AFNOR SPEC 2404

JUIN 2025

www.afnor.org

Ce document est à usage exclusif et non collectif des clients AFNOR.
Toute mise en réseau, reproduction et rediffusion, sous quelque forme que ce soit, même partielle, sont strictement interdites.

AFNOR, en tant que titulaire des droits d'auteur ou distributeur autorisé, s'oppose expressément à toute intégration, transmission ou absorption totale ou partielle du présent document par des moteurs ou algorithmes d'Intelligence Artificielle (IA). AFNOR s'oppose également à toute fouille de textes et de données ou création dérivée produite par une IA et basée sur le présent document.

This document is intended for the exclusive and non collective use of AFNOR customers. All network exploitation, reproduction and re-dissemination, even partial, whatever the form (hardcopy or other media), is strictly prohibited.

AFNOR, as copyright holder or authorized distributor, expressly objects to any integration, transmission or absorption, in whole or in part, of the present document by Artificial Intelligence (AI) engines or algorithms. AFNOR is also opposed to any text and data mining or derivative creation produced by an AI and based on the present document.

AFNOR
Pour : l.kremer@kassiopee.net

Email: l.kremer@kassiopee.net

Le : 20/06/2025 à 10:27

Diffusé avec l'autorisation de l'éditeur

Distributed under licence of the publisher

DOCUMENT PROTÉGÉ PAR LE DROIT D'AUTEUR

Droits de reproduction réservés. Sauf prescription différente, aucune partie de cette publication ne peut être reproduite ni utilisée sous quelque forme que ce soit et par aucun procédé, électronique ou mécanique, y compris la photocopie et les microfilms, sans accord formel.

Contacter :
AFNOR – Norm'Info
11, rue Francis de Pressensé
93571 La Plaine Saint-Denis Cedex
Tél : 01 41 62 76 44
Fax : 01 49 17 92 02
E-mail : norminfo@afnor.org

AFNOR SPEC

Juin 2025

Plan de sûreté

Exigences opérationnelles

© AFNOR
www.afnor.org

afnor

Sommaire

Avant-propos **3**

Liste des participants **4**

Logos des organismes participants **5**

Introduction **7**

1 Domaine d'application **8**

2 Références normatives **8**

3 Termes et définitions **8**

4 Exigences pour la mise en œuvre d'un plan de sûreté **10**

4.1 Généralités 10
4.2 Gestion du plan 11
4.3 Contenu du plan 11
4.4 Gestion de l'information 11
4.5 Autorités, responsabilités et rôles 11
4.6 Ressources humaines 12
4.7 Compréhension : identification, analyse et évaluation des risques de sûreté 12
4.8 Traitement du risque de sûreté 13
4.9 Évaluation, revue et amélioration du plan 13

5 Processus d'évaluation de la conformité **14**

5.1 Gestion de l'auto-évaluation 14
5.2 Étapes du processus d'évaluation de la conformité 14
5.2.1 Engagement et pilotage du processus d'évaluation de la conformité 14
5.2.2 Mise en œuvre de l'évaluation de la conformité 14

Annexe informative A - Identification des risques (recommandations) **15**

Annexe normative B - Indicateurs de l'évaluation de la conformité suggérés **16**

Annexe informative C - Analyse de risques : concept et cas concret **18**

Bibliographie **24**

AFNOR
(l.kremer@kassiopee.net) Pour : l.kremer@kassiopee.net

Avant-propos

Le présent document a été développé par un groupe de travail ouvert et reflète à ce titre l'accord de personnes et organisations ayant participé à son élaboration. AFNOR a mis à disposition des auteurs son savoir-faire en ingénierie normative afin de coordonner les travaux d'élaboration et éditer le document. En conséquence, le contenu de ce document n'engage que ses auteurs et ne saurait être considéré comme constituant le droit applicable. En effet, AFNOR n'étant ni habilitée à délivrer du conseil juridique ni législateur, AFNOR ne saurait être tenue responsable de l'utilisation qui est faite de ce document, notamment concernant la règlementation éventuellement citée dont la bonne application relève exclusivement de la responsabilité de chacun.

L'AFNOR SPEC :

— est un document technique développé et approuvé dans le cadre d'un processus transparent et ouvert ;

— représente l'approbation de ce seul groupe de travail sur le texte final et ne doit pas être présentée comme une norme française ou comme équivalente à une norme française.

