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 cybersécurité OFCS

24 novembre 2025

Les systèmes de gestion et la méthode de cybersécurité et de résilience

1 Contexte

La présente annexe propose un aperçu concis de trois approches relatives à la cyberrésilience : la norme minimale en matière de TIC (ou le *NIST Cyber Security Framework [CSF]*), la norme ISO/CEI 27001 et la méthode de cybersécurité et de résilience (MCSR). La MCSR est comparée aux deux autres méthodes sur le plan du contenu et de la forme, puis classée en fonction de son adéquation en tant que méthode de gestion, de pilotage et de preuve de la cyberrésilience des organisations ou des entreprises. Le texte se concentre sur l'essentiel et complète le document principal sans pour autant en répéter le contenu.

Le document s'adresse en particulier aux membres de la direction de l'entreprise et des départements, aux responsables de la sécurité de l'information (*chief information security officers*, CISO) ainsi qu'aux propriétaires de risques (*risk owners*), de services (*service owners*) ou d'actifs (*asset owners*). Il est destiné aux organisations et aux entreprises appliquant déjà la norme minimale en matière de TIC ou la norme ISO/CEI 27001 et qui souhaitent évaluer la transition ou le complément vers la MCSR.

La présente annexe a pour objectif de fournir une orientation claire et comparative : quelles sont la logique, les forces et les limites de la norme minimale en matière de TIC et de la norme ISO/CEI 27001 ; en quoi la MCSR se distingue-t-elle – en ce qui concerne la méthode, les décisions et les preuves – et quelle valeur ajoutée apporte-t-elle dans la pratique ? Par ailleurs, le texte sert d'aide à la décision en indiquant comment transférer les implémentations existantes vers la MCSR.

2 Norme minimale en matière de TIC et NIST CSF

La norme minimale en matière de TIC s'appuie sur le NIST CSF et le complète par des aspects de protection propres aux technologies opérationnelles (TO). Comme elle ne s'en écarte que légèrement (version 1.1), les considérations qui suivent s'appliquent, sauf indication contraire, aux deux cadres sans distinction.

La norme minimale en matière de TIC décrit une série de mesures organisationnelles et techniques à mettre en œuvre en fonction des besoins de protection identifiés. Il n'existe pas d'exigences minimales fixes à cet égard. Les besoins de protection sont déterminés à l'aide d'une évaluation probabiliste des risques. À cette fin, le NIST recommande l'utilisation du *NIST*

Risk Management Framework (RMF)[1]. Les dépendances entre les systèmes informatiques et les processus ayant un impact sur l'activité sont examinées séparément dans le cadre de la gestion des risques.

Un élément central de la mise en œuvre consiste à élaborer des directives et des stratégies internes, dont l'application cohérente doit être garantie au sein de l'organisation. Cela rend toutefois plus difficile la comparaison des implémentations entre les organisations. La norme minimale en matière de TIC sert elle-même de cadre permettant aux organisations, aux associations ou aux régulateurs de créer des profils spécifiques[2] définissant les mesures à mettre en œuvre ainsi que leur niveau d'exigence. La norme utilise à cet effet des degrés de maturité (*tiers*) fixes. Cette flexibilité présente certes des avantages, mais elle n'aboutit pas de manière déterministe à un niveau de cybersécurité et de résilience.

L'Office fédéral de la cybersécurité (OFCS) estime que certaines exigences devraient toujours être introduites en tant que mesures de base, tandis que d'autres – en particulier en cas de besoin de protection accru – devraient être propres au contexte, en fonction des données, des systèmes et des architectures informatiques. Certains profils peuvent certes refléter ces exigences fondamentales, mais ils n'offrent pas de méthodologie favorisant le développement des exigences supplémentaires en cas de besoin de protection accru. En raison du grand nombre d'exigences (108 sous-catégories dans le NIST CSF v1.1 et dans la norme minimale en matière de TIC), les profils sont souvent très volumineux et donc difficiles à mettre en œuvre dans la pratique, surtout pour les petites organisations. De plus, l'utilisation de profils comme référence de base complique la comparabilité entre organisations.

