.*
- HB 221:2004 *Business Continuity Management*.

Allemagne:

- Office fédéral pour la protection des populations et l'assistance en cas de catastrophes: *Schutz kritischer Infrastruktur – Risikomanagement im Krankenhaus*, 2008.
  http://www.bbk.bund.de/SharedDocs/Downloads/BBK/DE/Publikationen/Praxis_Bevoelkerungsschutz/Band_2_Praxis_BS_Risikomanagm_Krankenh_Kritis.pdf?__blob=publicationFile
- Office fédéral pour la protection des populations et l'assistance en cas de catastrophes: *Méthode d'analyse de risques dans la protection civile*, 2010.
  http://www.bbk.bund.de/FR/Publications/01_booklets/Methode_analyse_risques_protection_civile.html?nn=1900604 =4914E21B99FB591B6EC2A0CCDBB766CD.1_cid345?__blob=publicationFile
- Ministère fédéral de l'Intérieur: *Protection des infrastructures critiques – gestion des risques et des crises – Manuel destiné aux entreprises et aux administrations*, 2008.
  http://www.kritis.bund.de/SharedDocs/Downloads/BBK/FR/Leitfaden-Kritis-Risiko-Krisenmanagement_fr.html
- BSI-Standard 100-4: *Notfallmanagement,* Version 1.0, 2008 (porte principalement sur la gestion de la continuité des services informatiques).
  https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/ITGrundschutzstandards/standard_1004_pdf.pdf?__blob=publicationFile
- *Umsetzungsrahmenwerk zum Notfallmanagement nach BSI-Standard 100-4*, 2013 (porte principalement sur la gestion de la continuité des services informatiques).
  https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzStandards/Umsetzungsrahmenwerk/umra.html

Union européenne:

- Commission Staff Working Paper SEC (2010) 1626 final: *Risk Assessment and Mapping Guidelines for Disaster Management*, 2010.
  http://ec.europa.eu/echo/files/about/COMM_PDF_SEC_2010_1626_F_staff_working_document_en.pdf
- European Network and Information Security Agency (ENISA): *Good Practice Guide for Incident Management*, 2010.
  http://www.enisa.europa.eu/act/cert/support/incident-management/files/good-practice-guide-for-incident-management/at_download/fullReport

International Organization for Standardization (ISO):

- ISO/IEC 13335-1:2004: *Technologies de l'information – Techniques de sécurité – Gestion de la sécurité des technologies de l'information et des communications – Partie 1: Concepts et modèles pour la gestion de la sécurité des technologies de l'information et des communications.*
- ISO 22301:2012 – *Sécurité sociétale – Systèmes de management de la continuité d'activité – Exigences*
- ISO 22313:2012 – *Sécurité sociétale – Systèmes de management de la continuité d'activité – Lignes directrices. Première édition, 15 décembre 2012.*
- ISO 22320:2011 – *Sécurité sociétale – Gestion des urgences – Exigences des opérations des secours*, 2011.
- ISO 22399:2007 – *Sécurité sociétale – Lignes directrices pour être préparé à un incident et gestion de continuité opérationnelle.*
- ISO/IEC 27001:2013 – *Technologies de l'information – Techniques de sécurité -- Systèmes de management de la sécurité de l'information – Exigences.*

- ISO/IEC 27002:2013 – *Technologies de l'information – Techniques de sécurité -- Code de bonne pratique pour le management de la sécurité de l'information.*
- ISO 31000: 2009 – *Management du risque – Principes et lignes directrices.*

Autriche:

- Austrian Standards Institute: *ONR 49000:2010 ss. Risikomanagement für Organisationen und Systeme.* (Famille de normes englobant les normes ONR 49000, 49001, 49002-1, ONR 49002-2, 49002-3, 49003).

Suisse:

- OFPP: *Aide-mémoire KATAPLAN. Analyse cantonale des dangers et préparation aux situations d'urgence.* Janvier 2013.
  http://www.kataplan.ch
- OFPP: *Analyse nationale des dangers «Catastrophes et situations d'urgence en Suisse» – Rapport sur les risques 2012.*
  http://www.risk-ch.ch → Télécharger
- OFPP: *Methode zur Risikoanalyse von Katastrophen und Notlagen für die Schweiz,* Version 1.03, Stand: 17. April 2013.
- OFPP: *Gestion intégrale des risques. Importance pour la protection de la population et des bases d'existence,* 2014
  http://www.risk-ch.ch → Télécharger
- OFPP: *Manuel pour les membres des organes civils de conduite*, document 1300-00-5-f, 2013.
  http://www.bevoelkerungsschutz.admin.ch/internet/bs/fr/home/dokumente/aubildungsunterlagen/fuehrungsbehelf_fuer.html
- OFPP / PLANAT: *Aversion pour le risque: Développement d'instruments systématiques pour l'évaluation du risque et de la sécurité – Rapport de synthèse,* 2008.
  http://www.bevoelkerungsschutz.admin.ch/internet/bs/fr/home/themen/gefaehrdungen-risiken/studien/risikoaversion.html
- *Stratégie nationale pour la protection des infrastructures critiques 2018 – 2022* (FF 2018 491-528).
  http://www.bevoelkerungsschutz.admin.ch/internet/bs/fr/home/themen/ski.html → Publication PIC
- *Stratégie nationale pour la protection des infrastructures critiques du 27 juin 2012* (FF 2012 7173-7196).
  http://www.bevoelkerungsschutz.admin.ch/internet/bs/fr/home/themen/ski.html → Publication PIC
- OFPP: *Glossaire des risques,* Etat: 29.4.2013
- BCMnet.CH (Business Continuity Management Network Switzerland): *Glossar, Version 1.1*, April 2013.
  http://www.bcmnet.ch/downloads/Publikationen/BCMnet-Glossar-V1.1-1.4.14.pdf
- OFAE: *Guide BCM: Ma petite entreprise / connaît pas la crise...,* n° d'art. 750.142.f, novembre 2011.
  http://www.bwl.admin.ch/dienstleistungen/01197/index.html?lang=fr
- *Directives sur la politique de gestion des risques menée par la Confédération du 24 septembre 2010* (FF 2010 5965).
  http://www.admin.ch/opc/fr/federal-gazette/2010/5965.pdf
- AFF: *Handbuch zum Risikomanagement Bund,* Version vom 29.04.2013.
  http://www.efv.admin.ch/d/downloads/finanzpolitik_grundlagen/risiko_versicherungspolitik/Handbuch_Risikomanagement_Bund.pdf
- DDPS: *Weisungen über die Massnahmen zur Aufrechterhaltung der Führungsfähigkeit des VBS (WBCM) vom 3. November 2011.*
- DDPS/PIO: *Directives sur le concept de sécurité intégrale au DDPS (DCSI) du 12 novembre 2012.*
- PLANAT: *Rapport de synthèse «Stratégie Dangers naturels en Suisse»,* 2003.
- PLANAT: *Stratégie «Dangers naturels» Suisse - Guide du concept de risque,* 2009.
- PLANAT: *Niveau de sécurité face aux dangers naturels,* août 2013
- Association suisse des banquiers: *Recommandations en matière de Business Continuity Management (BCM),* 2013.