Liste des participants

Participants	Organisme
AGERON Sébastien	EQO
BAJAZET David	SAFE STREAMING
BARTHES Gilbert	BOUYGUES ENERGIES & SERVICES
BAUDOUIN Régis	EKSAE
BEHANZIN Chris	MINISTERE DE L'ECONOMIE ET DES FINANCES
BLONDE Guillaume	DGGN - Officier de liaison au Ministère des armées
BRUN Yann	MINISTERE DE LA CULTURE - DGPA - DIRI - Missa
BUTOR Patrick	COMPAGNIE D'INTELLIGENCE COLLECTIVE INTERNATIONALE
C. Kamel	DGPN - RAID
CUVELETTE Philippe	MOE-KAN
DE BAUFFREMONT Benoit	CNAF - CAISSE NATIONALE DES ALLOCATIONS FAMILIALES
D'ERCHIE Nathalie	SATT SUD EST
DOMINGUEZ Mickael	SUBSIDIUM
DURAND Guillaume	FORTRESS CONCEPT
ENGELBACH Patrick	MINISTERE DE L'ENSEIGNEMENT SUPERIEUR ET DE LA RECHERCHE
FOUSSE Alexandre	STRAAD.A
JANSSEN Florent	CDSE - Club des Directeurs de Sécurité des Entreprises
KREMER Laurent	KASSIOPEE
LAURIE Cédric	OFAPS
LEMOINE Vincent	NEVERHACK
MARCHAND Thierry	SYNDICAT DU CONSEIL EN SURETE
MUNIZ Alban	CNPP - CENTRE NATIONAL DE PREVENTION & PROTECTION
NGUYEN-PHUC Lise	DECLIC PERFORMANCE
NYS Franck	IMPERATRICE DEVELOPPEMENT CONSEIL
P. Emmanuel	DGPN - RAID
PICARD Jean-Marc	UNIVERSITE TECHNOLOGIQUE DE COMPIEGNE
PLENK Wilfried	S.P.2 Formation
ROBIN Mathieu	NEVERHACK
ROUSSEL Victoire	MINISTERE DES ARMEES - DIRECTION GENERALE ARMEMENT
SCUTO Nicolas	MINISTERE DE L'INTERIEUR
TEISSIER Bertrand	STRAAD.A
VANNEROT Sébastien	MEDEF DE L'EST PARISIEN
VERDEJO Dominique	PERSONAL INTERACTOR
ZVUNKA Jean Luc	CCI DU VAR - PORT DE TOULON

Logos des organismes participants

MINISTÈRE DES ARMÉES
Liberté
Égalité
Fraternité

MINISTÈRE CHARGÉ DE L'ENSEIGNEMENT SUPÉRIEUR ET DE LA RECHERCHE
Liberté
Égalité
Fraternité

MINISTÈRE DE LA CULTURE
Liberté
Égalité
Fraternité

MINISTÈRE DE L'INTÉRIEUR
Liberté
Égalité
Fraternité

ALLOCATIONS FAMILIALES
Caisse nationale

Ports Rade de Toulon
CCI VAR

CDSE
CLUB DES DIRECTEURS DE SÉCURITÉ DES ENTREPRISES

CNPP

eksaé
La proximité numérique

EQUANS
SERVICES
BÂTIMENTS & INFRASTRUCTURES

FORTRESS
CONCEPT

Impératrice
Développement Conseil

Kassiopée
Be secured

Mouvement des Entreprises de France
Est Parisien (93|94)

MOË KAN

Lise
Nguyên phùc

OFAPS

POLICE NATIONALE
RAID

SP2
formation

SATT
SUD-EST
ACCÉLÉRONS LE TRANSFERT DE TECHNOLOGIES

SISSE
Commissaire et Service
de l'Information Stratégique
et de la Sécurité Économiques

STRAAD.A
incubateur de vos ambitions

Subsidium
Améliorer la sécurité économique des entreprises

SCS
SYNDICAT DU CONSEIL EN SÛRETÉ

ALLIANCE
SORBONNE
UNIVERSITÉ
utc

AFNOR
(l.kremer@kassiopee.net) Pour : l.kremer@kassiopee.net

Introduction

Quelle que soit leur type ou leur taille, les organismes sont confrontés à la gestion des risques en matière de sûreté. Ils se doivent de les gérer en prenant en compte leur contexte spécifique, afin d'assurer un niveau de protection adéquat pour leurs actifs, de sauvegarder les intérêts des parties intéressées dans la perspective d'atteindre leurs objectifs.

Ce document propose aux organismes établis en France un ensemble d'exigences qui leur permet d'élaborer un plan de sûreté de premier niveau structuré, cohérent et nécessitant un minimum de ressources.

La partie 4 comprend des exigences (notées E) et des recommandations (notées R).

La conformité à ces exigences peut être constatée, au choix, par l'organisme lui-même, par une partie prenante de confiance (prestataire, fournisseur, client) ou par une partie extérieure (représentant public, autorités).

La partie 5 comprend les exigences pour l'évaluation de la conformité (notées C).

La mise en œuvre du plan [1] doit garantir l'application de mesures de sûreté adéquates.

Le plan de sûreté est le document support de l'ensemble des activités (processus) de sûreté.

Les dispositions et exigences de ce plan sont conçues pour s'intégrer le cas échéant à un système de management existant. [2]

Les menaces pour la sûreté sont évolutives et souvent inattendues. Par conséquent, le présent document introduit des éléments pour une approche planifiée, basée sur l'anticipation mais également pour une approche réactive c'est à dire agile et adaptative afin d'apporter des solutions à des situations imprévues.

Le plan de sûreté contribue à apporter la confiance dans l'organisation concernée, tout en préservant la confidentialité de certaines dispositions et informations.

Ce document d'exigences est compatible avec la norme NF ISO 22342:2023, *Sécurité et résilience — Sûreté préventive — Lignes directrices pour l'élaboration d'un plan de sûreté destiné à un organisme*.

