Direction Générale des Infrastructures, des Transports et de la Mer
Direction des Services de Transport
Mission Sûreté Défense

Arche Sud
92055 La Défense Cedex
msd.dst.dgitm@developpement-durable.gouv.fr
Téléphone : 01 40 81 17 90
Télécopie : 01 40 81 73 49

Présent pour l'avenir

Manuel d'Audit des Systèmes de Sûreté des Ports et des Installations Portuaires

DGITM/DST/MSD

1ère édition : octobre 2006
Edition d'octobre 2010
Approuvé le 27 octobre 2010

Tableau 1 : Historique des modifications du manuel d'audit des systèmes de sûreté des ports et IP

Version	Date	Auteur(s) (Nom, Prénom)	Partie(s) modifiée(s)	Objet de la modification /Commentaires	Approbation (Date et signature du chef de la DGITM/DST/MSD)
V01	27/02/06	JM AUBAS	Création du Manuel		
V02	28/02/06	JM AUBAS B DUMSER	Chapitres 3.2.4, 5.5, et 6	Modèles de rapport d'audit, refonte des procédures de suivi	
V03	21/01/08	P. ENTERIC	/	Mise à jour générale, notamment par rapport aux nouveaux textes en vigueur (décrets de 2007).	
V04	29/06/08	P. ENTERIC	/	Mise à jour : - Arrêtés d'application du décret du 29 mars 2007 ; - Réorganisation du secrétariat chargé des transports.	
V05	18/06/10	J. GIRAUD	/	Mise à jour générale afin d'améliorer la gestion documentaire et les procédures d'audit en termes d'assurance qualité et d'amélioration continue et de les formaliser. Audit présenté sous approche processus	
VO	27/10/10	B. DELSUPEXHE		Mis à jour suite aux observations des auditeurs	Le 27 octobre 2010 Le chef de la mission-sûreté-défens Michel DESCHAMPS

SOMMAIRE

Liste des tableaux & figures

- *Liste des tableaux :*

- *Liste des figures :*

I. ABRÉVIATIONS & DÉFINITIONS

Action corrective : Action proposée par l'exploitant pour remédier à une non-conformité, une remarque, un point faible ou une recommandation relevée lors de l'audit. Une action corrective doit être définie avec un délai d'application réaliste.

ACVS : Agent chargé des visites de sûreté.

Art. : Article.

ASC : Agent de sûreté de la compagnie.

ASIP : Agent de sûreté de l'installation portuaire.

ASN : Agent de sûreté du navire.

ASP : Agent de sûreté portuaire.

Audit : Processus systématique, indépendant et documenté, réalisé par la MSD en vue d'obtenir des preuves d'audit évaluées de manière objective pour déterminer dans quelle mesure les critères d'audit sont satisfaits.

Audit programmé : Audit programmé pour être effectué pendant la période de validité du plan de sûreté d'une installation ou d'un port avec un préavis notifié à l'exploitant. Un audit programmé sur une installation a lieu tous les cinq ans. En outre, si l'installation contient une ZAR, un deuxième audit programmé doit être effectué dans la période d'approbation du plan au cours de la troisième année suivant le premier audit programmé.

Audit de conformité : Audit effectué à la demande du préfet auprès de la MSD en vue pour celui-ci d'établir une déclaration de conformité d'installation portuaire ou de port.

Audit de suivi : Audit dont la procédure est la même que celle de l'audit programmé. Toutefois, son objectif est de constater si les actions correctives relatives aux non-conformités décelées lors du dernier audit programmé ont bien été réalisées dans les délais prévus dans le plan d'actions, approuvé par le préfet.

Audit inopiné : Audit non programmé, qui peut être provoqué par un événement imprévu et effectué sans préavis ou avec un préavis très court. Il est limité dans l'étendue de ses vérifications : on ne vérifie pas les aspects formels ou les infrastructures mais davantage la qualité de la mise en œuvre opérationnelle.

Auditeur : Personne ayant les compétences nécessaires et une qualification reconnue pour être habilitée par la DGITM à effectuer les audits. Les compétences nécessaires consistent en des qualités personnelles et une capacité démontrées à appliquer des connaissances et des aptitudes. Il existe deux types d'auditeurs : l'auditeur temps-plein qui est nommé auditeur national de sûreté portuaire et qui sera le chef de mission de l'audit, et l'auditeur volontaire, co-auditeur de l'auditeur temps-plein. En outre, l'art. L. 321-6 prévoit que l'activité d'auditeur puisse être exercée par le personnel d'un OSH.

Audité : L'autorité portuaire ou l'exploitant. L'organisme de sûreté habilité et l'organisme de formation pourront être également audités.

Autorité compétente : autorité nommée par le Gouvernement pour coordonner, mettre en œuvre et surveiller l'application des mesures de sûreté prescrites par les exigences réglementaires en ce qui concerne les navires, les ports et les installations portuaires. Il s'agit en France de la Direction Générale des Infrastructures, des Transports et de la Mer (DGITM) comprenant la DST/MSD, la DST/PTF et la DAM/SM.

Autorité portuaire : Autorité responsable des questions de sûreté à terre dans un port donné.

CE : Commission européenne.

CLSP : Comité Local de Sûreté Portuaire.

Code ISPS : (*International Ship and Port Facility Code*) Code international pour la sûreté des navires et des installations portuaires. Sa partie A représente les obligations tandis que la partie B consiste en des recommandations, dont certaines ont été rendues obligatoires au niveau européen par le Règlement (CE) 725/2004. Le Code ISPS, annexe 2 du Règlement, est applicable depuis le 1er juillet 2004.

Compétences : Qualités personnelles et capacités démontrées à appliquer des connaissances et des aptitudes.

Conclusions d'audit : Résultats d'un audit fournis par le chef de mission après avoir pris en considération les objectifs de l'audit et tous les constats d'audit.

Constats d'audit : Résultats de l'évaluation par l'équipe d'audit des preuves d'audit recueillies, par rapport aux critères d'audit.

Convention SOLAS : (*Safety of life at sea*) Convention pour la sauvegarde de la vie humaine en mer. Le Chapitre XI-2 « Mesures spéciales pour renforcer la sûreté maritime » de la Convention SOLAS a été adopté par l'Organisation Maritime Internationale le 12 décembre 2002 et publié en France par le décret 2004-290 du 26 mars 2004.

CPM : Code des Ports Maritimes. (sera prochainement intégré au Code des Transports)

Critères d'audit : ensemble de politiques, procédures ou exigences déterminées. Les preuves d'audit devront être en conformité avec les exigences réglementaires de sûreté internationales et nationales en vigueur ainsi qu'avec le plan de sûreté du port ou de l'IP lorsqu'il a été approuvé.

DAM : Direction des affaires maritimes de la Direction Générale des Infrastructures, des Transports et de la Mer.

Déclaration de conformité : Le Gouvernement contractant sur le territoire duquel l'installation portuaire est située peut délivrer une déclaration de conformité de l'installation portuaire appropriée. Cette déclaration certifie que la conformité de l'IP avec les dispositions du Règlement (CE) 725/2004 a été vérifiée et que ladite IP est exploitée conformément au PSIP approuvé. Un modèle de ce document est disponible en appendice de la partie B du Code ISPS.

DGITM : Direction Générale des Infrastructures, des Transports et de la Mer au sein du Ministère de l'écologie, de l'énergie, du développement durable et de la Mer. C'est l'autorité maritime compétente

au sens de l'article 2.7 du Règlement (CE) 725/2004. La DGITM a en charge l'ensemble des sujets relatifs aux transports terrestres et maritimes.

DST : Direction des Services de Transport de la Direction Générale des Infrastructures, des Transports et de la Mer.

Ecart : Constat d'audit révélant un non-respect des exigences réglementaires ou des dispositions du plan de sûreté approuvé. Les exigences en écart sont précisées et hiérarchisées en non-conformités majeures ou non-conformités simples et en remarques, les non-conformités devant être rectifiées prioritairement aux remarques.

Enregistrement : Formulaire informé, relatif à une procédure.

Equipe d'audit : Plusieurs auditeurs réalisant un audit. Un des auditeurs (l'auditeur temps-plein de préférence) est nommé chef de mission et sera alors le responsable de l'équipe d'audit. Cette équipe peut également être complétée d'auditeurs en formation et/ou d'observateurs.

ESIP : Evaluation de sûreté de l'installation portuaire.

ESP : Evaluation de sûreté portuaire.

Exploitant : Exploitant d'une installation portuaire ou d'un port, responsable notamment du plan de sûreté de son installation et de sa mise en œuvre.

HFDS : Haut Fonctionnaire de Défense et de Sécurité. Fonction exercée par le Secrétaire général du ministère. Le HFDS adjoint est chef du SDSIE.

Incident de sûreté : Tout acte suspect ou avéré, ou toute circonstance suspecte ou avérée, qui menace la sûreté de l'installation.

Infraction : Action ou comportement interdit par la loi et passible de sanctions pénales ou administratives : amende, peine d'emprisonnement, peines complémentaires, etc.

Installation portuaire : Cela désigne un emplacement tel que défini par le Représentant de l'Etat dans le Département où a lieu l'interface navire/port (terminal). En France, elle ne comprend généralement pas les zones telles que les zones de mouillage, les postes d'attente ou leurs abords à partir de la mer.

Installation : Installation portuaire ou Port.

Inspection de suivi : Elle a lieu après l'audit de suivi si les actions correctives qui auraient dû être réalisées à la date prévue dans le plan d'actions approuvé par le préfet n'ont pas été réalisées avant l'audit de suivi ou si elles n'ont démontré aucune progression. Le responsable de l'inspection de suivi est chargé de contrôler si lesdites actions correctives ont été mises en œuvre à la date de l'inspection. Dans le cas où un manquement à cette obligation est constaté, le rapport d'inspection pourra servir de fondement à l'élaboration de sanctions administratives décidées par le préfet.

IP : Installation portuaire.

Manquement : Action de manquer à un devoir, à une loi, à une règle. On qualifiera de manquement le non-respect d'une loi ou d'un règlement, ou encore d'une procédure décrite dans le plan de sûreté de l'installation ou du port.