http://www.swissbanking.org/fr/home/publikationen-link/shop.htm

Royaume-Uni:

- Business Continuity Institute: *Good Practice Guidelines* – 2010.
- British Standards Institute: BS 25999-1:2006 – *Business Continuity Management – Code of Practice.*
- British Standards Institute: BS 25999-2:2007 – *Specification for Business Continuity Management.*
- British Standards Institute: PAS 200:2011 – *Crisis Management. Guidance and Good Practice.*
- British Standards Institute: BS 31100:2011 – *Risk Management – Code of Practice and Guidance for the Implementation of BS ISO 31000.*
- British Standards Institute: Published Document 25666:2010 – *Business Continuity Management – Guidance on Exercising and Testing for Continuity and Contingency Programmes*, 2010.
- Center for the Protection of National Infrastructure: *Personnel Security Risk Assessment – A Guide,* 4th edition, 2013.
  http://www.cpni.gov.uk/documents/publications/2010/2010037-risk_assment_ed3.pdf?epslanguage=en-gb
- Center for the Protection of National Infrastructure: *Guide to Producing Operational Requirements for Security Measures*, 2013.
  http://www.cpni.gov.uk/documents/publications/2010/2010001-op_reqs.pdf?epslanguage=en-gb
- Financial Services Authority (FSA): *Business Continuity Management Practice Guide,* 2006.
  http://www.fsa.gov.uk/pubs/other/bcm_guide.pdf
- The Institute of Risk Management: *A Risk Management Standard*, 2002.

Etats-Unis:

- American National Standard: ASIS SPC.1-2009 – *Organizational Resilience: Security Preparedness, and Continuity Management Systems-Requirement with Guidance for Use*, 2009.
- National Fire Protection Association: NFPA 1600: *Standard on Disaster / Emergency Management and Business Continuity Programs*, 2010.
- Department of Homeland Security: *National Infrastructure Protection Plan*, 2013.
  https://www.dhs.gov/national-infrastructure-protection-plan

Autres auteurs et éditeurs:

- GUSTIN, Joseph F.: *Disaster & Recovery Planning: A Guide for Facility Managers*, The Fairmont Press, Lilburn GA, 2004.
- PricewaterhouseCoopers AG: *Internes Kontrollsystem – Führungssystem im Wandel*, 2007.
- Société suisse de réassurance Swiss Re: *«Präventive Schadenbewältigung: Mehr gewinnen als verlieren»*, 2001.

Annexe 2 – Indicateurs de dommages

Les 12 indicateurs de dommages ci-dessous sont tirés du document *Methode zur Risikoanalyse von Katastrophen und Notlagen für die Schweiz, Version 1.03.*

Annexe 2.1 – Victimes décédées

Description
Personnes dont le décès est dû à l'événement ou à son développement

A1	A2	A3	A4	A5	A6	A7	A8
0 – 1	2 – 3	4 – 10	11 – 30	31 – 1'00	101 – 3'00	301 – 1'000	> 1'000

Annexe 2.2 – Blessés/malades

Description

Personnes dont les blessures ou la maladie sont dues à l'événement ou à son développement. Cet indicateur regroupe toutes les formes de blessures et de maladies, physiques comme psychiques, en rapport avec la mise en danger prise en considération. On distingue les degrés suivants:

	Blessure	Maladie	Facteur
grave	Séjour à l'hôpital d'au moins sept jours. Aucune séquelle corporelle durable.	Maladie chronique, nécessité d'un traitement médical.	1
moyen	Séjour à l'hôpital d'un à six jours. Aucune séquelle corporelle durable.	Maladie grave, de longue durée, avec rétablissement complet; nécessité d'un traitement médical.	0,1
léger	Aucune séquelle corporelle durable, traitement médical mais pas de séjour à l'hôpital.	Maladie légère avec rétablissement complet, nécessité d'un traitement médical.	0,003

Les différents degrés de gravité des blessures sont pris en compte selon les facteurs de conversion indiqués.

A1	A2	A3	A4	A5	A6	A7	A8
≤ 10	101–30	31–100	101–300	301–1000	1001–3000	3001–10000	> 10'000

Les personnes qui succombent des suites de leurs blessures ou de leur maladie ne sont pas comptabilisées pour cet indicateur mais pour l'indicateur «Victimes décédées».

Annexe 2.3 – Personnes ayant besoin d'assistance

Description

Cet indicateur recense les personnes ayant dû être évacuées avant, pendant ou après l'événement, être hébergées temporairement ou ayant eu besoin d'une assistance quelle qu'elle soit. Il s'agit par exemple de l'hébergement d'urgence dans des locaux de fortune, de l'approvisionnement de personnes se trouvant dans des localités coupées du monde extérieur (denrées alimentaires) ou de l'assistance psychologique à court terme (aide psychologique d'urgence) fournie à des personnes qui ne pas physiquement atteintes. Il prend en compte la durée pendant laquelle les personnes directement touchées ont besoin d'assistance. Les conséquences telles que les problèmes et interruptions d'approvisionnement concernant une plus grande partie de la population sont comptabilisées sous l'indicateur «Problèmes/interruptions d'approvisionnement».

Le besoin d'assistance est indiqué en jours-personnes. On le calcule en multipliant le nombre de personnes ayant besoin d'assistance par la durée de la perturbation en jours. On obtient ainsi la durée effective du besoin d'assistance pour toutes les personnes touchées, la durée minimale par personne étant d'un jour. La durée prise en compte est celle pendant laquelle il existe un besoin d'assistance et non celle pendant laquelle des prestations d'assistance sont fournies. On compte par exemple le nombre de jours durant lesquels les personnes traumatisées suite à un événement requièrent une aide psychologique d'urgence et non la période durant laquelle les membres des organisations fournissant des prestations d'assistance sont engagés. Les coûts engendrés par les prestations d'assistance sont comptabilisés sous l'indicateur «Dommages patrimoniaux et coûts de maîtrise».

A1	A2	A3	A4	A5	A6	A7	A8
≤ 20'000	20'001–60'000	60'001–200'000	200'001–600'000.	600'001–2 millions	> 2–6 millions	> 6–20 millions	> 20 millions

Annexe 2.4 – Ecosystèmes dégradés

Description

Cet indicateur montre la taille de la surface, terrestre ou aquatique, qui a subi des dommages, p. ex. par des fuites de substances toxiques.

On estime qu'un écosystème est dégradé lorsque

a) l'équilibre naturel est fortement perturbé et que les systèmes doivent se régénérer

ou que

b) des fonctions essentielles de l'écosystème sont considérablement limitées (p. ex. lorsque des eaux de surface ne peuvent plus servir à l'approvisionnement en eau potable).