Adhésion au dispositif du ministère de l'Intérieur : La présente spécification est destinée aux organismes souhaitant adhérer au dispositif P.O.S Pacte sûreté du ministère de l'Intérieur en se conformant à ses exigences. Les organismes publics ou privés concernés sont des organismes de droit français.

[1] Le plan peut être incorporé dans d'autres plans et lui-même être organisé en plans ou sous-plans.

[2] Par exemple, la norme ISO 9001 Système de management de la qualité.

1 Domaine d'application

La présente spécification établit les exigences applicables à l'élaboration, à la mise en œuvre, à la tenue et à la mise à jour d'un plan de sûreté. La gestion du plan doit permettre de démontrer l'aptitude de l'organisme à assurer de manière continue la prévention des risques de malveillance et la protection des personnes et des biens matériels et immatériels dont il a la charge et ce conformément aux exigences légales et règlementaires applicables et aux attentes des parties intéressées.

Le présent document s'adresse à tout organisme public ou privé et particulièrement aux petites et moyennes entreprises souhaitant mettre en œuvre des mesures de sûreté destinées à prévenir les risques de malveillance et à en atténuer les conséquences. Il pose des principes, et modes de gestion sous forme d'exigences mais ne propose ni n'impose aucune solution spécifique ni choix technologique.

Ce document n'est pas destiné à être utilisé dans un cadre de certification.

2 Références normatives

Le document suivant est cité dans le texte de sorte que ce dernier constitue, pour tout ou partie de leur contenu, des exigences du présent document. Pour les références datées, seule l'édition citée s'applique. Pour les références non datées, la dernière édition du document de référence s'applique (y compris les éventuels amendements).

ISO 22300, Sécurité et résilience — Vocabulaire (consultable gratuitement en ligne)

3 Termes et définitions

L'ISO et l'IEC tiennent à jour des bases de données terminologiques destinées à être utilisées en normalisation, consultables aux adresses suivantes :

— ISO Online browsing platform : disponible à l'adresse https://www.iso.org/obp

— IEC Electropedia : disponible à l'adresse https://www.electropedia.org/

Pour les besoins du présent document, les termes et définitions de l'ISO 22300 et l'ISO 31000 ainsi que les suivants, s'appliquent à l'exception des termes suivants :

3.1
Responsabilité
Objectifs et charge assignés à une personne. Un responsable doit rendre compte

3.2
Organisme
Établissement d'une personne morale de droit public ou privé identifié par un SIRET

3.3
Organisation
Ensemble de dispositions mises en œuvre pour faire fonctionner l'organisme

3.4
Rôle
Dans une organisation humaine définit la finalité des activités d'une personne, d'une équipe, d'une entité

3.5
Mission/fonction
Responsabilité assignée à une personne à qui l'on a attribué des moyens pour atteindre un objectif. Une mission peut avoir un caractère accessoire, temporaire ou permanent. Dans ce dernier cas on parle plutôt de fonction

3.6
Autorité
Capacité reconnue et attendue d'une personne physique ou morale à obliger à fixer des responsabilités (ou des objectifs à atteindre) à une autre personne

3.7
Autorité légitime
Autorité publique et compétente

3.8
Incident
Évènement pouvant conduire à une situation indésirable

3.9
Menace
Cause potentielle d'un évènement indésirable et susceptible de porter préjudice

3.10
Sécurité
Situation caractérisée par l'absence de danger ou de menace inacceptable lorsque les procédures sont suivies ou après avoir pris les mesures appropriées (d'après ISO 22300:2021)

3.11
Sûreté
Action de rendre sûr face aux actes et aux menaces de malveillance

3.12
Risque de sûreté
Effets possibles de la malveillance

Note 1 à l'article : Le risque de sûreté est souvent compris comme « l'action potentielle d'une menace sur un actif vulnérable ».

3.13
Criticité
La criticité du risque est déterminée par sa vraissemblance (probabilité) et sa gravité potentielle

Note 1 à l'article : L'évaluation de la criticité d'un risque peut prendre en compte la détectabilité.

3.14
Urgence
Situation pour laquelle l'absence de mise en œuvre d'une solution pertinente dans un délai contraint comporte un risque

Note 1 à l'article : Généralement, la gestion des urgences utilise une approche management du risque pour la prévention, la préparation , la réponse et le rétablissement avant, pendant et après la survenue d'événements et/ou de perturbations potentiellement déstabilisants.

3.15
Planification
La planification est l'organisation des tâches dans le temps. Une tâche est planifiée lorsqu'elle est déclenchée de manière programmée, de façon régulière ou sur la base d'un évènement déclencheur (résultat ou de l'absence de résultat, d'un contrôle ou d'un calcul)

3.16
Plan de sûreté
Ensemble documenté de dispositions planifiées permettant de s'assurer que la sûreté est gérée de façon satisfaisante

Note 1 à l'article : le plan est conçu de façon à assurer l'application de mesures visant à protéger l'organisme d'un incident de sûreté. Ce plan peut être intégré à d'autres plans opérationnels.