Manuel : Description générale d'une organisation, des interactions entre les différents processus.

MEEDDM : Ministère de l'Ecologie, de l'Energie, du Développement Durable et de la Mer.

MSD : Mission Sûreté Défense de la DGITM/DST.

NC : Voir Non-conformité.

NC maj : Voir Non-conformité majeure.

Non-conformité : Constat d'audit relevant une non-satisfaction, un écart à une exigence spécifiée par des textes réglementaires en vigueur ou encore des procédures contenues dans le plan de sûreté approuvé. La mise en œuvre du critère d'audit évalué est insatisfaisante.

Non-conformité majeure : Constat d'audit relevant une non-satisfaction, un écart à une exigence spécifiée par des textes réglementaires en vigueur ou encore des procédures contenues dans le plan de sûreté approuvé. La mise en œuvre du critère d'audit évalué est insuffisante ou inexistante. La non-conformité majeure remet en cause à elle-seule la sûreté du système et donc sa viabilité. Elle devra être résolue en priorité, dans les plus brefs délais car elle met en péril la sûreté de l'installation de manière certaine OU immédiate.

OSH : Organisme de sûreté habilité, tel que défini dans le code ISPS sous le vocable « organisme de sûreté reconnu ». Il désigne un organisme, ayant des compétences appropriées en matière de sûreté et une connaissance suffisante des opérations des navires et des ports, qui est habilité à mener, aux conditions de la réglementation française, une activité d'évaluation ou de vérification ou d'approbation ou de certification prescrite aux termes du chapitre XI-2 de la Convention SOLAS ou de la partie A du Code ISPS. Les organismes de sûreté sont habilités selon l'arrêté du 26 juillet 2007.

PC : Voir point critiquable.

PF : Voir Point fort.

Point critiquable : Constat d'audit révélant des pratiques à risques ou actions restant à finaliser, sans écart avéré.

Point fort : Constat d'audit révélant une bonne pratique, qui répond bien aux exigences de la réglementation et aux mesures spécifiées dans le plan de sûreté approuvé.

Port : Abri naturel ou artificiel pour les bâtiments de navigation, muni des installations portuaires nécessaires à l'embarquement et au débarquement des marchandises et des passagers.

Préf. : Préfecture.

PREMAR : Préfecture maritime.

Preuves d'audit : enregistrements, énoncés de faits ou autres informations se rapportant aux critères d'audit et qui sont vérifiables. Ici, il s'agira notamment des documents de sûreté du port ou d'une installation portuaire. Les autres informations peuvent être celles recueillies lors de la visite du port ou de l'IP par constats visuels ou par entretiens de personnels présents sur le site.

Procédure : Manière spécifiée de réaliser une action, une activité.

Processus : Description d'un ensemble d'activités liées entre elles transformant des éléments d'entrée en éléments de sortie.

PSIP : Plan de sûreté de l'installation portuaire.

PSP : Plan de sûreté du port.

PTF : Sous-direction des Ports et Transports Fluviaux.

R : Voir Remarque.

REC : Voir recommandation.

Recommandation : Constat d'audit relevant des pistes d'amélioration face à un critère évalué.

Remarque : Dans ce type d'écart, le critère d'audit est mis en œuvre mais des lacunes dans la mise en œuvre du critère sont observées, révélant trop peu de pilotage ou de suivi. La remarque peut concerner un défaut dans la sémantique du plan de sûreté approuvé reflétant alors mal la pratique.

Sanction : Conséquence juridique entraînant une mesure répressive prévue par la loi et infligée par une autorité pour l'inexécution d'un ordre, ou le non respect d'un règlement, d'une loi. En fonction de la nature du droit qui a été violé, on distingue les sanctions civiles, les sanctions administratives et les sanctions pénales. Ce sont les deux dernières qui nous intéressent ici.

Sanction administrative : Sanction, indépendante de la sanction pénale, infligée par une autorité administrative, agissant dans le cadre de prérogatives de puissance publique, dans la mesure nécessaire à l'accomplissement de sa mission et assortie par la loi de mesures destinées à assurer la protection des droits et libertés constitutionnellement garantis.

Sanction pénale : Réponse de l'État contre l'auteur d'un comportement incriminé. Les sanctions pénales ne se distinguent des autres sanctions que par le fait qu'elles sont prévues dans le Code pénal et prononcées par une juridiction pénale. La peine applicable dépend de la qualification de l'infraction, en crime, délit ou contravention.

SDSIE : Service de Défense, de Sécurité et d'Intelligence Economique. L'adjoint pour la mer du chef du service assure notamment les responsabilités de point de contact national pour la sûreté maritime

SSAS : (*Ship Security Alert System*) Système d'alerte de sûreté du navire.

Système d'alerte de sûreté du navire : Cela désigne un système installé sur tous les navires (selon la Règle 6 du Chapitre XI-2 de la Convention SOLAS), leur permettant d'envoyer -via satellite- une alerte discrète en cas de problème majeur de sûreté, type détournement, prise d'otage, attaque du navire ou autre au point de contact de l'Etat du pavillon.

ZAR : Zone d'accès restreint. Une zone d'accès restreint est, sauf impossibilité technique avérée, créée dans toute installation portuaire dédiée à l'accueil de navires à passagers, à l'accueil de navires porte-conteneurs ou à l'accueil de navires pétroliers, gaziers ou transportant des marchandises dangereuses.

ZPS : Zone portuaire de sûreté au sens de l'article L.321-1 du CPM : elle est délimitée par l'autorité administrative et comprend le port dans ses limites administratives et les zones terrestres contiguës intéressant la sûreté des opérations portuaires.

II. Gestion du Manuel d'audit[1]

II. A. Objectifs du Manuel d'audit des systèmes de sûreté des ports et IP

Ce présent manuel a pour objectifs de déterminer les cadres réglementaire et organisationnel de l'audit de systèmes de sûreté portuaire. Plus précisément, il permet de :

- Définir l'organisation du processus « audit » (liens organisationnels entre les sous-processus le constituant et les responsabilités de chacun) et les termes liés à celui-là ;
- Servir de référence aux auditeurs lorsque survient une difficulté dans la mise en œuvre de l'audit.

Il peut également servir de support de formation d'auditeurs.

II. B. Champ d'application

Ce manuel est mis à la disposition des personnes suivantes :

- ✓ Auditeurs temps-plein chargés des audits des systèmes de sûreté portuaires ;
- ✓ Auditeurs volontaires accompagnant les auditeurs temps-plein ;
- ✓ Membres de la Mission Sûreté Défense qui sont responsables du management de ce manuel ;
- ✓ Préfets et autorités locales.

Chacun doit lire et respecter la méthodologie d'audit décrite dans ledit manuel.

II. C. Procédure de surveillance et de revue du Manuel d'audit

II. C. 1) Objectifs

La méthodologie d'audit développée dans le manuel doit évoluer et s'enrichir de l'expérience des audits réalisés. A cet effet, MSD organise au moins trois fois par an une rencontre avec tous les auditeurs temps-plein afin d'analyser les difficultés qu'ils ont rencontrées lors des audits et réfléchir avec eux aux évolutions souhaitables de la méthodologie d'audit et, éventuellement, de la réglementation. En dehors de ces rencontres, les auditeurs ont la possibilité de proposer à tout moment des modifications du présent manuel.

II. C. 2) Champs d'application

La MSD est responsable de la mise à jour dudit Manuel.

La revue du Manuel d'audit tient compte, par exemple :

- ✓ des indicateurs de performance du processus « audit » et de ses sous-processus,
- ✓ de la conformité aux procédures qui y seront développées,
- ✓ de l'équivalence du travail d'équipes d'audit dans les situations similaires,
- ✓ de l'évolution :
  - o du cadre réglementaire ou organisationnel,
  - o des besoins et attentes des parties intéressées,
  - o et des pratiques d'audit, différentes ou nouvelles.

[1] Ce Manuel s'est largement inspiré de la norme ISO 19011. Cette partie II « Gestion du Manuel d'audit » correspond en quelque sorte à la partie « Management d'un programme d'audit » de ladite norme.

II. C. 3) Méthodologie de surveillance et de revue du Manuel d'Audit

Pour faciliter la diffusion des propositions de modifications et assurer leur traçabilité et conservation, il convient d'utiliser le document « Enregistrement des propositions de modifications du Manuel d'audit » (présenté en Annexe 1). L'utilisation de ce document permet d'assurer un suivi de l'évolution du manuel afin que sa gestion puisse être reprise par un nouveau membre de la MSD. Il est divisé en trois parties qui se remplissent de la façon décrite ci-après :

1. Auteur de la proposition de modification

Celui-ci précise son nom, son prénom et sa fonction.

2. Méthodologie de proposition de modification

L'auteur de la modification précise :

- la présentation générale (dont l'objet) de la modification proposée ;
- la description de la situation d'audit ou tout autre événement qui motive la proposition : date, lieu (nom et adresse du port ou de l'IP), noms et prénoms des personnes présentes au moment de la constatation ;
- la version et la (ou les) partie(s) du manuel concernées par ladite modification ;

Il rédige ensuite :

- les amendements des parties du manuel à changer ;
- une évaluation des conséquences de ce changement (autres que son objet principal).

Ce document, daté et signé par l'auteur, est envoyé à la MSD qui, si suite peut être donnée, le diffuse aux autres auditeurs temps-plein afin qu'ils donnent leur avis dans les quinze jours suivant l'envoi de ladite proposition.

Lorsque la MSD souhaite suggérer une modification du Manuel, elle la diffuse aux auditeurs temps-plein afin d'obtenir leur avis en remplissant ce même document (Annexe 1).

3. Approbation ou refus par MSD

Après avoir recueilli l'avis des auditeurs, la MSD approuve ou refuse la modification et complète la partie finale du document (Annexe 1).

Afin de faciliter l'archivage, le fichier est enregistré après avoir été renommé comme suit :

- Si la proposition de modification est approuvée : aa mm jj_approbation_modification du manuel d'audit.doc (odt) ;
- Si la proposition de modification est refusée : aa mm jj_refus_modification du manuel d'audit.doc (odt).