Les répercussions peuvent par exemple provenir d'une pollution chimique ou radiologique, d'une contamination par des espèces exotiques (néobiontes) envahissantes ou d'atteintes physiques telles que l'érosion.

Les dégradations sont indiquées en *surface par année (km^2 x ans)*. Le résultat est obtenu en multipliant la surface dégradée par le nombre d'années qu'a duré la dégradation. Lorsqu'une surface est touchée par des dégradations de plusieurs sortes, elle n'est comptabilisée qu'une fois.

Les conséquences d'une dégradation des écosystèmes (p. ex. limitations de l'approvisionnement en biens et prestations vitaux comme des problèmes d'approvisionnement en eau potable jusqu'à ce que la logistique nécessaire soit mise en place) ne sont pas prises en considération ici. Elles sont recensées sous différents indicateurs (p.ex. détérioration de la qualité de vie).

A1	A2	A3	A4	A5	A6	A7	A8
≤ 15	16–45	> 45–150	> 150–450	> 450–1500	> 1500–4500	> 4500–15'000	> 15'000

Annexe 2.5 – Dommages patrimoniaux et coûts de maîtrise

Description

L'indicateur mesure les dommages subis par les valeurs patrimoniales existantes et les coûts de maîtrise.

Le patrimoine se compose d'une part de biens immobiliers et d'autre part de patrimoine financier. Cet indicateur prend en considération tous les dommages portant atteinte à la fortune, même si des compagnies d'assurance ou l'Etat remboursent les coûts.

Les coûts de maîtrise englobent par exemple les coûts des forces d'intervention ou les coûts des hébergements d'urgence et de la prise en charge des personnes ayant besoin d'assistance.

Cas de figure «inondations»: des inondations provoquent des dommages à plusieurs bâtiments ainsi qu'à une entreprise de production. Le pompage des caves et l'enlèvement des gravats et du bois flottant engendrent des coûts (de maîtrise). Les dommages matériels sont des dommages patrimoniaux car les bâtiments et installations ont perdu de la valeur suite au sinistre.

En fonction des répercussions d'une mise en danger, on peut choisir des points de vue différents pour évaluer les dommages patrimoniaux:

• Point de vue économique global: coûts de maîtrise et dommages patrimoniaux pour toute la Suisse.

• Point de vue individuel ou local: coûts de maîtrise et dommages patrimoniaux pour les particuliers ou pour une entité limitée géographiquement.

A1	A2	A3	A4	A5	A6	A7	A8
≤ 5 millions	6–15 millions	> 15–50 millions	> 50 millions–150 millions	> 150 millions – 500 millions	> 500 millions –1,5 milliards	> 1,5–5 milliards	> 5 milliards

Annexe 2.6 – Réduction de la capacité économique

Description

Cet indicateur couvre les conséquences économiques indirectes qui réduisent la création de valeur en Suisse.

Tandis que l'indicateur «Dommages patrimoniaux et coûts de maîtrise» (cf. annexe 2.5) englobe les coûts de maîtrise et les dommages au patrimoine existant, cet indicateur couvre les conséquences pour la création de valeur à venir.

Reprenons le cas de figure «inondations» présenté à l'annexe 2.5: l'entreprise touchée par les inondations doit cesser sa production pendant plusieurs semaines suite aux dommages causés par le sinistre. Elle doit par conséquent assumer des pertes de rendement.

En fonction des répercussions d'une mise en danger, on peut choisir des points de vue différents pour évaluer les dommages patrimoniaux:

• Point de vue économique global: en tant qu'indicateur de la productivité globale, on utilise la somme de la valeur créée à l'intérieur du pays. Celle-ci est quantifiée par le produit intérieur brut (PIB). Une réduction de la capacité économique correspond donc à une diminution du PIB.

• Point de vue individuel ou local: réduction de la capacité économique des personnes touchées ou d'une entité limitée géographiquement.

A1	A2	A3	A4	A5	A6	A7	A8
≤ 5 millions	6–15 millions	> 15–50 millions	> 50 millions–150 millions	> 150 millions – 500 millions	> 500 millions –1,5 milliards	> 1,5–5 milliards	> 5 milliards

Annexe 2.7 – Détérioration de la qualité de vie

Description

Cet indicateur permet d'évaluer la détérioration de la *qualité de vie* qu'entraînent pour la population les problèmes et les interruptions d'approvisionnement (remarque: les autres conséquences de défaillances, p. ex. subies par l'économie ou les dommages personnels qui peuvent en résulter sont évalués au moyen d'autres indicateurs). Cet indicateur englobe l'interruption ou une forte restriction de l'approvisionnement en biens ou prestations essentiels pour l'ensemble ou pour certaines parties de la population. Les biens et prestations sont répartis en trois groupes, en fonction de leur importance:

Importance	Biens	Prestations	Facteur
vitaux	Eau potable, denrées alimentaires de base, médicaments	Prise en charge médicale d'urgence, communication, forces d'intervention	1
très importants	Electricité, énergie de chauffage, gaz, vêtement, logement	Soins médicaux ambulatoires et stationnaires (hors soins d'urgence), soins infirmiers ambulatoires	0,3
importants	Autres denrées alimentaires, carburant	Téléphone et technologies de l'information, télévision, transport/trafic (routier, ferroviaire, fluvial, etc.)	0,1

La restriction d'approvisionnement est le résultat de la multiplication du nombre de personnes touchées par la durée des problèmes en jours. On obtient ainsi le total des jours de restriction d'approvisionnement pour toutes les personnes touchées. C'est la période durant laquelle une restriction existe réellement qui est prise en compte: on calcule par exemple la durée totale d'une interruption de l'alimentation en électricité en additionnant les temps de panne et non en comptant le nombre de jours où il y a eu une interruption quotidienne de quelques heures.

Les conséquences économiques comprennent les indicateurs «Dommages patrimoniaux et coûts de maîtrise» (annexe 2.5) et «Réduction de la capacité économique» (annexe 2.6) Les autres dommages éventuels subis par la population sont évalués au moyen des indicateurs «Victimes décédées», «Blessés/malades» et «Personnes ayant besoin d'assistance» (cf. annexes 2.1 à 2.3).

A1	A2	A3	A4	A5	A6	A7	A8
≤ 50'000	> 50'000 – 150'000	> 150'000 – 0.5 millions	> 0.5 millions – 1.5 millions	> 1.5 millions – 5 millions	> 5 millions – 15 millions	> 15 millions – 50 millions	> 50 millions

Annexe 2.8 – Restrictions touchant l'ordre public/la sécurité intérieure

Description

Cet indicateur montre le nombre de personnes vivant en Suisse pour lesquelles l'ordre public et la sécurité sont limités, et pendant combien de temps. Il correspond aux dégradations dues à des troubles internes, qui affectent la population dans sa vie quotidienne. Les restrictions se mesurent en jours-personnes. La durée minimale par personne est d'un jour.