La norme minimale en matière de TIC concerne la sécurité informatique et la sécurité de l'information, en particulier la protection des systèmes informatiques, des infrastructures ainsi que des informations traitées et transmises. Elle tente également de couvrir certains aspects relatifs à la sécurité opérationnelle (TO) à l'aide des mêmes exigences, sans toutefois tenir suffisamment compte des spécificités propres à ce domaine[3]. Le NIST CSF englobe la segmentation, les transitions sécurisées, la sécurité physique, le renforcement et la surveillance de manière technologiquement neutre. Les spécificités des TO et des systèmes de contrôle industriels restent volontairement abstraites et ne peuvent être concrétisées que de façon limitée dans un profil standard.

En résumé, la norme minimale en matière de TIC constitue un cadre, et non un modèle de procédure en plusieurs étapes. Elle requiert une décision basée sur les risques qui détermine les exigences applicables et les mesures à mettre en œuvre. Les profils servent à regrouper ces exigences, tandis que le modèle par degrés (*tier model*) en décrit l'ampleur et facilite l'auto-évaluation interne (*self-assessment*).

3 Norme ISO/CEI 27001

La norme ISO/CEI 27001 permet aux entreprises de mettre en place et d'exploiter un système de management de la sécurité de l'information (SMSI). Un SMSI conforme à la norme

---

[1] *NIST SP 800-37* Rev. 2, *Risk Management Framework for Information Systems and Organizations — A System Life Cycle Approach for Security and Privacy*, décembre 2018

[2] Profils de protection A, B, C ; ordonnance sur l'approvisionnement en électricité (OApEl), art. 5*a* en relation avec l'annexe 1*a* : caractère contraignant de la norme minimale en matière de TIC (« conformément au niveau de protection applicable ») et définition des niveaux de protection

[3] Les TO se distinguent des technologies de l'information (TI) notamment par des cycles de vie longs et une dépendance envers les fabricants, des possibilités de correction limitées dans des délais restreints ainsi que des exigences élevées en matière de disponibilité et de temps réel.

ISO/CEI 27001 comprend la politique, les procédures, les directives ainsi que les ressources et activités associées qu'une organisation pilote pour assurer la protection de ses informations. Visant à soutenir les objectifs d'affaires de l'organisation, il constitue un modèle systématique pour l'introduction, la mise en œuvre, l'exploitation, la surveillance, la vérification, la maintenance et l'amélioration continue de la sécurité de l'information.

Bien que la norme minimale en matière de TIC puisse aussi contribuer à la mise en place d'un SMSI, elle est avant tout conçue comme un cadre pour la gestion des cyberrisques. À l'inverse, la norme ISO/CEI 27001 propose un modèle de procédure fondé sur un cycle d'amélioration, généralement désigné sous le nom de *cycle PDCA* (*plan-do-check-act*). Elle décrit la mise en place et le fonctionnement d'un SMSI étape par étape : de la planification des objectifs et des mesures de sécurité à leur mise en œuvre et à leur surveillance continue, en passant par des améliorations et des contrôles réguliers. Le modèle de procédure favorise ainsi un processus d'amélioration itératif.

Par ailleurs, la norme ISO/CEI 27001 a pour objectif de garantir la possibilité de réaliser des audits et des certifications[4]. Elle contient des exigences permettant à des organismes de contrôle externes d'évaluer l'efficacité et la conformité du SMSI. Cette possibilité de vérification structurelle la distingue clairement de la norme minimale en matière de TIC, qui ne prévoit pas de certification formalisée.

Cependant, les deux normes présentent des similitudes sur de nombreux autres aspects.

- Les exigences applicables et les mesures (issues du catalogue correspondant) à mettre en œuvre sont déterminées dans les deux approches par une évaluation basée sur les risques et les probabilités.
- Les catalogues de mesures ne définissent ni des exigences fondamentales obligatoires ni une protection de base à mettre en œuvre indépendamment du risque.
- Ce sont les directives et les stratégies internes supplémentaires à mettre en place, et non les exigences du cadre lui-même, qui constituent la base principale pour la mise en œuvre des mesures.
- La priorité est donnée à la sécurité de l'information de l'organisation. La sécurité contre les perturbations et les incidents ne constitue pas un objectif central. L'accent est mis sur la protection de la confidentialité, sur l'intégrité et sur la disponibilité des informations et des systèmes de traitement de l'information, plutôt que sur la protection des processus d'affaires et de production eux-mêmes.