Il convient que la MSD élabore un tableau récapitulatif des propositions en précisant :

- la date,
- les nom et prénom de l'auteur de la proposition,
- la mention « approuvé » ou « refusé ».

Ce fichier est ensuite diffusé aux auditeurs temps-plein et volontaires.

En cas d'approbation, la modification est enregistrée dans le tableau en tête de document « Historique des modifications du Manuel d'Audit ».

II. C. 4) Historique des modifications du Manuel d'Audit

A chaque modification, cet historique est dûment complété, daté et signé par le chef de la mission MSD. Cette signature atteste de :

- ✓ l'approbation de la nouvelle version du manuel ;
- ✓ sa diffusion aux personnes concernées (Voir champ d'application du manuel).

La revue de ce manuel se fait de façon annuelle, lors de la 1ère réunion d'auditeurs qui a lieu dans l'année civile. Si la revue n'entraîne qu'une modification mineure (ex : l'appellation d'une autorité a changé), on ne changera pas le numéro de la version (ex : on passera de la version V-5.1 à la version V-5.2). Si la vérification entraîne une modification de la méthodologie d'audit elle-même, on passera à une autre version (ex : on passera de la version V-5 à la version V-6).

II. D. La base de données OSIRIS

OSIRIS (Outil de Suivi Informatique Relatif aux Informations de Sûreté) est une base de données gérée par la MSD. Elle est accessible, sous contrôle authentifié par intranet, par les auditeurs temps-plein et les membres de MSD.

Elle fournit en temps réel des informations enregistrées sur la sûreté des ports et IP. Ainsi, une fois qu'un audit est réalisé, les auditeurs l'intègrent sur la base en précisant de quel type d'audit il s'agit, les dates de réalisations, les noms et prénoms des personnes présentes (équipe d'audit, exploitant, ASP, ASIP).

MSD fournit les ressources nécessaires aux auditeurs afin d'optimiser la préparation des audits. A cet effet, elle met à jour OSIRIS en publiant les documents suivants pour chaque installation :

- ✓ Arrêté de création de la ZPS ;
- ✓ Arrêté de création de l'IP ;
- ✓ Arrêté de création de ZAR ;
- ✓ Arrêté concernant l'ASIP/l'ASP ;
- ✓ Evaluation de sûreté et plan de sûreté de l'installation ;
- ✓ Arrêté d'approbation des ESIP/ESP ainsi que des PSIP/PSP ;
- ✓ Plans d'actions correctives approuvés suite aux audits réalisés ;
- ✓ Notes et commentaires utiles à tous.

Si la base de données OSIRIS ne fournit pas les données désirées, les auditeurs s'adaptent en demandant les documents souhaités auprès des parties intéressées. Si OSIRIS ne fournit pas l'ESP/ESIP ou le PSP/PSIP, les auditeurs demandent ces documents à la MSD.

Une fois un audit réalisé, l'auditeur temps-plein qui l'a effectué enregistre sur OSIRIS qu'il a réalisé un audit en spécifiant les références de l'installation portuaire ou du port audité. Il précise également de

quel type d'audit il s'agit et la date à laquelle celui-ci a eu lieu. Cela facilitera la programmation annuelle des audits.

III. Cadre général du Processus « Audit »

III. A. Cadre réglementaire

III. A. 1) Au niveau international

- ✓ Chapitre XI-2 de la Convention SOLAS ;
- ✓ Code ISPS – Parties A et B.

III. A. 2) Au niveau européen

- ✓ Règlement CE 725/2004 modifié relatif à l'amélioration de la sûreté des navires et des installations portuaires (version en vigueur au 31 mars 2009) ;
- ✓ Directive CE 2005/65 relative à l'amélioration de la sûreté des ports ;
- ✓ Règlement CE 324/2008 du 9 avril 2008 établissant les procédures révisées pour la conduite des inspections effectuées par la Commission dans le domaine de la sûreté maritime.

III. A. 3) Au niveau français

- ✓ Code des Ports Maritimes (Art. L321-1 à L321-8 et R321-1 à R321-52) ;
- ✓ Décret n° 2007-937 du 15 mai 2007 relatif à la sûreté des navires ;
- ✓ Arrêté du 10 avril 2007 fixant la liste des ports mentionnée à l'article R321-15 ;
- ✓ Arrêté du 26 juillet 2007 relatif à l'habilitation des organismes de sûreté ;
- ✓ Arrêté du 7 août 2007 pris en application de l'art. R. 321-6 du CPM ;
- ✓ Arrêté du 22 avril 2008 définissant les modalités d'établissement des évaluations et des plans de sûreté portuaires et des installations portuaires ;
- ✓ Arrêté du 20 mai 2008 fixant la liste des équipements et systèmes intéressant la sûreté portuaire et maritime mis en œuvre dans les zones d'accès restreint ; tels que définis par l'article R. 321-41 du CPM ;
- ✓ Arrêté du 2 juin 2008 fixant les conditions d'organisation des exercices et entraînements de sûreté dans les ports et les installations portuaires ;
- ✓ Arrêté du 4 juin 2008 relatif aux conditions d'accès et de circulation en zone d'accès restreint des ports et des IP et à la délivrance des titres de circulation ;
- ✓ Arrêté du 18 juin 2008 relatif à la délivrance d'un agrément nécessaire pour l'exercice de missions de sûreté ou d'une habilitation nécessaire pour l'accès permanent à une zone d'accès restreint ;
- ✓ Arrêté du 23 septembre 2009 fixant les conditions d'approbation des formations des agents chargés des visites de sûreté préalables à l'accès aux zones d'accès restreint définies aux articles R. 321-31 et R. 321-32 du CPM.

III. B. Cadre normatif

La méthodologie d'audit des systèmes de sûreté portuaire retenue dans ce manuel a été élaborée en suivant « au mieux »[2] la norme internationale ISO 19011 : 2002, appelée « Lignes directrices pour l'audit des systèmes de management de la qualité et/ou de management environnemental ». Ce

[2] Le Manuel et la méthodologie d'audit qui y est décrite ne visant pas à la certification, les auteurs se contentent seulement de suivre « au mieux » les normes ISO citées.

manuel est en parfaite cohérence avec les procédures utilisées par les inspecteurs de la Commission européenne.

III. C. Cadre organisationnel national

Le Gouvernement a mis en place un dispositif institutionnel compétent en matière de sûreté[3]. Le haut fonctionnaire de défense et de sécurité du MEEDDM anime et coordonne la politique en matière de défense, de vigilance, de prévention de crise et de situation d'urgence. Il contrôle la préparation des mesures d'application. De plus, *il s'assure de l'élaboration et de la mise en œuvre des politiques de sécurité dans les secteurs d'activités relevant du ministère, notamment lorsqu'ils sont reconnus d'importance vitale.*
Le Secrétaire général du ministère, haut fonctionnaire de défense et de sécurité "est responsable des missions de défense, de sécurité et d'intelligence économique du ministère". A ce titre il dispose du service de défense, de sécurité et d'intelligence économique qui assure notamment les responsabilités de point de contact national pour la sûreté maritime telles que définies par les dispositions communautaires et internationales.
En matière de sûreté maritime, la Commission européenne indique au HFDS - SDSIE - Point de contact les inspections qu'elle a l'intention de conduire sur le territoire national. Il importe donc que les audits nationaux s'attachent à répondre aux exigences de la réglementation communautaire.

Ce dispositif d'audits nationaux s'articule autour de plusieurs instances décrites ci-dessous.

III. C. 1) Une autorité de sûreté maritime compétente[4]

L'autorité de sûreté maritime compétente est le Directeur Général des Infrastructures, des Transports et de la Mer (DGITM). Placée au sein du Ministère de l'Ecologie, de l'Energie, du Développement Durable et de la Mer, la DGITM a en charge l'ensemble des sujets relatifs aux transports terrestres et maritimes. La Figure 1 ci-après présente la composition de la DGITM.

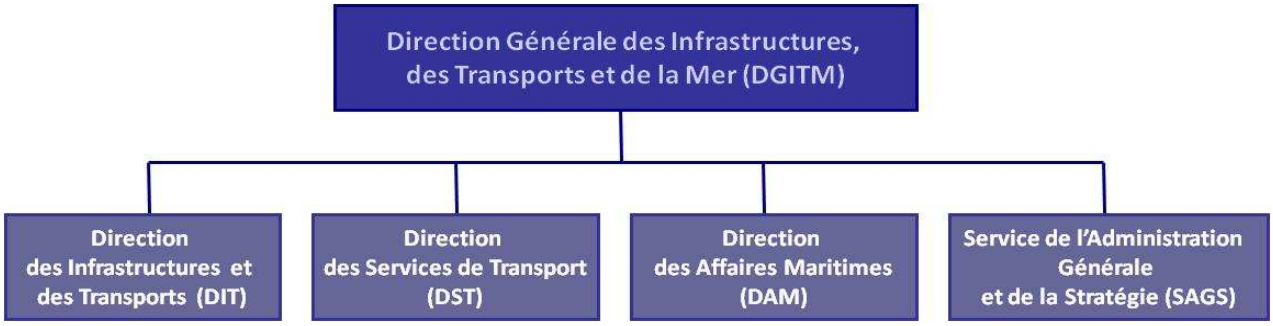

Figure 1 : Composition de la DGITM

III. C. 2) La Direction des Services de Transport (DST)

La DST est composée selon la figure 2 ci-dessous.

[3] Exigence des réglementations internationale et européenne définies précédemment.
[4] « Autorité de sûreté maritime compétente » telle que définie dans le Règlement CE 725/2004. Elle représente aussi l' « autorité désignée » telle que définie dans la règle 1 du Chapitre XI-2 de la Convention SOLAS.