A1	A2	A3	A4	A5	A6	A7	A8
≤ 10'000	> 10'000 – 30'000	> 30'000 – 100'000	> 100'000 - 300'000	> 300'000 - 1 millions	> 1 millions – 3 millions	> 3 millions – 10 millions	> 10 millions

Annexe 2.9 – Perte de confiance en l'Etat/les institutions

Description

Cet indicateur révèle l'intensité d'une dégradation de la confiance en l'Etat dans son ensemble et en ses institutions, ainsi que la proportion de la population qui a perdu confiance. Les institutions englobent les organes exécutifs, législatifs et judiciaires, au niveau fédéral et cantonal, tels que les administrations, l'armée ou encore la police. Mais cela vaut également pour les infrastructures critiques, car la population s'attend à ce que la disponibilité des biens et services essentiels tels que l'électricité, l'eau, le gaz, etc. ne soit pas sérieusement compromise en Suisse.

La gravité de la perte de confiance est décrite de manière qualitative.

A1	A2	A3	A4	A5	A6	A7	A8
Perte de confiance inexistante ou limitée à quelques jours et portant sur des thèmes secondaires (p. ex. comptes rendus critiques dans les médias suisses)	Perte de confiance d'une durée allant de plusieurs jours à quelques semaines, portant sur des thèmes secondaires (p. ex. comptes rendus critiques dans les médias suisses)	Perte de confiance limitée à quelques jours et portant sur des thèmes de moyenne importance (p. ex. comptes rendus très critiques dans les médias suisses)	Perte de confiance durant entre une et quelques semaines et touchant à des thèmes de moyenne importance (p. ex. comptes rendus très critiques dans les médias suisses, manifestations isolées)	Perte de confiance durant entre une et quelques semaines et touchant à des thèmes importants (p. ex. comptes rendus extrêmement critiques dans les médias suisses; manifestations isolées)	Perte de confiance pouvant durer quelques semaines et touchant à des thèmes importants (p. ex. grèves, manifestations majeures)	Perte de confiance durant plusieurs semaines et touchant à des thèmes importants (p. ex. grèves multiples, manifestations de masse isolées)	Perte importante et généralisée de la confiance, durant plusieurs semaines (p. ex. grèves de longue durée dans de nombreux secteurs, manifestations de masse dans tout le pays)

Annexe 2.10 – Atteinte à la réputation

Description

Cet indicateur reflète l'intensité et la durée d'une atteinte à l'image de la Suisse à l'étranger: en d'autres termes, il montre dans quelle mesure la réputation de la Suisse est entachée et les partenariats du pays dans le cadre d'accords bilatéraux, multilatéraux et internationaux sont remis en cause. Cet indicateur prend en compte tant l'importance de l'atteinte à la réputation que sa durée.

A1	A2	A3	A4	A5	A6	A7	A8
Atteinte à la réputation durant un ou deux jours et touchant à des thèmes de faible importance (p. ex. échos négatifs dans quelques médias étrangers)	Atteinte à la réputation durant un ou deux jours voire plus et touchant à des thèmes de faible importance (p. ex. échos négatifs dans de nombreux médias étrangers)	Atteinte à la réputation durant un ou deux jours et touchant à des thèmes de moyenne importance (p. ex. échos négatifs dans quelques médias étrangers)	Atteinte à la réputation durant un ou deux jours voire plus et touchant à des thèmes de moyenne importance (p. ex. échos négatifs dans de nombreux médias étrangers)	Atteinte à la réputation durant plusieurs jours et touchant à des thèmes de moyenne importance (p. ex. échos très négatifs dans quelques médias étrangers)	Atteinte à la réputation durant une voire plusieurs semaines et touchant à des thèmes de moyenne importance (p. ex. échos très négatifs dans de nombreux médias étrangers)	Atteinte à la réputation durant plusieurs semaines (p. ex. échos négatifs dans presque tous les médias étrangers importants)	Grave atteinte à la réputation durant plusieurs semaines (p. ex. échos très négatifs dans presque tous les médias étrangers importants)

Annexe 2.11 – Endommagement/perte de biens culturels

Description

Cet indicateur mesure la dégradation ou la perte de biens culturels suisses. Les biens culturels dignes de protection comprennent les biens meubles et immeubles revêtant une grande importance pour l'héritage culturel des peuples. Il s'agit par exemple d'édifices, d'œuvres d'art, de monuments commémoratifs, de sites archéologiques, de livres, de manuscrits, de collections scientifiques, d'archives ou de reproductions de biens culturels. Les bâtiments tels que les musées, les bibliothèques, les archives, les couvents ou encore les lieux où les biens culturels meubles peuvent être mis en sécurité font également partie de ce patrimoine (cf. Convention de La Haye de 1954, art. 1).

On distingue les biens culturels selon que leur importance est locale ou régionale (objets B) ou nationale (objets A); il existe en outre une catégorie comprenant les objets sous «protection renforcée» (selon la Commission fédérale de la protection des biens culturels).

On entend par «endommagement» tout effet grave subi par un bien culturel qui entraîne sa destruction ou une dégradation telle qu'une restauration ou reconstruction nécessiterait un travail long et onéreux. «Perte» désigne la disparition (vol) ou la destruction irréversible d'un bien culturel (due p. ex. à un incendie, à une explosion ou à une inondation).

A1	A2	A3	A4	A5	A6	A7	A8
Quelques dommages éventuels ou perte de quelques BC d'importance locale	Endommagement ou perte de plusieurs BC d'importance locale	Quelques dommages éventuels ou perte de quelques BC d'importance régionale	Endommagement ou perte de plusieurs BC d'importance régionale ou de quelques BC d'importance nationale	Endommagement ou perte de plusieurs BC d'importance régionale et de quelques BC d'importance nationale	Endommagement ou perte de plusieurs BC d'importance nationale	Endommagement ou perte de nombreux BC d'importance nationale	Endommagement ou perte de nombreux BC d'importance nationale et de BC sous «protection renforcée»

Annexe 3 – Indicateurs permettant d'évaluer la probabilité d'occurrence / plausibilité

Le tableau ci-dessous propose des indicateurs permettant d'évaluer la probabilité d'occurrence et la plausibilité des scénarios[20].