Une différence essentielle par rapport à la norme minimale en matière de TIC réside dans l'obligation de documentation et de preuve. En effet, la norme ISO/CEI 27001 ne prévoit ni niveaux ni degrés de mise en œuvre, mais toutes les mesures doivent être décrites dans une déclaration appelée *Statement of Applicability* (*SoA*) et être attribuées de manière compréhensible.

4 Méthode de cybersécurité et de résilience (MCSR OFCS)

Les différences et les atouts de la MCSR, comparée aux approches susmentionnées, sont résumés dans les sections qui suivent.

[4] OFCS, Considérations technologiques – Mesure et vérification de la sécurité informatique, Berne, 10 juin 2025 ; disponible en ligne à l'adresse : ncsc.admin.ch

Exigences fondamentales et approches en cas de besoin de protection accru

La MCSR définit 20 exigences fondamentales pour tous les systèmes TI et TO ainsi qu'une méthode de modélisation des menaces en cas de besoin de protection accru. Les exigences fondamentales sont formulées de manière à être compréhensibles pour les spécialistes en informatique, pertinentes pour la cybersécurité et la résilience, et vérifiables. Les exigences qui ne contribuent pas directement à améliorer la résilience n'ont pas été prises en compte. Le langage clair et concis facilite la mise en œuvre et permet aux entreprises et aux autorités d'atteindre une protection de base efficace. La méthode de modélisation des menaces complète les exigences fondamentales et favorise l'élaboration de mesures supplémentaires en fonction du contexte, de l'architecture et des besoins de protection.

Évaluations des risques liés aux processus d'affaires et de production

Les objectifs fondamentaux de la MCSR sont la garantie des activités importantes, des processus d'affaires et de production correspondants, la protection des biens de l'organisation ou de l'entreprise, le respect des lois et des autres prescriptions réglementaires, ainsi que la protection contre les perturbations et les incidents. Si nécessaire, des mesures techniques et organisationnelles (MTO) supplémentaires doivent être définies et mises en œuvre en plus de celles répondant aux exigences fondamentales.

Un modèle de procédure plutôt qu'un cadre

La MCSR met l'accent sur une procédure en plusieurs étapes visant à atteindre la cybersécurité et la résilience. La méthode se base sur les risques, mais elle renonce volontairement à une évaluation probabiliste. Elle s'appuie sur l'évaluation qualitative des menaces pesant sur la sécurité informatique et de leurs répercussions potentielles sur les processus d'affaires afin d'identifier rapidement les écarts non admissibles et de les gérer de façon appropriée.

Des objets protégés plutôt que des actifs (*assets*)

La méthode part du principe que les composants matériels et logiciels (y c. les TO et les appareils périphériques) peuvent être regroupés en objets informatiques à protéger. Cette possibilité d'agrégation représente une extension et une précision importantes des modèles-cadres courants pour la gestion des cyberrisques, en particulier en ce qui concerne l'utilisation pratique. Elle favorise par ailleurs une allocation cohérente et compréhensible des ressources pour la mise en œuvre de MTO appropriées. À l'inverse, la norme ISO/CEI 27001 et la norme minimale en matière de TIC partent du principe que chaque actif (ou bien) doit être protégé individuellement.

Directives en matière de sécurité de l'information

Un autre atout de la MCSR réside dans le fait que sa mise en œuvre n'exige pas que chaque organisation élabore et documente ses propres directives en matière de sécurité de l'information ou de gestion des cyberrisques. Il s'agit d'une différence importante par rapport à la norme minimale en matière de TIC et à la norme ISO/CEI 27001, qui exigent souvent que la mise en œuvre des mesures soit examinée dans le contexte des directives propres à l'organisation.

En comparaison, la MCSR peut être considérée comme une directive globale. Des normes techniques ainsi que des directives de mise en œuvre et d'utilisation pour des tâches principalement opérationnelles – telles que la gestion des vulnérabilités, des incidents, des fournisseurs et des autorisations ainsi que les mesures de formation et de sensibilisation – restent toutefois nécessaires. L'OFCS recommande à cet effet de développer des modèles sectoriels afin d'harmoniser ces tâches et de réduire la charge de travail des différentes organisations.

La méthode vise essentiellement à ce que les entreprises et les autorités puissent se concentrer sur la mise en œuvre de mesures et sur la documentation des systèmes et des responsabilités sans avoir à développer au préalable leur propre méthodologie. Cette approche accroît l'efficience de l'implémentation tout en renforçant la cybersécurité et la résilience.