3.17
Retour d'expérience (RETEX)
Méthodologie systématique de collecte d'informations fondée sur le retour d'expérience visant à faciliter l'amélioration du plan de sûreté

3.18
Processus
Ensemble d'activités corréélées partageant une même finalité. Un processus bénéficie de ressources de la part de l'organisme

3.19
Vulnérabilité
Faille dans un actif ou dans une mesure de sécurité qui peut être exploitée par une menace

[SOURCE : ISO/IEC 27000:2009]

4 Exigences pour la mise en œuvre d'un plan de sûreté

Les paragraphes précédés par une lettre E ou R suivi d'un numéro itéré par 10 identifient respectivement des exigences et des recommandations. Cela permet de faciliter la lecture et la référence au présent document.

4.1 Généralités

(E-100) Les dispositions et les activités relatives à la sûreté sont gérées dans le cadre d'un plan de sûreté.

(E-110) Le plan de sûreté doit être accessible à l'ensemble des fonctions concernées, sous réserve de la confidentialité de certains éléments inhérents à son intégrité ou sa mise en œuvre.

(E-120) Le plan de sûreté doit être cohérent avec la stratégie et le fonctionnement de l'organisme.

(E-130) L'organisme assure les ressources nécessaires à la mise en œuvre de son plan de sûreté.

(E-140) Les dispositions opérationnelles du plan de sûreté doivent permettre une réaction rapide, adaptée et en adéquation avec les exigences légales et réglementaires en vigueur.

AFNOR
(l.kremer@kassiopee.net) Pour : l.kremer@kassiopee.net

4.2 Gestion du plan

(E-150) Le plan doit être revu au moins une fois par an et le cas échéant, ponctuellement en cas d'incident de sûreté.

(E-160) Le plan doit préciser les éventuelles dérogations (motifs et modes opératoires).

4.3 Contenu du plan

(E-170) Le plan doit contenir ou induire toute disposition d'organisation nécessaire à l'obtention de la conformité aux exigences des présentes.

(E-180) Le plan doit comprendre des dispositions planifiées pour prévenir et traiter les situations indésirables. Il définit également le cadre d'élaboration et de mise en œuvre des actions correctives.

(E-190) Le plan doit fournir un cadre pour réagir à des situations imprévues et la recherche de solutions; cela comprend les situations d'urgence.

(E-200) Le plan doit mentionner les risques couverts, les personnes, les lieux et les activités concernés. Les risques couverts doivent comprendre les atteintes potentielles et avérées aux personnes, aux actifs matériels et immatériels ; cela comprend la sécurité financière, la sécurité physique, la cybersécurité et la réputation.

(E-210) Le plan doit contenir les coordonnées à jour des autorités légitimes, des autres parties intéressées et autres points de contact utiles.

4.4 Gestion de l'information

(E-220) La gestion des risques doit intégrer la protection des informations sensibles contenues dans le plan, en veillant à leur protection, leur confidentialité, leur intégrité, leur authentification, leur disponibilité et à leur accès.

(E-230) Le plan de sûreté doit faire l'objet de versions et de révisions.

(R-240) Note : l'information peut prendre diverses formes notamment physiques et/ou numériques.

(E-250) La direction de l'organisme ou son représentant met à la disposition des autorités légitimes, à leur demande, tout ou partie du plan en mentionnant ses évolutions significatives.

4.5 Autorités, responsabilités et rôles

(E-260) La direction générale nomme un représentant membre de l'organisme qui, nonobstant d'autres fonctions, a la responsabilité de la fonction de sûreté et de son plan dont il rend compte.

(E-270) La fonction de sûreté doit être pourvue afin d'assurer la continuité de service.

(E-280) Le fonctionnement de l'organisme est connu des personnels de sûreté.

(E-290) Les rôles et responsabilités en matière de sûreté doivent être identifiés, connus en interne et validés par la direction. Cela comprend notamment : la création et la mise à jour du plan de sûreté, la formalisation de procédures et consignes relatives à la sûreté, l'instauration et l'entretien de relations étroites avec les autorités légitimes, les modalités de communication avec le public, le compte rendu de l'état de la sécurité lors des revues et de la survenue d'incidents.

(E-300) Les délégations en matière de sûreté doivent *a minima* :

- être formalisées et connues des parties intéressées internes et externes ;
- être acceptées par le délégataire ;
- être validées par la chaîne hiérarchique ;
- concerner un personnel apte et formé.

(E-310) Le responsable de la fonction sûreté doit être associé aux activités de l'organisme pour être en mesure d'identifier les risques de sûreté.

(E-320) Dans une logique de continuité et transversalité, le responsable de la fonction sûreté doit entretenir les relations avec les personnels internes et externes en lien avec la sûreté.

(E-330) Les prestataires et intervenants externes doivent offrir toutes garanties quant à leur compétence, leur impartialité et leur confidentialité, concernant les conditions de détention, d'élimination et d'utilisation d'informations sensibles y compris à caractère personnel.

Note prise en compte le cas échéant d'un engagement de non divulgation dans le cadre du secret des affaires.

4.6 Ressources humaines

(E-340) L'organisme tient compte de la sûreté dans le recrutement, l'arrivée, le suivi, et le départ de ses personnels de l'organisme. Les contrats de travail, fiches de postes et documents afférents sont rédigés en conséquence.

(E-350) L'organisme doit assurer la sensibilisation initiale et continue de l'ensemble des personnels aux enjeux et pratiques de sûreté.