Classe P	Description	Probabilité	1 x tous les ... ans	Fréquence (1/an)
P 8	Survient en Suisse en moyenne peu de fois pendant la durée d'une vie humaine.	> 30 %	< 30	> $3*10^{-2}$
P 7	Survient en Suisse en moyenne une fois pendant la durée d'une vie humaine.	10 - 30 %	30 - 100	$3*10^{-2}$ - 10^{-2}
P 6	S'est déjà produit en Suisse, mais peut remonter à plusieurs générations.	3 - 10 %	100 - 300	10^{-2} - $3*10^{-3}$
P 5	Ne s'est peut-être pas encore produit en Suisse mais s'est produit à l'étranger selon informations disponibles.	1 - 3 %	300 - 1000	$3*10^{-3}$ - 10^{-3}
P 4	S'est produit à plusieurs reprises dans le monde selon informations disponibles.	0,3 - 1 %	1000 - 3000	10^{-3} - $3*10^{-4}$
P 3	S'est produit de rares fois dans le monde selon informations disponibles.	0,1 – 0,3 %	3000 – 10 000	$3*10^{-4}$ - 10^{-4}
P 2	S'est produit de manière isolée dans le monde selon informations disponibles mais est possible en Suisse.	003 – 0,1 %	10 000 – 30 000	10^{-4} - $3*10^{-5}$
P 1	Si tant est qu'il se soit produit, n'est survenu qu'à de rares reprises dans le monde selon informations disponibles. Un tel événement, bien que se produisant très rarement dans le monde, ne peut être totalement exclu en Suisse.	< 0,03%	> 30 000	< $3*10^{-5}$

Proposition d'indicateurs pour l'évaluation de la probabilité d'occurrence

Selon la nomenclature ci-dessus, la fréquence correspond au nombre d'événements (attendus) par unité de temps. En général, la fréquence est indiquée en nombre d'événements par année (p. ex. nombre d'avalanches se produisant en Suisse par an).

Probabilité

La probabilité se rapporte à un événement susceptible de se produire et indique dans quelle mesure il est probable qu'il se produise réellement. Une valeur entre 0 et 1 lui est attribuée, qui peut aussi se traduire par une valeur entre 0 et 100 %.

La fréquence indique le nombre d'événements auxquels on peut s'attendre sur une période donnée, tandis que la probabilité désigne la possibilité d'occurrence d'un événement lorsque les conditions sont réunies pour ce cas précis.

S'agissant de menaces d'origine naturelle ou technique, la probabilité et la fréquence d'un scénario de danger sont déterminées avec autant de précision que possible, par exemple en se fondant sur des statistiques ou des estimations de spécialistes lorsque les données de référence sont insuffisantes.

[20] Ces échelles se fondent sur la méthode et les travaux relatifs aux *Catastrophes et situations d'urgence en Suisse* (2013).

Plausibilité

La menace pouvant évoluer rapidement, il n'est pas toujours possible d'attribuer une fréquence ou probabilité d'occurrence précise aux événements provoqués intentionnellement, p. ex. en relation avec des événements politiques, des attentats terroristes ou des conflits armés. Pour les mises en danger de ce type, on peut estimer la plausibilité qu'un tel événement survienne (p. ex. au cours des dix prochaines années).

Comme pour la probabilité et la fréquence, une classe de plausibilité peut être attribuée à chaque scénario de danger[21].

[21] Cf. *Methode zur Risikoanalyse von Katastrophen und Notlagen für die Schweiz*, Version 1.03, 17. April 2013, p. 8 (tableau 3: classes de plausibilité).

Annexe 4 – Coûts marginaux et facteur d'aversion

Annexe 4.1 – Exemples de coûts marginaux

Indicateur	Coûts marginaux par unité
Victimes décédées	CHF 4 millions
Blessés/malades	CHF 400 000
Personnes ayant besoin d'assistance	CHF 250
Ecosystèmes dégradés	CHF 11 500
Dommages patrimoniaux et coûts de maîtrise	CHF 1
Réduction de la capacité économique	CHF 1
Dégradation de la qualité de vie	CHF 500
Restrictions touchant l'ordre public/la sécurité intérieure	CHF 300
Perte de confiance en l'Etat/les institutions	A1: 2.5 millions; A2: 10 millions; A3: 32.5 millions; A4: 100 millions; A5: 325 millions; A6: 1 milliard; A7: 3.25 milliards; A8: 10 milliards
Atteinte à la réputation	A1: 2.5 millions; A2: 10 millions; A3: 32.5 millions; A4: 100 millions; A5: 325 millions; A6: 1 milliard; A7: 3.25 milliards; A8: 10 milliards
Endommagement/perte de biens culturels	A1: 2.5 millions; A2: 10 millions; A3: 32.5 millions; A4: 100 millions; A5: 325 millions; A6: 1 milliard; A7: 3.25 milliards; A8: 10 milliards

Source: *Methode zur Risikoanalyse von Katastrophen und Notlagen für die Schweiz*, Version 1.03, Stand 17. April 2013 - tableau. 5, p. 23.

Annexe 4.2 – Propositions relatives au facteur d'aversion

Une étude menée conjointement par l'OFPP et PLANAT en 2008 propose un facteur d'aversion φ, auquel sont subordonnés les trois effets découlant de l'incertitude croissante:

- φ1: incertitude dans l'estimation de la probabilité d'occurrence
- φ2: incertitude dans l'estimation des dommages
- φ3: incertitude quant à l'attitude intrinsèque face au risque.

Ces trois facteurs sont déterminés individuellement pour l'application pratique, puis réunis en un seul facteur φ.

Quantification du facteur d'aversion φ:

On procède tout d'abord à une estimation des facteurs partiels φ1 et φ2, correspondant respectivement à l'incertitude quant à la probabilité d'occurrence *p* et à celle de l'estimation de l'ampleur des dommages *A*, en tenant compte d'un intervalle de confiance de 95 % (env. 2σ). Les deux facteurs partiels φ1 et φ2 sont ensuite réunis en un facteur φ 1+2, dont les valeurs figurent dans le tableau ci-dessous:

Nombre de victimes décédées	1	10	100	1'000	10'000	100'000	1'000'000
Probabilité d'occurrence par année	5.0 p+00	1.1 p-01	6.2 p-03	2.8 p-04	1.8 p-05	2.4 p-06	5.0 p-07
Facteur φ_{1+2}	1.0	1.25	1.5	1.8	2.15	2.5	2.9

La seconde estimation s'applique au facteur partiel φ3, lequel concerne l'aversion au sens strict. La question de savoir dans quelle mesure la collectivité doit tenir compte de ces effets partiels ne nécessite pas de réponse objective. Cette détermination devrait théoriquement être le fait, p. ex., d'un groupe de personnes bien informées, représentatif d'une tranche de la population, au sens d'un public de substitution. Vu l'envergure et l'exigence d'une telle démarche toutefois, l'étude de l'aversion pour le risque de 2008 propose les valeurs suivantes:

Nombre de victimes décédées	1	10	100	1'000	10'000	100'000	1'000'000
Facteur φ_3	1.0	1.3	1.8	2.5	3.2	3.8	4.0

La combinaison des facteurs partiels φ1+2 et φ3 s'opère selon une multiplication, pour aboutir à la formule suivante:

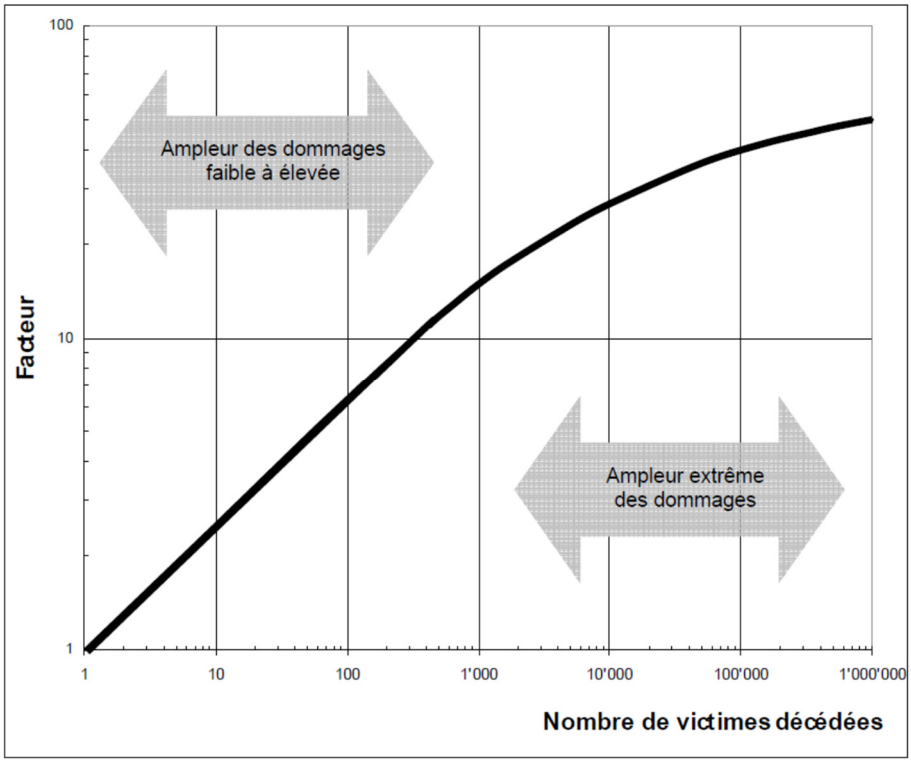
$$R_m = \sum_i p_i \cdot A_i \cdot f_i \cdot \varphi_i \cdot CM$$

où:

i	index de scénarios
R_m	risque monétarisé de tous les scénarios
p_{ii}	probabilité d'occurrence [/année]
A_i	ampleur des dommages [victimes décédées]
f_i	facteur complémentaire de dommage
φ_i =	$(\varphi_{1+2} * \varphi_3)$: facteur d'aversion
CM	coûts marginaux

L'effet cumulé de ces facteurs est représenté dans la figure ci-après.

Les facteurs partiels ont en outre été réunis au sein d'un facteur général comparable aux facteurs d'aversion existants. Sont distingués ici deux domaines relatifs à l'ampleur des dommages A: d'une part le domaine délimitant une ampleur des dommages faible à élevée (jusqu'à 1000 morts), d'autre part le domaine délimitant une ampleur extrême des dommages (de 1000 à 1 million de morts).



Adapté à partir de: OFPP/PLANAT: *Aversion pour le risque. Développement d'instruments systématiques pour l'évaluation du risque et de la sécurité. Rapport de synthèse*. Berne, 2008, p. 15 à 17

Annexe 5 – Exemples de mesures de protection

Annexe 5.1 – Exemples de mesures techniques et architecturales

Mesures techniques et architecturales

Situation de l'objet

- Protection contre les dangers naturels (inondations, séismes, raz-de-marée, glissements de terrain et éboulements, avalanches, tempêtes, etc.)
- Distance par rapport aux bâtiments voisins
- Eviter une architecture fermée (l'accès par les toits adjacents ou autre est plus difficile)
- Protection contre les dangers d'origine technique (centrales nucléaires, incidents chimiques, etc.)

Structure de la construction

- Liaisons permettant le transit (sorties de secours)
- Protection contre les entrées non autorisées ou violentes
- Situation du bâtiment à protéger
- Façades planes (aucune partie saillante)
- Aucun élément susceptible d'aider à escalader les façades
- Conduites et raccordements d'approvisionnement enterrés ou sécurisés
- Prises extérieures pouvant être mises hors tension

Protection de l'accès

- Clôture (aucune ouverture, sans risque de perforation, hauteur minimale, protection contre un accès par le haut (fil de fer barbelé), protection anti-reptation, surveillance vidéo)
- Portes protégées contre les intrusions
- Contrôles techniques de l'accès (interphone, vidéo, fonction de sas, lecteur de carte d'identification, codes chiffrés sur clavier, etc.)
- Détection électronique automatique (clôtures et portes sous alarme, système vidéo pourvu de capteurs, protection du haut du mur, balayage radar, détecteurs photoélectriques à haute fréquence, alarme antieffraction)
- Eclairage extérieur (si possible sans ombre portée et d'utilisation sûre)
- Personnel engagé pour le contrôle des moyens électroniques de détection
- Personnel de surveillance qualifié, prêt à intervenir et correctement équipé (p. ex. détecteurs thermiques ou dispositifs de vision nocturne)
- Des plantations dans la propriété réduisent la possibilité de passer outre les mesures de protection techniques et architecturales

Protection du bâtiment

- Pour les domaines sensibles: bâtiment à l'abri des regards
- Pour les domaines sensibles: renoncer à fournir des plans de situation
- Domaine de la sécurité séparé
- Protection des domaines de la sécurité séparés (électronique, mécanique, contrôles d'accès, surveillance spéciale)
- Alarme antieffraction aux portes, fenêtres, puits de lumière
- Grillages aux fenêtres
- Protection des puits de lumière (grille de protection fixe, sécurité empêchant de la soulever)
- Protection des puits d'approvisionnement et d'évacuation (grille)
- Protection des fenêtres souvent ouvertes (p. ex. dans les toilettes) par une grille
- Vitre de sécurité dans les domaines de sécurité spéciaux
- Fenêtre de protection (ferrures antieffraction, verre de sécurité feuilleté résistant aux impacts, poignées de fenêtres verrouillables, parcloses vissées)
- Nombre limité de portes donnant sur l'extérieur
- Protection de l'entrée principale (lecteur de carte ou de puce, serrures couplées/à verrouillage automatique, gâche de sécurité électrique, ferme-portes de sécurité automatique, interphone, sas, séparation entre l'entrée et la sortie)
- Protection des sorties de secours (serrures à verrouillage automatique, ferme-portes automatique, portes sous alarme)
- Remise des clés uniquement aux personnes autorisées
- Conservation en sécurité des clés de réserve
- Gestion des autorisations relatives aux accès

Protection contre l'incendie

- Protection contre la foudre
- Respect des prescriptions de protection contre l'incendie
- Planification et exercices de protection contre l'incendie
- Permanence assurée à proximité de l'installation de signalisation des dangers