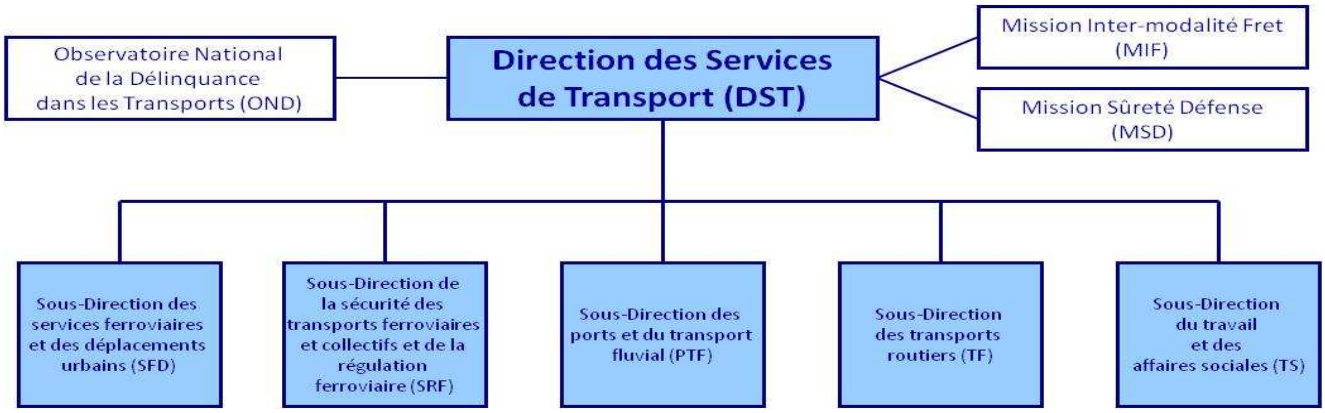

Figure 2 : Composition de la DST

Dans le domaine maritime, la DST prend en charge les missions suivantes :

- ✓ Orientations économiques et organisationnelles de la politique portuaire,
- ✓ Réglementation et régulation économique des transports maritimes ;
- ✓ Sûreté dans les ports.

III. C. 3) La Mission Sûreté Défense (MSD)

Afin de respecter un haut niveau de fiabilité de sûreté dans les transports, la Mission Sûreté-Défense, en liaison directe avec les services de la DST et de la DAM, sous le contrôle du Secrétaire général et haut fonctionnaire de défense et de sécurité, assure le pilotage de l'ensemble des questions de sûreté et de défense liées aux transports terrestres et maritimes.

En termes de sûreté, les missions de la MSD sont les suivantes :

- ✓ Elaborer, dans un esprit d'amélioration continue, les règles et méthodes applicables pour :
  - o les audits,
  - o la délivrance des agréments, habilitations et autres autorisations administratives,
  - o le contrôle des compétences techniques des personnels ;
- ✓ Organiser le contrôle de la mise en œuvre des exigences pour la sûreté maritime.

En termes d'audit de sûreté des installations, la MSD assure les rôles suivants :

- o Organiser les audits des systèmes de sûreté portuaire ;
- o Définir et faire évoluer la méthode d'audit ;
- o Garantir l'homogénéité et la qualité des méthodes d'audit sur tout le territoire et des compétences et connaissances des auditeurs ;
- o Mesurer et contrôler la conformité des installations avec le niveau de sûreté requis.

III. C. 4) Les Auditeurs temps-plein[5]

- ***Recrutement :***

Ils sont choisis parmi les agents du MEEDDM.

- ***Compétences :***

[5] Les inspecteurs nationaux mentionnés dans le règlement CE 324/2008 sont choisis parmi les auditeurs temps-plein.

Pour être habilités par la DGITM, les auditeurs doivent justifier des compétences et connaissances annotées dans le tableau 2 suivant.

Tableau 1 : Domaines de connaissances et de compétences des auditeurs et conditions de formation

Domaine de connaissances et de compétences	Conditions de formation
Monde maritime, organisation et exploitation des ports[6]	Lorsque cette connaissance n'est pas acquise, le futur auditeur doit suivre une formation d'initiation au monde portuaire agréée par la DGITM. Actuellement, est reconnue la formation d'ASIP, délivrée notamment par les centres de l'Ecole Nationale Supérieure Maritime.
Règlementation en matière de sûreté portuaire et maritime	Les auditeurs doivent avoir suivi une formation dont certains agents, en raison de leurs connaissances professionnelles, peuvent être dispensés. Les formations d'ASIP, d'ASN et d'ASC sont reconnues suffisantes pour assurer ce complément de formation. Les autres formations doivent être préalablement reconnues par MSD.
Règles et méthodes applicables pour les audits portuaires	Les auditeurs doivent avoir suivi une formation agréée par la DGITM, dont certains agents, en raison de leurs connaissances professionnelles peuvent être dispensés. Le stage de formation à l'audit portuaire est actuellement délivré par le centre de Nantes de l'école nationale supérieure maritime. Les auditeurs doivent respecter la méthodologie décrite dans ce présent manuel.

- ***Légitimité :***

La qualification d'auditeur temps-plein fait l'objet d'une attestation.

Ils sont désignés par une lettre de mission permanente du directeur de la DGITM pendant la durée de leur affectation à la MSD. Ils sont fondés à détenir les titres suivants:

- ✓ un titre de circulation national[7] ;
- ✓ une carte de commissionnement qu'ils utilisent pour justifier de leur identité et de leur mission ;
- ✓ une assermentation leur permettant de témoigner des écarts rencontrés lors de l'audit en cas de procédures de sanctions administratives.

III. C. 5) Les Auditeurs Volontaires

- ***Recrutement :***

Les auditeurs temps-plein peuvent être accompagnés lors de l'audit par des auditeurs volontaires assurant cette fonction pendant 5 à 10% de leur temps de travail.

Ils peuvent appartenir à différentes entités publiques ou privées telles que le MEEDDM, ou autres ministères concernés par la sûreté maritime. Les officiers de ports détachés dans les ports autonomes et GPM peuvent être auditeurs volontaires.

- ***Compétences :***

[6] Cette connaissance des ports est supposée acquise pour les personnes ayant travaillé dans les services ou établissements suivants : Services maritimes, DAM, Ecole Nationale de la Marine Marchande, ENSM, Centre de Sécurité des Navires, DST, MSD, GPM, Ports autonomes ou concédés. Cette liste n'est pas limitative, notamment en ce qui concerne d'autres ministères dont le personnel est affecté à des tâches en relation avec les ports.

[7] Conformément aux dispositions de l'article R.321-35 du CPM.

L'auditeur volontaire doit disposer de compétences et de connaissances similaires à celles d'un auditeur temps-plein (Voir Tableau 3). Il peut participer à tous les sous-processus de l'audit (sauf 6'inspection), et participe obligatoirement au sous-processus de rédaction du rapport qu'il signe en même temps que l'auditeur temps-plein, chef de mission.

III. C. 6) Conditions d'expérience pour acquérir et conserver la qualification d'auditeur

- ***Auditeur temps plein :***

Afin de maintenir continuellement leur compétence, les auditeurs temps plein doivent justifier d'un minimum de quatre audits effectués dans les 12 mois précédant l'audit (à l'exception des quatre premiers audits nécessaires à la qualification initiale), dont au moins un audit d'une installation contenant une ZAR.

- ***Auditeur volontaire :***

Afin de maintenir continuellement leur compétence, les auditeurs doivent justifier d'un minimum de deux audits effectués dans les 12 mois précédant l'audit (à l'exception des quatre premiers audits nécessaires à la qualification initiale), dont au moins un audit d'une installation contenant une ZAR. A défaut, l'auditeur volontaire se rapprochera de la MSD pour une nouvelle validation éventuelle.

III. C. 7) Documents mis à la disposition des auditeurs temps-plein et volontaires

Tableau 2 : Documents mis à la disposition des auditeurs

Document	Type d'auditeur ayant accès aux documents	Qui fournit les documents ?
Manuel d'audit	Temps-plein et volontaires	MSD
Documents déposés sur la base de données OSIRIS	Temps-plein	MSD et auditeurs temps-pleins
Lettre de notification des audits	Temps-plein et volontaires	MSD
Lettre de notification du rapport d'audit	Temps-plein et volontaires	MSD
Plan d'actions correctives	Temps-plein	L'exploitant
Liste de contrôle	Temps-plein et volontaires	MSD

III. C. 8) Organismes de Sûreté Habilités (OSH)

- ***Délégation des activités d'audit à un organisme de sûreté habilité :***

L'autorité compétente a la faculté juridique de déléguer les activités d'audit à des Organismes de Sûreté Habilités[8] (OSH) dans le cadre d'une relation contractuelle rémunérée. Les organismes de sûreté reçoivent une habilitation telle que prévue dans les articles R. 321-7 à R321-11 du CPM, et ses textes d'application, notamment l'arrêté du 26 juillet 2007.

- ***Compétences :***

[8] Selon l'Art. L321-6 du CPM, « des missions d'évaluation et de contrôle de la sûreté maritime et portuaire peuvent être confiées par l'autorité administrative à des organismes habilités à cet effet. ».

Ces OSH disposent au travers de leurs agents de compétences appropriées en matière de sûreté, et d'une connaissance suffisante des opérations des navires et des ports, pour effectuer une activité d'évaluation, de vérification, d'approbation ou de certification.
Les organismes de sûreté sont habilités par le ministre chargé de la mer pour un ou plusieurs domaines dans lesquels ils sont autorisés à exercer leurs compétences[9].

- ***Conditions d'expérience pour conserver sa qualification :***

Pour effectuer un audit, un OSH et le personnel responsable de l'audit au sein de celui-ci doivent justifier d'un minimum de quatre audits effectués dans les 12 mois précédents l'audit (à l'exception des quatre premiers audits de formation). La réalisation complète d'une évaluation ou d'un plan de sûreté approuvé d'une installation est équivalente à la réalisation d'un audit pour satisfaire à cette condition d'expérience.
L'OSH s'engage sur la vérification de cette condition d'expérience tant pour elle-même que pour son personnel. A tout moment, l'autorité compétente peut demander à l'OSH la justification du respect de cette condition d'expérience.

III. C. 9) Conflits d'intérêts

Les principes de l'audit rendent son exercice impossible si l'auditeur possède des liens juridiques, commerciaux ou hiérarchiques avec l'audité ou en a possédé au cours des trois dernières années.

III. D. Cadre organisationnel local

III. D. 1) Le Préfet

En tant que représentant de l'Etat dans le département, le préfet est responsable :

- ✓ du contrôle des mesures de sûreté des installations portuaires ;
- ✓ de la direction des services de l'Etat concourant à la sûreté des ports et des IP (police, gendarmerie, douanes, etc.).