(R-360) Note : un programme d'exercices et d'entraînement à la détection et au traitement de situations prévues et imprévues peut être mis en œuvre de façon à créer des scénarios de risques réalistes. Ce programme peut comprendre l'utilisation d'éléments de solutions préconçues.

4.7 Compréhension : identification, analyse et évaluation des risques de sûreté

(E-370) La compréhension des risques doit faire l'objet d'études planifiées. Ces études doivent être centralisées dans un document spécifique dédié à la malveillance, couvrant l'intégralité du domaine d'application du plan de sûreté.

(R-380) Le responsable de la fonction sûreté peut attribuer la gestion des risques pris en compte par l'organisme à des propriétaires de risques.

(E-390) L'organisme doit mettre en œuvre une démarche méthodique en matière de compréhension du risque comprenant :

- l'identification du risque ;
- la détection et le contrôle (mesures de surveillance) ;
- l'analyse et l'évaluation du risque ;
- la prévention et le traitement du risque (limitation de l'exposition et des conséquences).

(E-400) Le traitement du risque de sûreté doit :

— envisager le fonctionnement en mode dégradé de la sûreté ;

— prendre en compte les exigences de sûreté de la continuité d'activité, de la résilience et de la gestion de crise.

4.8 Traitement du risque de sûreté

(E-410) Toute détection d'un risque doit conduire à son identification et à son traitement.

(E-420) Le traitement du risque y compris la prise de décision doit faire l'objet de dispositions pour :

— adopter les meilleures mesures face à une situation ou un contrôle non satisfaisant ;

— appliquer des solutions prédéfinies à des situations connues par des fiches réflexes ou des procédures/plans spécifiques ;

— faciliter la recherche et l'élaboration de solutions adaptées à des situations imprévues ;

— le cas échéant, communiquer les informations de manière adaptée aux parties intéressées.

(E-430) Les actifs de l'organisme doivent être protégés en fonction de leur niveau de sensibilité par des dispositifs adaptés aux risques identifiés. L'Annexe A propose quelques éléments de base pour un processus d'identification des risques.

4.9 Évaluation, revue et amélioration du plan

(E-440) La direction de l'organisme doit réaliser sur la base du présent référentiel une évaluation interne, *a minima* annuelle, du plan de sûreté quant à son application et à son efficacité. Cette revue préparée par le responsable de la fonction sûreté comporte en entrée :

— (E-450) les résultats des évaluations et inspections ;

— (E-460) le bilan des incidents, des non-conformités et leurs traitements ;

— (E-470) la revue des parties intéressées ;

— (E-480) les informations et exigences pertinentes des parties intéressées ;

— (E-490) le précédent plan d'amélioration et le bilan des actions menées depuis la dernière revue ;

— (E-500) le point sur l'adéquation des ressources allouées par l'organisme.

Cette revue comporte en sortie :

— (E-510) le traitement non achevé des incidents et non conformités ;

— (E-520) les actions correctives et préventives appropriées ;

— (E-530) les dispositions d'actualisation et d'amélioration du plan.

5 Processus d'évaluation de la conformité

(C-2100) Le processus d'évaluation de la conformité doit être intégré dans le plan de sûreté de l'organisme.

(C-2110) Durant le processus d'évaluation, l'organisme peut être accompagné par tout prestataire qu'il agréé au regard du niveau de sensibilité des actifs à protéger.

(C-2120) Le processus d'évaluation de la conformité inclut notamment les éléments suivants :

- (C-2130) les parties prenantes au processus d'évaluation, notamment les propriétaires de risques ;
- (C-2140) les ressources utilisées pour la gestion du processus d'évaluation ;
- (C-2150) la planification de l'évaluation de la conformité ;
- (C-2160) les indicateurs d'activité qui attestent de l'exécution des activités planifiées ;
- (C-2170) les indicateurs de résultats qui attestent de l'atteinte des objectifs ;
- (C-2180) des préconisations d'amélioration autant que de besoin.

5.1 Gestion de l'auto-évaluation

(C-2190) L'organisme doit procéder à une auto-évaluation afin d'identifier les écarts entre l'état constaté et l'état attendu suivant les exigences du chapitre 5.

(C-2200) Les résultats de cette auto-évaluation doivent faire l'objet d'un rapport circonstancié.

5.2 Étapes du processus d'évaluation de la conformité

5.2.1 Engagement et pilotage du processus d'évaluation de la conformité

(C-2210) La direction de l'organisme doit s'assurer de la mise en œuvre du processus d'évaluation de la conformité en y consacrant les ressources nécessaires.

(C-2220) La mise en œuvre du processus d'évaluation de la conformité doit être pilotée par le responsable de la fonction de sûreté de l'organisme concerné.

5.2.2 Mise en œuvre de l'évaluation de la conformité

(C-2230) Les résultats de l'évaluation doivent faire l'objet d'un rapport formel transmis à la direction de l'organisme.

(C-2240) La revue de sûreté doit comprendre l'examen des principaux résultats et indicateurs.

AFNOR
(l.kremer@kassiopee.net) Pour : l.kremer@kassiopee.net

Annexe informative A - Identification des risques (recommandations)

L'organisme devrait envisager :

— (R-390-1) les effets dominos ;

— (R-390-2) les risques de suraccident ;

— (R-390-3) les transitions telles que le passage d'un état de fonctionnement normal à un état de maintenance ;

— (R-390-5) les risques de confusion induits par la surinformation ;

— (R-390-6) les défauts de synchronisation des activités.