…etc.…

Annexe 5.2 – Exemples de mesures organisationnelles et administratives

Mesures organisationnelles et administratives

Internes à l'entreprise

- Responsable de la sécurité
- Personnel de sécurité appartenant à l'entreprise (connaissant bien les prescriptions légales nécessaires à l'exercice de ses fonctions, les obligations spécifiques et habilitations, ainsi que leur application pratique)
- Directives claires concernant les exigences légales et normes relatives à la sécurité
- Exigences de sécurité réglementées (p. ex. guides, directives)
- Enregistrement des incidents touchant à la sécurité
- Conséquences tirées de ces incidents
- Connaissances du personnel dans les domaines de la sécurité au travail, de la lutte contre l'incendie, des premiers secours
- Identification des dangers potentiels et des éléments d'alerte précoce
- Inventaire des processus, objets, systèmes et éléments critiques
- Liste des substances dangereuses
- Plan de toutes les conduites d'approvisionnement et d'évacuation (p. ex. électricité, eau, gaz, téléphone, etc.)
- Plans pour les différents scénarios de menaces
- Stratégie de montée en puissance en cas d'incident affectant la sécurité
- Plan de transmission de l'alarme
- Règles de comportement et voies de communication en cas d'incident affectant la sécurité
- Information concernant les sorties de secours
- Exercices d'évacuation
- Exercices, maintien (p. ex. en cas d'incident dans les environs)
- Exercices de lutte contre l'incendie
- Prise en compte des connaissances acquises lors des exercices effectués en formation
- Communication de crise
- Assistance psychologique pendant les incidents affectant la sécurité

Externe à l'entreprise

- Commutation de secours pour la télécommunication
- Système intégral et indépendant de gestion de la sécurité (c.-à-d. uniquement aux mains de l'entreprise)
- Accords entre l'entreprise et le fournisseur de services de sécurité (structure de contrats, collaboration pratique, compétences en cas de crise)
- Formation/perfectionnement du personnel de sécurité
- Analyse de la criticité de l'externalisation (*Outsourcing*) des prestations
- Evitement de la mise à disposition *Open Source* (p. ex. prises de vue aériennes de l'entreprise sur internet, etc.)

… etc. …

Annexe 5.3 – Exemples de mesures relatives au personnel

Mesures de protection relatives au personnel

Personnel (interne et externe)

- Contrôle de sécurité des collaborateurs (internes et externes)
- Obligation pour le personnel de se conformer aux lois, aux obligations, aux prescriptions, aux réglementations internes, etc.
- Sensibilisation du personnel aux questions relatives à la sécurité (formations, exercices, séminaires, exercices en équipe, etc.)
- Recrutement (expérience, connaissance, contrôle des données personnelles (extrait de casier judiciaire, etc.), intégrité, vérification des références)
- Sortie (reddition de tous les documents, du matériel de bureau, des clés, des mots de passe, des badges, etc., *accord de non-divulgation,* etc.)
- Protection des cadres (protection des personnes, etc.)

Personnes étrangères à l'entreprise

- Inscription de l'arrivée et du départ dans le registre des visiteurs
- Rapide identification des visiteurs (p. ex. badge visiteur)
- Accompagnement/surveillance des visiteurs
- Contrôle des livreurs et des marchandises

… etc. …

Annexe 5.4 – Exemples de mesures juridiques

Mesures de protection juridiques

Contrats et service-level agreements concernant

- Stockage et moyens de production supplémentaires dans un autre site
- Arrangements avec des prestataires externes pour livrer les moyens de production requis dans des délais brefs
- Convention de déviation des livraisons aux délais très serrés vers d'autres sites
- Stockage de moyens de production dans des entrepôts sécurisés ou emplacements en vue du transport maritime
- Transfert de certaines étapes de production dans d'autres sites disposant des moyens de production nécessaires
- Accord quant à l'utilisation d'autres moyens de production
- Accords contractuels pour les situations d'urgence

… etc. …

Annexe 5.5 – Exemples de mesures permettant de garantir la continuité des activités

Mesures permettant de garantir la continuité des activités

Garantir la continuité des fonctions clés
L'entreprise doit élaborer des stratégies adéquates en vue de maintenir les connaissances et compétences essentielles en son sein:

- Documentation sur la manière de réaliser les processus et les activités critiques
- Entraînement polyvalent (*multi-skills)* pour les principaux collaborateurs et prestataires
- Partage des activités essentielles (*core-skills)* afin d'éviter une concentration inutile des risques
- Participation de tiers
- Planification de la succession réglementée
- Protection et gestion du savoir-faire

Garantie d'autres emplacements ou locaux pour poursuivre les activités
L'entreprise doit avoir une stratégie claire pour minimiser les conséquences de l'indisponibilité d'une succursale ou de locaux:

- Possibilité d'utiliser des locaux séparés, dans une autre succursale ou un autre site appartenant à l'entreprise
- Possibilité d'utiliser des locaux séparés, dans une autre succursale ou un autre site hors de l'entreprise (p. ex. chez des entreprises partenaires, etc.)
- Possibilité d'utiliser des locaux séparés, dans une autre succursale ou un autre site chez des prestataires externes
- Possibilité de travail à domicile et de postes de travail avec accès à distance
- Possibilité de recourir à d'autres ressources (personnel), dans d'autres locaux ou d'autres succursales/sites

Rétablissement de la capacité opérationnelle de la technique/technologie et disponibilité d'alternatives (en particulier pour les TIC)
Le type de stratégie retenue dépend fortement des technologies utilisées dans l'entreprise:

- répartition géographique des installations et ressources technologiques
- disponibilité d'installations et ressources technologiques de remplacement

Il faut en outre choisir des stratégies propres à la technologie de l'information:

- Identification et définition des RTO (durée maximale d'interruption admissible), surtout pour les activités et processus considérés comme critiques
- Répartition géographique et distance entre les emplacements clés du point de vue de la technologie
- Nombre d'emplacements clés du point de vue de la technologie
- Accès à distance
- Utilisation d'emplacements sans personnel (*un-staffed / dark)*
- Liaisons de télécommunication et redondance des lignes
- Type de «basculement» (failover): démarrage manuel ou automatique des systèmes redondants
- Liaisons via des tiers (prestataires externes)

Sauvegarde/restauration d'informations
Les informations essentielles pour que l'objet critique puisse fonctionner doivent être protégées et doivent pouvoir être restaurées (conformément aux délais fixés dans l'analyse). Vous trouverez des informations complémentaires à ce sujet dans la norme BS ISO/IEC 27001.

Les éléments suivants doivent être garantis pour toute information nécessaire au fonctionnement des processus critiques ou de l'objet:

- confidentialité;
- intégrité;
- disponibilité;
- actualité (validité);
- copies physiques;
- copies électroniques.