Plus particulièrement, le préfet est responsable :

- ✓ de la délimitation de la zone portuaire de sûreté, des IP et des ZAR ;
- ✓ de l'approbation des évaluations et des plans de sûreté des installations.

En termes d'audit, le préfet et les services qu'il a mandatés pour cela assurent principalement les rôles suivants :

- ➢ Destinataire des rapports d'audits de sûreté des installations situées dans son département, le préfet doit prendre connaissance des conclusions d'audit qui y sont relatées ;
- ➢ Destinataire du plan d'actions correctives constitué par l'exploitant après rapport d'audit, le préfet est responsable de la validation ou du refus de celui-ci ;

[9] Selon l'arrêté du 26 juillet 2007 relatif à l'habilitation des organismes de sûreté, les domaines dans lesquels les OSH peuvent être habilités sont les suivants :
- Pour les IP : terminaux à passagers (transbordeurs et navires de croisière) ; terminaux à conteneurs ; terminaux pour les produits pétroliers, gaziers et autres marchandises dangereuses ; autres terminaux.
- Pour les navires : navires à passagers ; porte-conteneurs ; pétroliers, navires-citernes pour produits chimiques et transporteurs de gaz ; autres navires.

- Une fois le plan d'actions correctives approuvé, il doit le diffuser à l'ASIP et l'ASP, à la MSD (et à l'équipe d'audit) ;
- Le préfet doit s'assurer que l'échéancier d'application de ces actions correctives est bien respecté. Un audit de suivi peut néanmoins être réalisé par la MSD ;
- En cas de non respect de l'échéancier fixé et approuvé, le préfet doit prendre les mesures adaptées : cela peut consister en une mise en demeure ou au retrait de la déclaration de conformité. Pour prendre une telle décision, il s'appuiera, le cas échéant, sur les constats d'audit effectués lors de l'audit de suivi.

III. D. 2) Le Comité Local de Sûreté Portuaire (CLSP)

Dans chacun des ports soumis au Règlement (CE) 725/2004[10], est établi un comité local de sûreté portuaire, présidé par le préfet. Le CLSP est chargé[11] :

- d'apporter son avis au préfet sur la sûreté du port et des installations portuaires et l'adéquation des mesures de sûreté adoptées ou envisagées ;
- de proposer au préfet, en cas de circonstances exceptionnelles, l'adoption de mesures spécifiques temporaires s'ajoutant aux mesures permanentes de sûreté ;
- d'examiner la répartition des tâches entre les divers organismes ayant des responsabilités en matière de sûreté ;
- d'apporter un avis au préfet sur les évaluations et les plans de sûreté des ports et installations portuaires pour que celui-ci donne son approbation initiale ou ultérieure (cas de renouvellement ou de modifications significatives).

[10] Selon l'article R 321-15 du Code des Ports Maritimes.
[11] Selon l'Art. R 321-5 du Code des Ports Maritimes.

IV. CONFIDENTIALITÉ

IV. A. Qu'entendons-nous par la notion « CONFIDENTIEL – SÛRETE » ?

La mention « CONFIDENTIEL – SÛRETE » sera apposée (en majuscules rouges et caractères gras) en en-tête et/ou pied de page des documents suivants:

- rapport d'audit ;
- lettre de notification d'envoi du rapport d'audit ;
- liste de contrôle renseignée ;
- ESIP, PSIP, ESP et PSP à jour de leur dernière modification.

Il s'agit d'une **mention de protection** du document visant à la **diffusion restreinte** de celui-ci, car la divulgation non autorisée des informations qu'il contient pourrait nuire à la sûreté de l'installation. Il convient donc de définir dans chaque plan des règles de diffusion, de conservation, d'archivage et de destruction de tout document ainsi marqué.
Il ne s'agit pas d'une « confidentialité de défense » relevant de l'IGI 1300 SGDN, approuvée par arrêté du 23 juillet 2010, qui peut être appliquée à des documents connexes relevant d'autres réglementations pouvant intéresser la sûreté portuaire.
Toutes les personnes participant à un audit sont tenues de garantir la confidentialité des faits, informations et documents qu'ils ont à connaître lors de l'audit. Afin de pouvoir accéder à tous les documents se rapportant à leur mission, les auditeurs sont habilités « Confidentiel Défense ».

IV. B. Critères de gestion des documents portant la mention « CONFIDENTIEL – SÛRETE »

Tableau 3 : Critères de gestion des documents portant la mention "CONFIDENTIEL-SÛRETE"

Document	Personnes ou catégories de personnes autorisées à consulter ce document	Mode d'envoi	Règle de conservation et d'archivage
Rapport d'audit	- Auditeurs temps-plein et temps-partiel - DGITM/DST/MSD - Préfet et les personnes de la préfecture qu'il aura désignées - Exploitant - ASIP - ASP	- Courriel chiffré - ou courrier postal. Concernant le PSP ou le PSIP, l'idéal est que la MSD (ou les auditeurs le cas échéant) les reçoive, non pas en version imprimée, mais enregistré sur un CD protégé par un code. Ce code sera notifié dans une lettre envoyée séparément. Le PSP ou PSIP sera alors diffusé sur OSIRIS.	• *Conservation :* Ces documents sont conservés sous format électronique sur des systèmes informatiques protégés (accessibles par mots de passe) auxquels seules les personnes autorisées à consulter ce document ont accès. La signature de ces documents sera apposée sous forme d'image. Une version papier peut exister dans les bureaux respectifs de ces personnes autorisées. Cependant, celles-ci doivent prendre les mesures nécessaires afin que ces documents restent confidentiels. • *Archivage :*
Lettres de notification du rapport d'audit	Destinataires de la lettre. Ce peut être : - DGITM/DST/MSD - Préfet et les personnes de la préfecture qu'il aura désignées - Exploitant - ASIP - ASP		

Liste de contrôle renseignée (Voir modèle de la liste de contrôle en annexe 2)	- Auditeurs temps-plein et volontaires ; - DGITM/DST/MSD ; - Préfet et les personnes de la préfecture qu'il aura désignées ; - Exploitant ; - ASIP ; - ASP		Il convient de garder ces documents pendant 5 ans minimum, délai après lequel ils seront supprimés du serveur informatique et les versions papiers détruites. Une version ne devrait pas être conservée plus de 10 ans.

V. LE PROCESSUS « AUDIT »

V. A. Qu'entendons-nous par « audit des systèmes de sûreté portuaire » ?

V. A. 1) Objectifs

Les objectifs de l'audit des systèmes de sûreté des ports et des IP sont les suivants :

- ✓ Déterminer le degré de conformité du système de sûreté de l'installation par rapport à la réglementation (l'auditeur comparera les preuves d'audit obtenues aux critères déterminés dans les exigences réglementaires) ;
- ✓ Evaluer la maîtrise du système de sûreté de l'installation ;
- ✓ Obtenir la rectification des non-conformités détectées dans les délais les plus brefs possibles ;
- ✓ Fournir à la DGITM des indicateurs de mesure du niveau de la sûreté des installations et de la tendance d'évolution, afin que celle-ci oriente son programme et ses méthodes d'audits.

Insistons sur le fait que les auditeurs et l'autorité compétente doivent entretenir une relation de long terme avec les audités s'ils veulent observer une réelle coopération de leur part. Ils doivent accompagner l'exploitant dans l'évolution du système de sûreté de son installation et ceci dans une démarche qualité et ainsi un processus d'amélioration continue.
A cet égard, l'audit n'a pas pour objectifs :

- ✓ d'être inquisiteur ou insidieux, mais est basé sur le factuel, le tangible et l'objectivité ;
- ✓ de sanctionner l'exploitant pour les non-conformités constatées mais l'audit peut servir à alimenter le dossier permettant d'initier des sanctions administratives et pénales[12].

V. A. 2) Principes de l'audit

Les principes d'audit suivants doivent s'appliquer à chaque auditeur :

- ✓ **La déontologie :** la confiance, l'intégrité et la discrétion représentent le fondement du professionnalisme dans un audit ;
- ✓ **L'impartialité :** les constats, les conclusions et les rapports d'audit reflètent de manière honnête et précise les activités de l'audit. L'auditeur doit consigner :
  - o les obstacles importants rencontrés,
  - o les questions non résolues,
  - o les avis divergents ;
- ✓ **La conscience professionnelle :** les auditeurs doivent agir en accord avec l'importance des tâches qui leur sont confiées et la confiance que leur ont accordée l'autorité compétente, le préfet et les audités ;
- ✓ **L'indépendance :** voir le paragraphe « Conflits d'intérêts » ;
- ✓ **Approche fondée sur la preuve :** les preuves d'audit sont vérifiables et s'appuient sur des échantillons d'information disponibles. La confiance accordée aux conclusions d'audit est liée à cet échantillonnage (dont l'étendue des ressources et la durée sont limitées).

[12] Sanctions prévues aux articles R. 321-49 à 52 du Code des ports maritimes.

V. B. Champ d'application de l'audit

L'audit des systèmes de sûreté porte sur les ports et les installations portuaires. Cependant, même si ce manuel ne s'applique pas directement aux audits des OSH et entreprises de formation à la sûreté, la méthodologie d'audit qui y est décrite pourrait être employée à cet effet[13].

V. C. Présentation de l'audit par approche processus

De façon générale, le processus « audit » est piloté par l'autorité compétente. Les divers acteurs, définis dans les parties « Cadre organisationnel national », « Cadre organisationnel local » interviennent dans les sous-processus.

Le processus « audit » est constitué (Figure 1) des six sous-processus suivants :

1. Programmation des audits,
2. Déclenchement et notification de l'audit,
3. Préparation de l'audit,
4. Réalisation de l'audit,
5. Rédaction et diffusion du rapport d'audit,
6. Suivi de l'audit.

Un septième sous-processus peut apparaître après le suivi de l'audit, le sous-processus 6', appelé « inspection de suivi », si les preuves de l'audit de suivi révèlent que les actions correctives prévues dans le plan d'actions approuvé n'ont pas été effectuées dans les délais impartis.