Annexe normative B - Indicateurs de l'évaluation de la conformité suggérés

L'évaluation de la conformité du plan peut faire appel à des indicateurs variables pourvu qu'ils couvrent toutes les exigences. Les indicateurs fournis ci-après y concourent mais ne sont pas exhaustifs.

Chaque indicateur se rapporte à une ou plusieurs exigences du présent référentiel.

Indicateur 0 : présence d'une politique de sûreté et tenue d'une revue périodique et de plans d'action associés ;

Indicateur 1 : (exigences E-110, E-210, E-250, E-300) information sur les exigences du référentiel auprès des parties prenantes ;

Définition : les informations relatives aux exigences du plan de sûreté et au processus d'évaluation de la conformité de l'organisme sont diffusées auprès des parties prenantes concernées.

Indicateur 2 : (exigences C-210) planification de l'évaluation de la conformité ;

Définition : l'évaluation de la conformité fait l'objet d'un plan formel et validé par la direction de l'organisme.

Indicateur 3 : (exigences E-150, E-160) gestion du plan de sûreté et de ses révisions ;

Définition : le plan de sûreté est mis à jour, est validé et est connu des parties prenantes concernées.

Indicateur 4 : (exigences E-170 à E-200) formalisation du contenu du plan de sûreté ;

Définition : le plan de sûreté est conforme aux exigences de la présente spécification.

Indicateur 5 : (exigences E-220, E-230) gestion des informations au regard des risques analysés et des niveaux de sensibilité ;

Définition : la gestion de l'information est cohérente avec les risques et les niveaux de sensibilité.

Indicateur 6 : (exigences E-260 à E-300) attribution et identification des responsabilités et des relations en sûreté ;

Définition : les responsables de la sûreté de l'organisme, y compris externes, sont nommés et identifiés dans un document à jour.

Indicateur 7 : (exigences E-130, E-340, E-350) gestion des ressources en matière de sûreté ;

Définition : les moyens financiers et techniques ainsi qu'un environnement approprié sont mis à disposition et adaptés à la gestion du plan de sûreté.

Indicateur 8 : (exigences E-370 à E-430) gestion des risques de sûreté ;

Définition : le processus de compréhension et de traitement des risques de sûreté est formalisé et à jour.

Indicateur 9 : (exigences E-440 à E-530) gestion de l'amélioration continue ;

Définition : le responsable de la sûreté veille à la mise en œuvre des mesures d'amélioration du plan de sûreté y compris des actions correctives et des non-conformités identifiées.

Annexe informative C - Analyse de risques : concept et cas concret

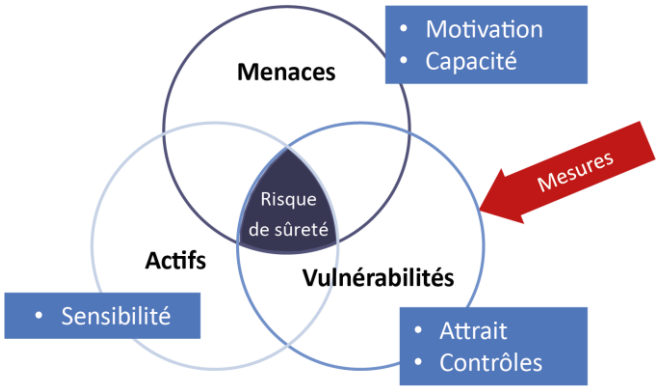
Biliographie d'application volontaire :

ISO 31000, *Management du risque — Lignes directrices*

ISO 31010, *Management du risque — Techniques d'appréciation du risque*

1/ COMPRÉHENSION DES RISQUES MALVEILLANTS : ÉLÉMENTS DE BASE

Caractéristiques des 3 paramètres du risque



Le risque peut faire l'objet de plusieurs approches conceptuelles :

1) Action potentielle d'une menace sur un actif vulnérable

   Exemple : une personne malveillante face à un actif de grande valeur et mal protégé.

2) Effets de l'incertitude sur les objectifs

   Exemple : avec cet acte malveillant, nous risquons de ne pas livrer à temps.

Le concept de menace = cause potentielle d'un évènement indésirable et susceptible de porter préjudice.

Le traitement du risque en 5 étapes majeures :

1. **Dissuader**
2. **Détecter**
3. **Alerter**
4. **Ralentir**
5. **Intervenir**

Le tableau suivant vise à aider le responsable de la sûreté à mieux intégrer le processus de gestion du risque sur la base d'un cas concret fictif : une entreprise de peintures brevetées.