Garantie de la disponibilité des prestations externes:
L'entreprise doit établir une liste des moyens de production essentiels aux processus et aux objets critiques. On prendra également en considération les points suivants:

- Stockage de moyens de production supplémentaires dans un autre site
- Arrangements avec des prestataires externes pour la livraison des moyens de production nécessaires dans les délais les plus brefs
- Convention de déviation des livraisons aux délais très serrés vers d'autres sites
- Stockage de moyens de production dans des entrepôts sécurisés ou emplacements en vue du transport maritime
- Transfert de certaines étapes de production dans d'autres sites disposant des moyens de production nécessaires
- Identification de moyens de production de remplacement

- Augmentation du nombre de sous-traitants (pour réduire la dépendance vis-à-vis d'un seul sous-traitant)
- Promotion des stratégies de BCM auprès des sous-traitants
- Accords contractuels pour les situations d'urgence
- Identification de sous-traitants de remplacement

… etc. …

Annexe 6 – Concept de protection intégrale. Proposition de structure d'un rapport général

Résumé

1. **Introduction**
   - Situation de départ
   - Objectifs du rapport
   - Organes participant à son élaboration

2. **Documents de base et travaux préalables**
   - Documents généraux
   - Bases légales
   - Travaux préalables

3. **Analyse**
   - Description de l'infrastructure critique
   - Désignation des processus critiques
   - Identification des ressources et des vulnérabilités importantes
   - Analyse des risques
   - Mesures d'urgence éventuelles

4. **Evaluation**
   - Evaluation en fonction des prescriptions en vigueur
   - Définition des risques prioritaires
   - Détermination des coûts marginaux et du facteur d'aversion
   - Quantification des risques / vue d'ensemble des risques

5. **Mesures (de protection)**
   - Vue d'ensemble des mesures possibles
   - Choix des mesures prioritaires et coûts correspondants
   - Détermination de la combinaison optimale des mesures
   - Pesée générale des intérêts
   - Implémentation des mesures (adaptation en fonction des bases légales)
   - Recommandations pour la mise en œuvre (compétences, procédure), contrôle et actualisation
   - Fixation des modalités des comptes rendus et de vérification de l'avancement de la mise en œuvre des différentes mesures

6. **Suite des opérations**
   - Requête concernant la suite de la procédure

Annexes
- Documentation relative aux processus critiques
- Liste des experts et organes spécialisés contactés

Annexe 7 – Secteurs et sous-secteurs critiques

Secteurs	Sous-secteurs
Autorités	Recherche et enseignement
	Biens culturels
	Parlement, gouvernement, justice, administration
Énergie	Approvisionnement en gaz naturel
	Approvisionnement en pétrole
	Approvisionnement en électricité
	Chauffage à distance et production de chaleur industrielle
Élimination	Déchets
	Eaux usées
Finances	Services financiers
	Services d'assurance
Santé	Soins médicaux
	Prestations de laboratoires
	Chimie et produits thérapeutiques
Information et Communication	Services informatiques
	Télécommunications
	Médias
	Services postaux
Alimentation	Approvisionnement en denrées alimentaires
	Approvisionnement en eau
Sécurité publique	Armée
	Organisations d'urgence (police, sapeurs-pompiers, services sanitaires)
	Protection civile
Transports	Trafic aérien
	Trafic ferroviaire
	Trafic fluvial
	Trafic routier

Source: *Stratégie nationale pour la protection des infrastructures critiques 2018* , FF 2018 491.

Annexe 8 – Services fédéraux assurant la coordination

Secteur	Sous-secteur	Organes fédéraux compétents (liste non exhaustive)*
Autorités	Recherche et enseignement	SEFRI
	Biens culturels	OFPP, OFC
	Parlement, gouvernement, justice, administration	SP, ChF, DFAE, MétéoSuisse, fedpol, SIO, SRC, AFF, UPIC et FP, OFEV
Énergie	Approvisionnement en gaz naturel	OFEN, IFP, OFAE
	Approvisionnement en pétrole	OFEN, IFP, OFAE
	Approvisionnement en électricité	OFEN, ElCom, ESTI, IFSN, OFAE
	Chauffage à distance et chaleur industrielle	OFEN
Élimination	Déchets	OFEV
	Eaux usées	OFEV
Finances	Services financiers	FINMA, AFF, SFI, OFAE, OFCOM
	Assurances	FINMA, AFF, SFI, OFAS
Santé	Soins médicaux	SSC, OFSP
	Services de laboratoires	OFSP, OSAV, OFPP
	Produits chimiques et thérapeutiques	OFAE, Swissmedic, Pharmacie de l'armée
Information et communication	services informatiques	OFAE, UPIC
	Télécommunications	OFCOM, OFAE
	Médias	OFCOM
	Services postaux	OFCOM, OFAE
Alimentation	Approvisionnement en denrées alimentaires	OFAE, OFAG
	Approvisionnement en eau	OFEV, OFAE
Sécurité publique	Armée	Groupement Défense
	Organisations d'urgence (police, sapeurs-pompiers, services sanitaires)	fedpol, OFPP
	Protection civile	OFPP
Transports	Trafic aérien	OFAC, OFAE
	Trafic ferroviaire	OFT, OFAE
	Trafic fluvial	OFT, OFAE
	Trafic routier	OFROU, OFAE

* Les organes mentionnés, en collaboration avec le secrétariat PIC, désignent les autres organes responsables en matière de vérification et d'amélioration de la résilience qu'il convient d'impliquer (Confédération, cantons, organisations, etc.). Les compétences en vigueur restent inchangées.

Abréviations des services fédéraux compétents

AFF	Administration fédérale des finances
BNS	Banque nationale suisse
DDPS	Département fédéral de la défense, de la protection de la population et des sports
DETEC	Département fédéral de l'environnement, des transports, de l'énergie et de la communication

DFAE	Département fédéral des affaires étrangères
ElCom	Commission fédérale de l'électricité
ESTI	Inspection fédérale des installations à courant fort
fedpol	Office fédéral de la police
FINMA	Autorité fédérale de surveillance des marchés financiers
IFP	Inspection fédérale des pipelines
IFSN	Inspection fédérale de la sécurité nucléaire
OFAC	Office fédéral de l'aviation civile
OFAE	Office fédéral pour l'approvisionnement économique du pays
OFAG	Office fédéral de l'agriculture
OFAS	Office fédéral des assurances sociales
OFC	Office fédéral de la culture
OFCL	Office fédéral des constructions et de la logistique
OFCOM	Office fédéral de la communication
OFEN	Office fédéral de l'énergie
OFEV	Office fédéral de l'environnement
OFPP	Office fédéral de la protection de la population
OFROU	Office fédéral des routes
OFSP	Office fédéral de la santé publique
OFT	Office fédéral des transports
PIO	Protection des informations et des objets (Etat-major de l'armée, DDPS)
SEFRI	Secrétariat d'Etat à la formation, à la recherche et à l'innovation
SFI	Secrétariat d'Etat aux questions financières internationales
SG DETEC	Secrétariat général du DETEC
SRC	Service de renseignement de la Confédération
SSC	Service sanitaire coordonné
UPIC	Unité de pilotage informatique de la Confédération