[13] Parallèlement, les inspecteurs de sécurité maritime appliquent leur propre méthodologie d'audit à l'occasion de leur visite de navires.

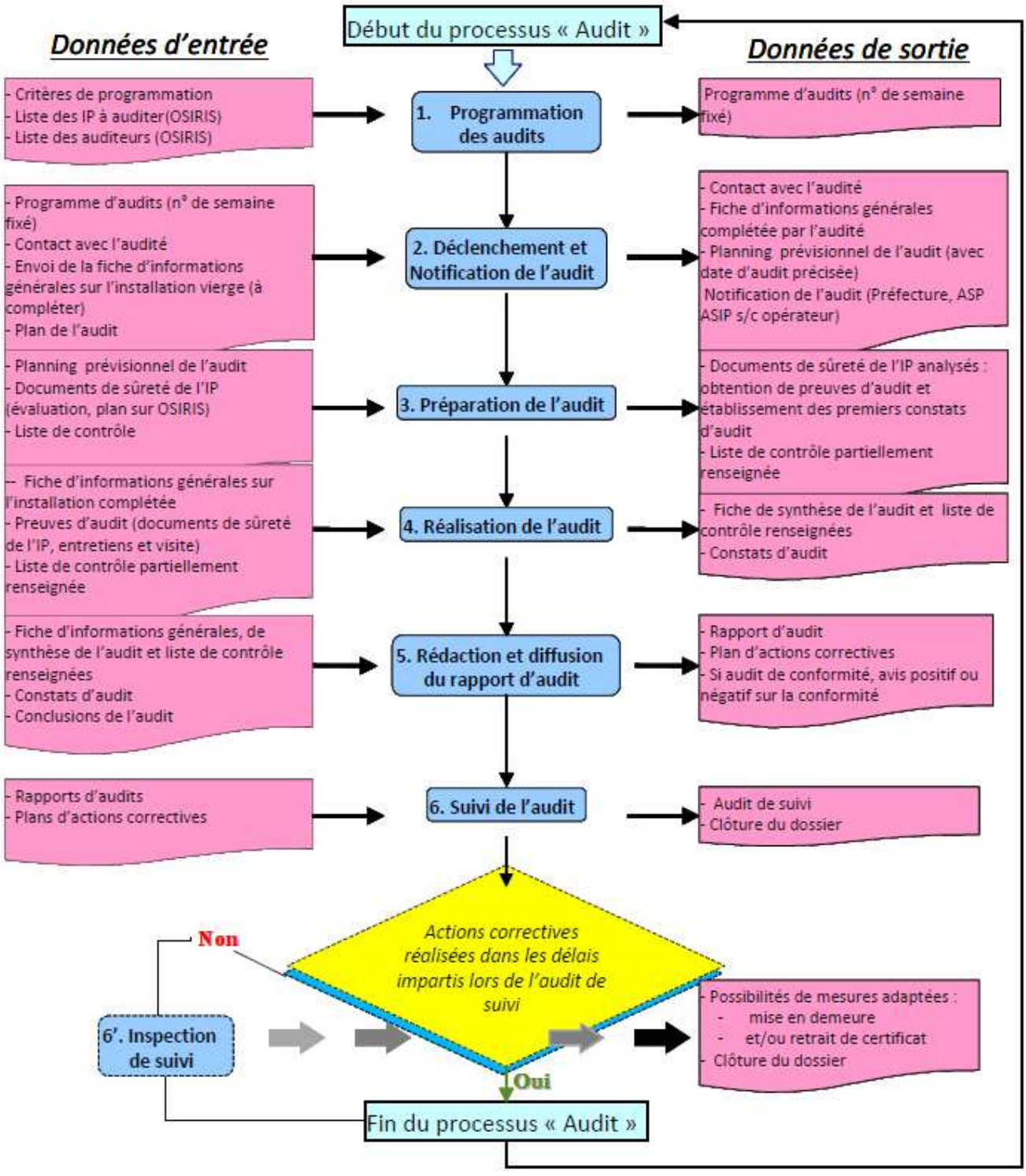

Figure 3 : Logigramme organisant les phases du processus "audit"

VI. Sous-Processus « Programmation des audits »

VI. A. Présentation générale du sous-processus « Programmation des audits »

La **programmation** a pour but de définir à l'avance dans le temps et dans l'espace les activités et audits à mener et les responsabilités associées.
En moyenne, doivent être réalisés annuellement une vingtaine d'audits par auditeur temps-plein. La base de données OSIRIS fournit les données sur les audits réalisés et permet le choix des audits à réaliser.
Le logigramme suivant (Figure 4) présente les activités du sous-processus de programmation des audits.

VI. B. Méthodologie de programmation des audits

VI. B. 1) Activités du sous-processus « Programmation des audits »

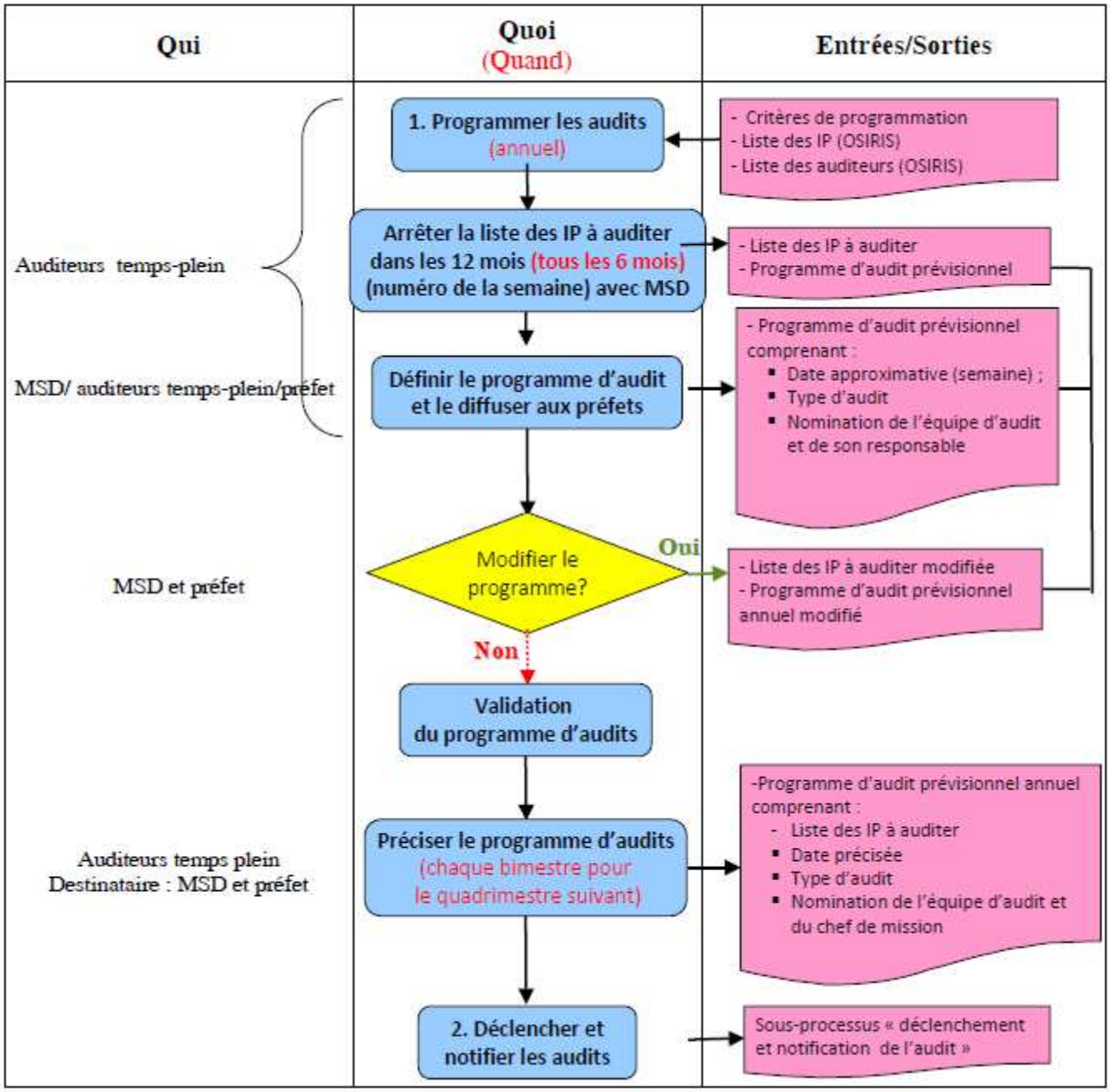

Figure 4 : Logigramme présentant les liens organisationnels entre les activités du sous-processus "Programmation des audits"

VI. B. 2) Responsabilités

Les auditeurs temps-plein établissent leurs programmes d'audits respectifs et le soumettent à l'autorité compétente qui elle-même informe les préfets des audits prévus dans leurs départements respectifs.
Au préalable, MSD doit fournir aux auditeurs (sur OSIRIS) les données ressources nécessaires (voir données d'entrées Figure 4).

VI. B. 3) Périodicité

En suivant le déroulement des activités décrites en Figure 4, au 1er janvier et au 1er juillet de chaque année (voir explication Figure 5 ci-après), les auditeurs temps-plein établissent un programme d'audits prévisionnel annuel glissant.
Pour un meilleur suivi du programme, l'auditeur temps-plein rend compte tous les deux mois à l'autorité compétente du programme d'audits des quatre mois suivants (voir explication Figure 5 ci-après). Celle-ci fait part au préfet des audits programmés au moins un mois avant leur exécution.