AFNOR SPEC 2404 2025-06

Étapes	Exemples de points sensibles à traiter	Exemples de questions à se poser	Cas d'une entreprise de peintures brevetées
1. Identifier : **Le contexte externe :** localisation, site, criminalité, cybermenaces … **Le contexte interne :** nature des activités, personnels	Objectifs Actifs stratégiques Contextes technologique, économique, réglementaire, politique, social et environnemental Activités et marché : clients, fournisseurs, concurrents	Quels sont les événements redoutés déjà rencontrés ? La stratégie, l'organisation et le contexte sont-ils cohérents ? Quelle est notre couverture assurantielle ? Quelle est la solidité de notre réputation ?	Une entreprise de peintures brevetées obtient un marché pour l'armement. Elle doit réviser sa gestion des risques
2. Identifier les risques et les menaces	Relatifs aux éléments suivants : — personnes internes et externes ; — données et système de sécurité de l'information ; — actifs matériels ; — actifs immatériels dont propriété intellectuelle ; — méthodes et production ; — réputation et image.	Que peut-il se passer ? Comment cela peut-il se produire ? Quelles sont mes vulnérabilités ? Quels actes de malveillance pourraient porter atteinte à mon organisme ?	Agressions/Vol Actions violentes Cyberattaque (ransomware, phishing...) Fuites d'informations/Espionnage industriel Intrusion physique Vandalisme/Sabotage Corruption/conflit d'intérêts Fraudes/Contrefaçon
3. Analyser les risques	La vraisemblance et l'impact des risques les plus critiques	Quelles échelles de vraisemblance et de gravité adopter ? Quelles seraient les conséquences pour l'entreprise ?	Risque de vol de la peinture brevetée : — vraisemblance ? — gravité ?
4. Classer/prioriser les risques	— Limites d'acceptation — Hiérarchisation en fonction de critères	Doit-on le traiter immédiatement ? Quelles sont les limites d'acceptation du risque (Gravité/Vraisemblance) ? Quels sont les critères ?	L'entreprise peut supporter le vol de quelques pots de peintures standards. => Risque acceptable Elle ne peut pas supporter le vol de la peinture brevetée. => Risque non acceptable

AFNOR (l.kremer@kassiopee.net) Pour : l.kremer@kassiopee.net

AFNOR SPEC 24042025-06

Étapes	Exemples de points sensibles à traiter	Exemples de questions à se poser	Cas d'une entreprise de peintures brevetées
5. Traiter les risques Limiter l'exposition et les conséquences	— Mesures pour prévenir, protéger, réagir — Incidents/non conformités	Faut-il : — Accepter le risque ? — Réduire le risque par la mise en place de barrière/parade ? — Contourner ? — Transférer ? changement de technologie, sous-traiter… — Assurer ? lorsque la réparation financière est possible — Refuser ? Abandon du marché, de l'activité	Contournement : déporter le stock chez le client Sensibiliser/Former le personnel aux risques liés à la nouvelle peinture
6. Surveiller et revoir (voir également fiché annexe sur la surveillance)	— Diagnostic — Audit — Test — Retour d'expérience sur les dispositions mises en place	Y-a-t-il un plan de surveillance ? Quelles sont les systèmes de détection ? Quelles sont les décisions à prendre ? Quels sont les moyens de contournement des dispositions prises ?	Mise en place de capteurs (surveillance humaine, vidéosurveillance, alarme...)
7. Communiquer et consulter	Implication des personnels, des partenaires, des autorités	Qui est concerné par les différentes procédures de sûreté ? Les personnels sont-ils suffisamment formés/sensibilisés au regard de leurs activités en sûreté de l'organisme ? Comment impliquer les équipes ?	Faire des exercices de simulation intrusion avec les personnels Coopérer avec les autorités locales

AFNOR (l.kremer@kassiopee.net) Pour : l.kremer@kassiopee.net

AFNOR SPEC 2404 2025-06

Exemple d'évaluation des risques

Type de menace	Vulnérabilité	Exemple de risque identifié	Vraisemblance	Impact	Niveau de risque	Mesures existantes	Mesures à prendre
Cyberattaque (phishing)	Employés peu formés à la cybersécurité	Tentative d'hameçonnage visant les emails professionnels	Élevée	Élevé	Élevé	Antivirus, filtrage de mails	Sensibilisation, test de phishing, MFA (multi-authentification)
Intrusion physique	Locaux sans alarme ni caméra	Vol de matériel	Moyenne	Moyen	Moyen	Serrures classiques	Contrôle d'accès sécurisé, alarme
Employé mécontent	Absence de contrôlé d'accès au système d'information	Sabotage interne : effacement ou altération de données	Faible	Élevé	Moyen	Absence politique claire et connue	Charte sûreté, règlement intérieur, sauvegardes
Usurpation d'identité	Contrôle faible des processus comptables	Fraude via faux fournisseurs ou changement de RIB	Moyenne	Élevé	Élevé	Double signature sur factures	Vérification d'identité fournisseurs, alerte bancaire
Espionnage industriel	Données mal protégées (clé USB, cloud)	Vol de plans techniques	Moyenne	Élevé	Moyen	Aucun chiffrement	Chiffrement, formation, charte sûreté

AFNOR (l.kremer@kassiopee.net) Pour : l.kremer@kassiopee.net

2/ SURVEILLANCE DU RISQUE MALVEILLANT : DÉMARCHE MÉTHODOLOGIQUE

Tout risque doit faire l'objet d'une surveillance sous la forme d'une suite d'étapes ou chaîne.