Convergence des TI et des TO

Le développement de la MCSR s'est principalement concentré sur la création d'une méthode uniforme reliant les systèmes TI et TO. L'objectif est de tenir compte de la convergence croissante des TI et des TO, également dans le domaine de la cybersécurité préventive.

La MCSR est conçue pour être appliquée non seulement aux activités principales et aux processus d'affaires des entreprises, mais aussi aux systèmes de gestion de la production et de l'exploitation ainsi qu'aux systèmes de contrôle des processus, de commande et de surveillance. Elle s'applique également aux actionneurs numériques et aux capteurs utilisés dans les processus de fabrication industriels. Le modèle de procédure de la méthode tient compte de cette intégration en plusieurs étapes : la première étape définit les objectifs de protection en tenant compte de la protection contre les perturbations et les incidents. La deuxième étape intègre explicitement les composants des systèmes TO dans les objets à protéger. La troisième étape évalue si une violation des objectifs de protection informatique peut compromettre les objectifs de processus ainsi que la protection contre les perturbations et les incidents. La quatrième étape exige que le concept de sécurité et les exigences fondamentales soient aussi mises en œuvre dans les systèmes TO.

Une comparaison détaillée de cette méthode avec les modèles et les exigences de la norme CEI 62443 est en cours de préparation.

Mise en œuvre d'un SMSI

Comparée à la norme ISO/CEI 27001, la MCSR constitue une approche plus simple visant à mettre en place un SMSI. Cependant, elle n'exclut pas une mise en œuvre complémentaire selon la norme ISO/CEI 27001, notamment lorsque cela est nécessaire pour des raisons de conformité. L'OFCS a publié sa propre analyse de technologie[5] sur le thème de la gestion de la sécurité de l'information et du SMSI.

Reporting et évaluation de la résilience

Le NIST CSF permet de rendre compte de l'état d'avancement de la mise en œuvre à l'aide de degrés appelés *tiers*. La norme minimale en matière de TIC élargit ce concept en facilitant par ailleurs l'évaluation et la comptabilisation des mesures mises en œuvre dans le but de calculer un degré de maturité moyen.

La MCSR elle-même ne définit pas la forme du rapport. L'OFCS est toutefois conscient qu'un reporting standardisé revêt une importance capitale dans le contexte de l'introduction de la méthode. Une évaluation de la résilience[6] est donc en cours d'élaboration dans le cadre d'un projet distinct, actuellement en phase pilote. Elle doit permettre aux organisations et aux entreprises de présenter de manière transparente les caractéristiques de sécurité et de résilience par processus d'affaires, par processus de production ou par produit, renforçant ainsi le sentiment de confiance de la clientèle et de la société.

Toutefois, cette transparence fait souvent défaut dans la norme minimale en matière de TIC et dans la norme ISO/CEI 27001, étant donné que les documents de mise en œuvre correspondants (par exemple, le *Statement of Applicability* selon la norme ISO/CEI 27001) ne sont généralement pas communiqués aux clients. De plus, la documentation est le plus souvent établie au niveau de l'organisation et non par processus d'affaires, par processus de production ou par produit.

---

[5] OFCS, Analyse de technologie – Gestion de la sécurité de l'information et SMSI, Berne, 2 juillet 2025 ; disponible en ligne à l'adresse : ncsc.admin.ch

[6] Pour cette évaluation, nous nous basons sur le *UK Cyber Assessment Framework* ainsi que sur les conclusions relatives à la mesure et à la vérification de la sécurité informatique (note de bas de page 4).

Prise en compte de la sûreté comme objectif d'entreprise

La sûreté[7] – c'est-à-dire la protection des personnes et de l'environnement contre les dommages involontaires résultant de risques techniques, de dangers naturels ou d'influences similaires – est souvent considérée comme secondaire dans le domaine de la sécurité de l'information et de la cybersécurité, ce qui se reflète aussi dans les cadres existants. La MCSR, en revanche, considère la sûreté comme une composante à part entière de la gestion des risques. Les perturbations et les incidents non admissibles doivent être pris en compte tant dans l'analyse des processus d'affaires et de production que dans l'évaluation des besoins de protection. Les exigences en matière de protection contre les événements naturels, le vieillissement ou l'usure des composants techniques sont ancrées dans les exigences fondamentales de la MCSR. Cette méthode se prête donc également à une utilisation dans les infrastructures techniques et dans les installations industrielles.