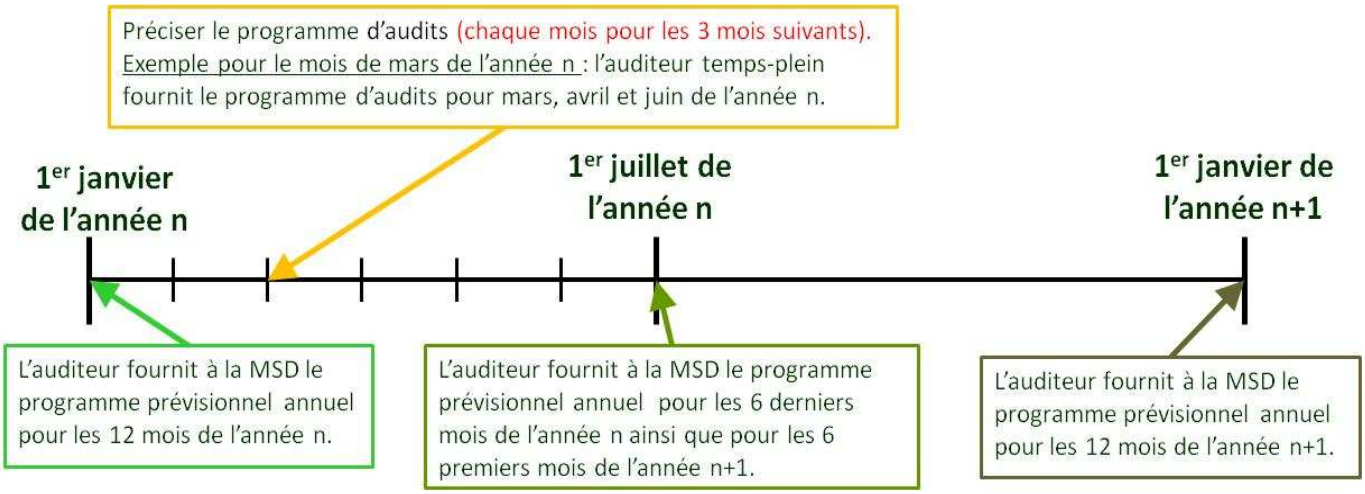

Figure 5: Illustration de la réalisation du programme d'audits glissant

VI. B. 4) Critères de programmation

Lorsqu'il réalise son programme d'audits, l'auditeur temps-plein doit se baser sur les critères objectifs présentés dans le tableau 5 ci-dessous, afin d'optimiser son temps de travail, ses frais de déplacement, le nombre d'audits réalisés par an.

Tableau 4 : Critères de programmation des audits

Critères de programmation	Ressources	Responsabilités de l'auditeur temps-plein relatives aux critères de programmation
Audit de conformité	*Demande d'audit de conformité par le CLSP et le préfet*	Il devra intégrer dans son programme annuel cet audit.
Département d'implantation de l'IP ou du port	*Disponibles sur OSIRIS :* - *Liste des ports et IP* - *Liste des IP avec ZAR*	Il établit son programme d'audits sur la façade maritime qui lui est attribuée. S'il la partage avec un autre auditeur temps-plein, ceux-ci doivent se concerter pour établir leurs programmes respectifs.
Disponibilités des auditeurs temps-plein et volontaires ainsi que des audités (Critères de déprogrammation)	- *Coordonnées des auditeurs sur OSIRIS* - *Contact avec l'audité*	Une équipe d'audit est constituée à minima d'un auditeur temps-plein et d'un volontaire. L'auditeur temps-plein sera désigné comme chef de mission (ou responsable de l'audit). Il faut éviter d'avoir deux auditeurs temps-plein sur un même audit car les compétences s'avèreraient mal réparties entraînant peu d'efficience du programme annuel. (En cas d'indisponibilité d'un auditeur ou de l'audité, il s'agira de déprogrammer l'audit uniquement si aucun contact avec l'audité et le préfet n'a eu lieu)
Liste des IP et ports non-audités	*Doivent être disponibles sur OSIRIS :* - *Dates et types des audits réalisés pour chaque installation (publiés par les auditeurs temps-plein) ;* - *Les rapports d'audits (publiés par les auditeurs temps-plein) ;* - *Le plan d'actions correctives concernant les non-conformités, remarques et points faibles détectés lors des derniers audits (publiés par MSD)*	Les installations encore non auditées au moment de la mise en œuvre du programme d'audit doivent être considérées en priorité. Ensuite, l'auditeur temps-plein choisit d'auditer en priorité, parmi les installations non auditées, celles qui contiennent des ZAR et qui devront donc être auditées tous les deux ans et demi.
Critère de proximité en fonction de la situation géographique des installations à auditer	- *Liste des installations encore non auditées* - *Carte de France si nécessaire*	Une fois que l'auditeur temps-plein a repéré une installation à auditer en priorité, il doit prendre en compte les installations encore non auditées situées à proximité ou nécessitant un audit de suivi d'ici peu. En effet, afin d'économiser des frais de mission, même si la (ou les) installation(s) n'est pas à auditer en priorité, l'auditeur envisagera de l'auditer au cours du même voyage effectué pour auditer l'installation prioritaire.
Inspection européenne ou visite US Coast Guard programmées	- *Notification de l'inspection ou de la visite à MSD* - *Compte-rendu d'inspection à fournir par MSD sur OSIRIS*	Dans le cas où une inspection de la CE ou une visite US Coast Guard est prévue sur une installation à la même période que celle que l'auditeur temps-plein avait prévue pour l'audit programmé, cette installation ne sera alors plus à auditer en priorité et

(Critère de déprogrammation) ainsi que les constats lors des inspections		l'audit programmé sera alors repoussé (dans environ 1 an). Lorsque l'installation a déjà été inspectée par la CE, l'auditeur devra tenir compte des constats faits durant l'inspection car si ces constats ont révélé des non-conformités majeures, l'auditeur temps-plein devra davantage se baser sur un audit de suivi que sur un audit programmé.
Constats réalisés lors du dernier audit	*Rapports d'audit, validés par MSD et publiés par les auditeurs temps-pleins sur OSIRIS* *Et* *Plans d'actions correctives approuvés par le préfet.*	Selon l'importance des constats effectués lors de l'audit précédent, l'auditeur temps-plein pourra intégrer dans son programme un (ou des) audit(s) de suivi. L'auditeur temps-plein peut consulter le plan d'actions correctives et les échéanciers de mise en œuvre de celles-ci. L'audit de suivi se fera préférentiellement au terme prévu de mise en œuvre des actions. Dans le cas où les plans d'actions correctives et les rapports d'audit ne font apparaître que des remarques ou des recommandations, un audit de suivi sur site n'est pas nécessaire.
	Documents de sûreté de l'installation disponibles sur OSIRIS	En cas de constats entraînant une modification de l'évaluation ou du plan de sûreté, l'auditeur pourra consulter la bonne progression du système de sûreté de l'installation en consultant si le nouveau plan de sûreté a été approuvé dans les délais fixés. Dans le cas contraire, l'audit de suivi sera impératif.
Audit inopiné	*A la demande de l'autorité compétente.*	Par définition, l'audit inopiné n'est pas programmé mais réalisé à la demande de la MSD.
Adaptation à la situation pour un meilleur échantillonnage des preuves d'audit sur site	*Contact et discussion avec l'audité*	Afin de pouvoir réellement observer les mesures de sûreté appliquées, lorsque l'auditeur définit son plan de l'audit, il sera préférable qu'il fixe la date d'audit d'une installation au jour où doit avoir lieu une interface avec un navire si cela est en adéquation avec les critères qu'il souhaite vérifier.

VI. B. 5) Mise en œuvre du programme d'audits

Le document généré, appelé « Enregistrement du programme d'audits annuel » doit comprendre, sous forme de tableau, les éléments suivants :

- Nom, numéro et adresse (ville et code postal) de l'IP ou du port audité,
- Noms et prénoms des représentants de l'IP : exploitant, ASP et ASIP,
- Identité de l'équipe d'audit (auditeur temps-plein, auditeur volontaire)
- Non-conformités décelées lors du dernier audit,
- Semaine prévue pour l'audit (et la date lorsque le programme d'audit est confirmé chaque mois),
- Type d'audit (programmé, demandé, suivi, ou inopiné).

VI. C. Indicateurs de performance du sous-processus

Il conviendra de fixer des indicateurs de performance de cette programmation afin de visualiser l'évolution de la performance de la programmation des audits.

On suivra en particulier :

- ✓ l'évolution du nombre d'audits programmés réalisés dans l'année civile,
- ✓ l'évolution du nombre d'audits programmés réalisés par façade maritime et par auditeur dans l'année civile,
- ✓ l'évolution du nombre d'audits déprogrammés dans l'année civile.

VII. Sous-Processus « Déclenchement et Notification de l'audit »

VII. A. Présentation générale du sous-processus « Déclenchement et Notification de l'audit »

Ce sous-processus est un préliminaire à la préparation de l'audit par l'équipe d'audit. Afin d'optimiser le temps imparti pour les audits, il conviendra de respecter les délais fixés.
Le **déclenchement de l'audit** consiste en :

- ✓ la prise de contact avec l'audité par le chef de mission afin d'étudier l'organisation de l'audit,
- ✓ la réalisation d'un document de cadrage de l'audit, le « Plan de l'audit », par le chef de mission. Ce document sera une aide à la réalisation de la « Fiche de synthèse de l'audit ».

La **notification de l'audit** a pour objet l'information des différentes parties intéressées de l'avènement prochain de l'audit. Afin de cadrer l'audit, cette notification devra préciser les éléments définis dans le planning de l'audit que le chef de mission aura réalisé.