Sous la responsabilité d'un propriétaire de risques, cette surveillance commence avec l'aide d'un capteur (humain ou matériel) de **bas niveau (SBN)** qui transmet des informations **à la surveillance de haut niveau (SHN)** en charge du traitement du risque. Ce concept de chaine assure la cohérence de la surveillance du risque. L'absence d'un seul maillon ou un défaut d'interface rompt la chaîne et constitue un risque structurel qu'il faut combattre. On considère la chaine composée de maillons que l'on définit. Ils sont au nombre de 10 dans l'exemple qui suit :

Maillon ou élément de la chaîne de surveillance	SBN	SHN
1. Une réflexion régulière (sous forme d'études) permet d'identifier des risques potentiels qu'il convient de surveiller (monitoring) et à quelle fréquence. L'évolution de la nature des risques et de leur niveau est prise en compte par les propriétaires.		
2. La surveillance recueille des données (mesures) via des capteurs (dispositif humain ou matériel).		
3. Une analyse des données par confrontation des résultats à un référentiel permet de qualifier la situation observée et de détecter la présence d'anomalies ou de signaux à considérer.		
4. La communication d'un signalement ou l'émission d'alertes est à destination du haut-niveau.		
5. L'alerte est audible ou visualisable via une alarme ou un indicateur (tableau de bord).		
6. La surveillance suffisamment à l'écoute perçoit les alertes et autres signaux et prend la main.		
7. La surveillance adopte les bons réflexes et réagit de manière appropriée.		
8. La situation est analysée et comprise. L'alerte transmise est infirmée ou confirmée.		
9. Le risque potentiel ou avéré est évalué. La prise de décision est réalisée par application de procédures ou par construction raisonnée pour les cas imprévus.		
10. Le traitement du risque est effectué par l'activation des barrières ou des parades, agissant sur les causes, l'exposition et ou les effets du risque considéré.		

À la recherche d'un maillon manquant : s'assurer de la complétude de la chaîne

Dès qu'un maillon fait défaut, la chaine est interrompue. L'absence d'un maillon doit faire réagir le propriétaire du risque ou la fonction sûreté. Cette absence est susceptible de révéler une défaillance dans la surveillance des risques. Vérification de la chaine : à partir d'un maillon, on recherche la présence du précédent et du suivant en prenant soin de vérifier leur compatibilité, la qualité des interfaces, les règles d'accusé de réception, les risques de sous et de surinformation.

Exemple de questions à se poser par type de maillon en cas de défaut

1.	Y a-t-il une liste ou cartographie des risques pris en compte ? Des maillons sont -ils redondants ?
2.	Quelles personnes ont des objectifs en matière de surveillance des risques ? Dispose-t-on de surveillance ou contrôles automatisés ? Lesquels ?
3.	La compréhension d'un risque est-elle faite sur la base d'un référentiel validé en lien avec des études de risques pertinentes et à jour ?
4.	A-t-on des règles ou des dispositifs, éventuellement redondants pour relayer les alertes ?
5.	Alerte : le dispositif matériel et/ou humain est-il adapté, fiable et efficace ?
6.	La forme et l'ergonomie des alertes sont-elles pertinentes (efficaces, connues et acceptées,…) ?
7.	Quel personnel est désigné et formé pour réagir à chaque type d'alerte ?
8.	Dispose-t-on si besoin d'experts pour les risques critiques ou formés à l'analyse et à la compréhension des situations critiques ?
9.	La prise de décision est-elle construite avec un nombre de cas préétablis prévus et connus ? En cas de situation inédite, des dérogations sont-elles prévues ?
10.	Quelles barrières et/ou parades associe-t-on aux risques ?

Au final il convient d'assurer l'intégrité et la résilience de la chaine, élément de la « tour de contrôle ».

Pour aller plus loin il est envisageable de développer des chaines ou parties de chaines redondantes formant des réseaux. Ces réseaux de surveillance peuvent être discrets, visibles voire comporter des leurres : des caméras de vidéosurveillance factices par exemple.

Bibliographie

- **Diagseco** (Ministère de l'Economie, des Finances et de la Souveraineté Industrielle et Numérique), un outil pour établir un diagnostic de sécurité économique de l'entreprise. Cet outil s'adresse à toutes les entreprises, quels que soient leur taille ou leur secteur d'activité. Il n'a pas de valeur réglementaire. Diagseco propose, à travers une série de questions précises mais non exhaustives, d'évaluer les points de vulnérabilité de l'organisation en matière d'information stratégique et de sécurité économiques : https://www.entreprises.gouv.fr/espace-entreprises/etre-accompagne/diagseco-loutil-pour-etablir-un-diagnostic-de-securite

- **Cartographie des risques**, un outil conjoint du MEDEF et de l'AMRAE : https://www.macartodesrisques.fr/

- **Mon Aide Cyber (ANSSI),** un programme d'accompagnement et de formation gratuit à destination d'une communauté d'Aidants leur permettant de guider leur écosystème pour mettre en œuvre une démarche de cybersécurité : https://monaide.cyber.gouv.fr/

- **Outils de test cyber** :
  - Outil du MEDEF : https://cybersecurite.medef.com/
  - Outil CCI Auvergne: https://www.puy-de-dome.cci.fr/produit/auto-diag-cybersecurite

- **Mooc sur la sécurité numérique (ANSSI)** : https://cyber.gouv.fr/le-mooc-secnumacademie