5 Mise en œuvre simultanée de la norme minimale en matière de TIC, de la norme ISO/CEI 27001 et de la MCSR

5.1 Doublons

Une mise en œuvre parallèle de la MCSR et de la norme minimale en matière de TIC ou de la norme ISO/CEI 27001 est en principe possible, mais elle entraîne des doublons dans les rapports et potentiellement dans la gestion des cyberrisques. La réalisation complémentaire d'une analyse des risques probabiliste n'apporte qu'une valeur ajoutée limitée. Elle peut certes être utilisée pour identifier des mesures supplémentaires, mais ne doit pas servir à rejeter des mesures définies dans le cadre de la MCSR ou à les présenter comme des risques résiduels.

La MCSR prévoit que les objectifs relatifs aux processus d'affaires et aux processus de production soient adaptés en conséquence lorsque certaines mesures ne sont pas mises en œuvre. Cette approche soutient la gouvernance, étant donné que les effets sont immédiatement visibles. Par ailleurs, la direction peut se concentrer sur l'évaluation des répercussions acceptables sans devoir se pencher sur des questions techniques détaillées, ce qui simplifie la prise de décision.

5.2 Quelles sont les nouveautés apportées par la MCSR ?

L'OFCS s'attend à ce que l'application de la MCSR engendre les charges supplémentaires ci-dessous en matière de pilotage et d'orientation de la sécurité de l'information.

- Pour déterminer les besoins de protection, les processus d'affaires et de production doivent être évalués en fonction des répercussions acceptables des cyberincidents.
- Il convient de définir comment les composants matériels et logiciels peuvent être regroupés de manière judicieuse en objets à protéger.
- Les directives existantes en matière de sécurité de l'information et les normes techniques de mise en œuvre doivent être examinées afin de vérifier si elles tiennent compte des exigences fondamentales de la MCSR. À cet effet, la méthode fournit de nombreuses recommandations de mise en œuvre qui peuvent être directement adoptées. Elle va même plus loin sur certains points, par exemple en formulant des exigences en matière

[7] Contrairement à la sûreté (*safety*), la sécurité (*security*) vise à protéger les systèmes et les données contre les attaques et les manipulations intentionnelles, disponible en ligne à l'adresse : ncsc.admin.ch

de renforcement du système (exigence fondamentale 3.1), en exigeant la réalisation d'une sauvegarde hors ligne (exigence fondamentale 3.7) et en définissant des prescriptions pour un développement logiciel sécurisé (exigence fondamentale 3.8).

- Une collaboration plus étroite entre des équipes qui travaillaient jusqu'à présent séparément peut s'avérer nécessaire, étant donné que la MCSR couvre à la fois les systèmes TI et TO ainsi que des aspects du processus lié à la continuité des activités.

Par ailleurs, cette méthode entraîne un changement de paradigme : ce ne sont plus la sécurité de l'information ou la conformité qui sont au centre des préoccupations, mais la cyberrésilience en tant qu'objectif fondamental.

6 Informations utiles pour les entreprises et les autorités qui mettent aujourd'hui en œuvre la norme minimale en matière de TIC

À l'exception de quelques exigences, la MCSR couvre tous les aspects de la norme minimale en matière de TIC. Sa mise en œuvre permet donc, en règle générale, de répondre à la plupart des exigences de cette norme. Les sous-catégories de la norme minimale en matière de TIC qui nécessitent une attention particulière – en sus des différences méthodologiques dans la gestion des cyberrisques – sont examinées ci-dessous.

- ID.BE-2 exige que *l'importance de l'organisation en tant que partie intégrante des infrastructures critiques soit identifiée et communiquée, de même que son rôle au sein du secteur concerné*. Cette identification et cette communication s'effectuent en dehors du champ d'application de la MCSR.
- ID.RA-2 demande que *des informations actuelles sur les cybermenaces soient obtenues au moyen d'échanges réguliers dans des forums et des comités d'experts*. RS.CO-5 exige quant à elle *un échange régulier d'informations, sur une base volontaire, avec des acteurs externes afin de les sensibiliser davantage à la situation présente en matière de cybersécurité*. La MCSR ne prévoit pas explicitement ces exigences, étant donné que la cyberrésilience doit en principe être assurée indépendamment du niveau de menace du moment. L'OFCS tient toutefois compte de cet aspect dans le cadre de l'élaboration des processus opérationnels, par exemple dans la gestion des vulnérabilités et des incidents.
- ID.SC-3 requiert que *les contrats conclus avec les fournisseurs et les tiers les engagent à mettre en œuvre et à respecter les mesures nécessaires pour atteindre les objectifs du programme de cybersécurité de l'organisation*. Dans ce contexte, la MCSR exige l'identification et la surveillance des dépendance ainsi que la mise en œuvre de mesures de protection appropriées (exigence fondamentale 2.2). La méthode n'exige pas explicitement la conclusion d'accords contractuels, même s'ils sont toutefois implicitement considérés comme une mesure possible. L'OFCS estime à cet égard que les contrats ne garantissent pas à eux seuls la cybersécurité ou la résilience, mais qu'ils servent avant tout à assurer une protection juridique.
- PR.AT-3 demande que *tous les acteurs impliqués en dehors de leur entreprise (fournisseurs, clients, partenaires) soient conscients de leur rôle et de leurs responsabilités.* La MCSR ne prévoit pas explicitement cette exigence car, dans la pratique, sa mise en œuvre n'est en général possible que de manière limitée.
- PR.DS-8 exige que *les organisations mettent en place un processus permettant de vérifier l'intégrité du matériel utilisé.* La MCSR ne définit pas cette vérification comme une

exigence fondamentale. En cas de besoin de protection accru, il est toutefois possible de la prendre en compte au moyen de mesures supplémentaires.

- PR.IP-1 exige qu'*une configuration standard soit créée pour l'infrastructure d'information et de communication ainsi que pour les systèmes de contrôle industriels afin de garantir le respect des principes fondamentaux de sécurité*. L'OFCS ne prévoit pas explicitement une telle exigence, vu que les exigences fondamentales de la MCSR constituent déjà une référence fondamentale en matière de sécurité. Une référence supplémentaire propre à l'entreprise n'est pas nécessaire et compliquerait inutilement la mise en œuvre. Toutefois, des normes de configuration spécifiques au système – par exemple pour les configurations de pare-feu ou de réseau – doivent être élaborées et prises en compte dans les processus opérationnels appropriés.
- PR.IP-3 requiert *la mise en place d'un processus visant à contrôler les modifications de configuration*. La MCSR ne l'exige pas explicitement. Cependant, conformément à l'exigence fondamentale 4.1, il convient de s'assurer que les modifications ayant une incidence sur la sécurité soient consignées et évaluées. Des prescriptions détaillées concernant la gestion de la configuration doivent être définies et mises en œuvre dans le cadre des processus opérationnels.
- PR.IP-7 exige que *les processus relatifs à la sécurité de l'information soient continuellement développés et améliorés*. La MCSR n'exclut pas l'amélioration continue, mais ne l'exige pas explicitement. L'objectif est d'établir et de mettre en œuvre une structure des processus en matière de cybersécurité garantissant la résilience de l'organisation face aux cyberrisques. Une amélioration continue n'est donc pas obligatoire : des processus efficaces et stables suffisent. Il est en revanche essentiel de vérifier régulièrement l'efficacité des mesures existantes et de retirer rapidement celles qui s'avèrent inefficaces dans la pratique. Cet aspect fait partie intégrante de la cinquième étape de la MCSR.
- RS.AN-3 demande que *des analyses forensiques soient réalisées après un incident.* La MCSR requiert uniquement la mise en place d'une gestion des incidents permettant de trier et de résoudre rapidement les incidents et les dysfonctionnements détectés (exigence fondamentale 5.1). En cas de besoin de protection accru, des exigences spécifiques devraient prévoir l'obligation d'effectuer des analyses forensiques.
- RC.CO-2 exige qu'*après un incident de cybersécurité, l'organisation veille à être à nouveau perçue positivement.* La MCSR ne formule pas cet aspect de manière aussi concrète. L'exigence fondamentale 5.3 stipule toutefois que les objectifs de la communication doivent être connus pour les plans d'urgence. Les enseignements tirés des incidents ne sont pas explicitement mentionnés comme exigence fondamentale, la méthode partant du principe que la communication fait partie intégrante du processus de gestion des incidents à mettre en place.