VII. B. Méthodologie de déclenchement et de notification de l'audit

VII. B. 1) Responsabilités

Déroulement de l'audit : Chef de mission
Notification de l'audit : Autorité compétente

VII. B. 2) Activités du sous-processus « Déclenchement et notification de l'audit »

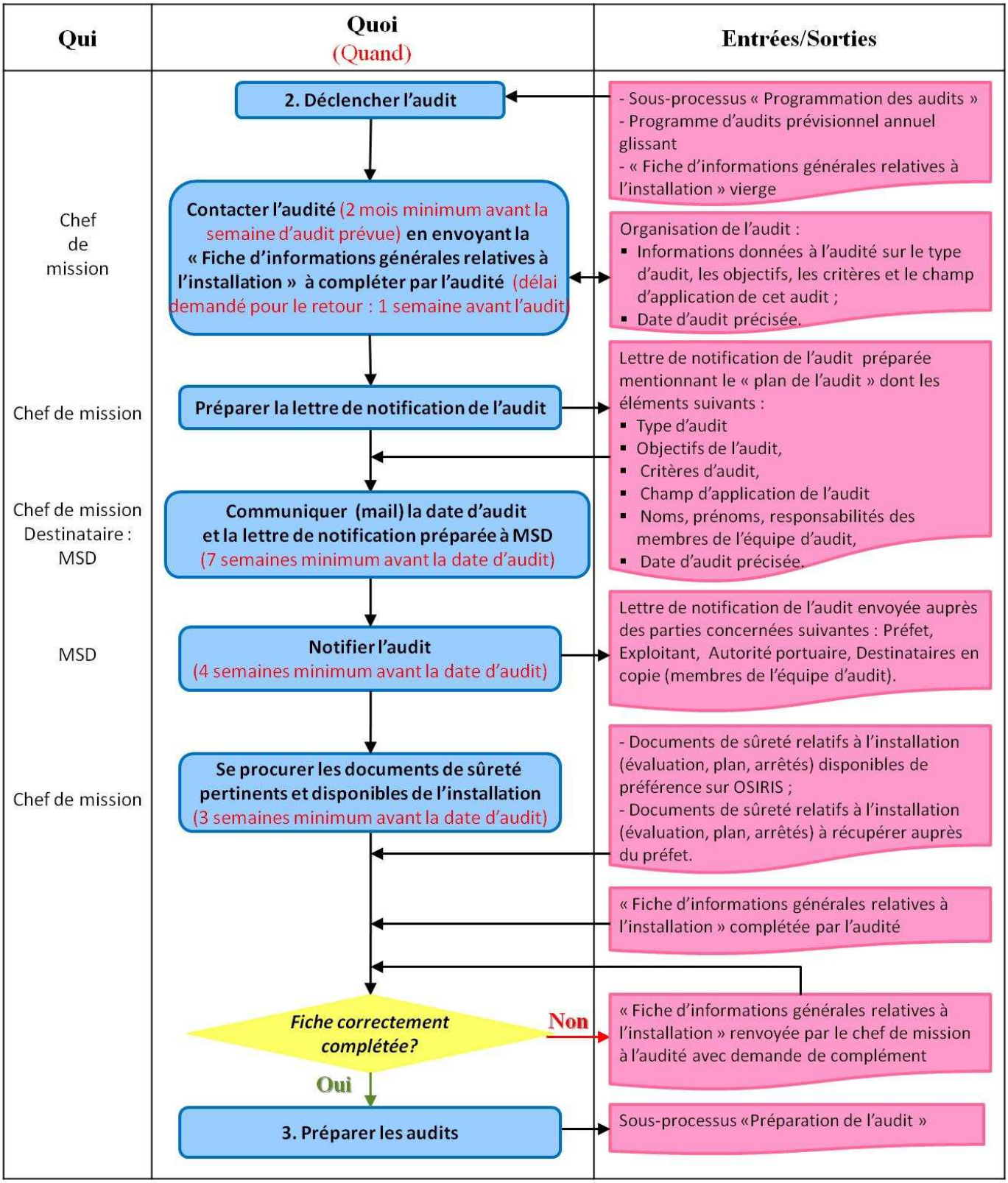

Figure 6 : Logigramme présentant les liens organisationnels entre les activités du sous-processus "Déclenchement et Notification de l'audit"

VII. B. 3) Déclenchement de l'audit

A partir du programme d'audits annuel prévisionnel, le chef de mission contacte l'audité deux mois minimum avant la semaine d'audit prévue afin :

- d'informer celui-ci de l'audit à venir et plus particulièrement du type d'audit, des objectifs, des critères et du champ d'application de l'audit ;
- de préciser la date exacte de l'audit ;
- de lui envoyer la « Fiche d'informations générales relatives à l'installation » vierge pour que l'audité la complète et lui retourne dûment renseignée au moins une semaine avant l'audit. L'auditeur la renverra à l'audité en lui demandant de compléter les informations manquantes le cas échéant.

Afin de cadrer ses activités d'audit, le chef de mission se prépare un document « Plan de l'audit » précisant les éléments suivants :

- Date d'audit précisée
- Type d'audit,
- Objectifs de l'audit,
- Critères de l'audit,
- Champ d'application de l'audit,
- Nom et prénoms des membres de l'équipe d'audit.

Il prépare alors la lettre de notification de l'audit mentionnant les éléments du plan de l'audit ci-dessus et communique cette lettre à la MSD.

VII. B. 4) Notification de l'audit

L'autorité compétente envoie la lettre de notification (des modèles types de lettres de notification sont disponibles à la MSD) rédigée par le chef de mission quatre semaines minimum avant l'audit programmé.
S'il s'agit de l'audit d'un port, cette lettre sera envoyée au préfet, ainsi qu'à l'autorité portuaire. S'il s'agit de l'audit d'une IP, la lettre sera envoyée au préfet ainsi qu'à l'exploitant de l'installation portuaire.
Dans les deux cas, l'autorité compétente met en copie les membres de l'équipe d'audit.

Une fois la lettre de notification reçue, le chef de mission peut alors se procurer, en priorité sur OSIRIS, les documents relatifs à la sûreté de l'installation, minimum 3 semaines avant l'audit, afin de passer au 3ème sous-processus « Préparation de l'audit ». Si ces documents ne sont pas disponibles sur OSIRIS, le chef de mission les demande au préfet concerné.

Les audits de conformité sont réalisés à la demande du préfet et intégrés dans le programme général des audits.
Les audits inopinés peuvent être notifiés sans préavis à l'exploitant lors de l'arrivée des auditeurs sur l'installation (un préavis de quelques jours est néanmoins préférable), mais ils sont systématiquement notifiés au préfet.

VIII. Présentation de la Liste de Contrôle de l'Audit

VIII. A. Objectifs

- ✓ Guider l'auditeur pour l'aider à balayer la totalité :
  - o du champ réglementaire de la sûreté portuaire,
  - o le maximum de preuves d'audit possibles de manière à faire converger celles-ci pour obtenir des constats d'audit fiables ;
- ✓ Garantir l'homogénéité des audits quels que soient les auditeurs et les installations ;
- ✓ Servir de recueil des constats d'audit y compris les mineures ;
- ✓ Compiler les suggestions possibles d'actions correctives par les auditeurs.

Ce n'est pas un cadre limitatif ; les auditeurs peuvent aller au-delà de cette liste, en particulier pour prendre en compte les informations complémentaires qu'ils ont reçues lors de la réunion de démarrage.

VIII. B. Utilisation

La liste de contrôle se présente sous forme d'un fichier EXCEL comportant trois feuilles :

- ➢ Un glossaire des abréviations utilisées dans la liste de contrôle ;
- ➢ La liste de contrôle avec ses commentaires ;
- ➢ Et la liste de contrôle que l'auditeur doit renseigner (présentée en Annexe 2 de ce manuel pour les ports (appendice 2.1) et pour les IP (appendice 2.2)).

Les deux types de liste sont également disponibles sous format PDF.

VIII. B. 1) La liste de contrôle et ses commentaires

Ses commentaires serviront en quelque sorte de guide à l'auditeur. Elle est composée des rubriques suivantes :

1. Critère et Questionnement : les critères sont les items sur lesquels l'audit va être effectué et chaque questionnement concerne un point précis, relatifs aux items, à évaluer.

2. Mode de preuve : afin de répondre à chacun des questionnements de manière certaine, l'auditeur devra récupérer des sources d'informations (preuves d'audit) de quatre types. Selon que les cases PSP, D, V ou I sont cochées ou non, l'auditeur pourra recueillir une à quatre preuves d'audit de façon à confirmer son constat. Les quatre types de preuves sont les suivants :

- ➢ **L'évaluation et le plan de sûreté de l'installation** (disponibles en priorité sur OSIRIS ou récupérées par le chef de mission de l'audit auprès des parties concernées) **(ESP-PSP ou ESIP-PSIP)** : l'auditeur consulte ces documents afin de savoir si les menaces, vulnérabilités et risques ont été correctement identifiés selon une méthode appropriée. Le plan de sûreté de l'installation doit alors présenter quels sont, en termes de sûreté, les mesures, les procédures et les moyens humains, organisationnels et techniques mis en œuvre pour faire face aux risques identifiés lors de l'évaluation ;
- ➢ **Les preuves documentaires (D)** (autres que l'évaluation et le plan de sûreté de l'installation) qui seront davantage consultées lors du processus « réalisation de l'audit ». **Ces documents sont des**

preuves écrites importantes de la bonne application du plan de sûreté sur le terrain au quotidien. Il peut s'agir de :

- Arrêtés préfectoraux (disponibles en priorité sur OSIRIS).
- Registres de sûreté de l'installation dont le registre des incidents de sûreté renseigné par les actions correctives qui ont été mises en place dans l'immédiat et ensuite. Ce peut être les registres de formation, exercices et entraînements réalisés, les registres relatifs aux modifications du niveau de sûreté, registres des inspections et audits internes effectués, etc.
- Documents consultés sur site tels que la politique de sûreté de l'installation, les objectifs, les normes, les plans, des dessins, des contrats, des supports de formation, des conventions entre parties, etc.
- Enregistrements consultés sur site tels que des contrôles, des comptes-rendus de réunion, des rapports d'audits internes, etc. ;

➢ **Constats visuels lors de la visite sur site (V)** : ils permettent d'observer si les moyens techniques et humains définis dans le plan de sûreté sont réellement mis en œuvre sur le terrain et si les procédures sont effectuées de la même manière que celle décrite dans le plan de sûreté. L'auditeur peut alors vérifier le bon fonctionnement du matériel de sûreté. L'auditeur peut prendre des photos de l'installation et de ses activités en respectant la vie privée d'autrui et leur confidentialité. Ces photos peuvent illustrer les écarts identifiés. En analysant ces photos après la visite, elles pourraient permettre de déceler des écarts qui n'auraient pas été vus lors de la visite.

➢ **Les informations recueillies lors des interview/entretiens de personnes présentes sur l'installation (I)** : agents de sûreté de l'installation, personnels de l'installation ou d'entreprises extérieures qu'ils aient ou non des tâches relatives à la sûreté. La présence de leurs supérieurs hiérarchiques ou de l'audité est déconseillée.

3. COMMENTAIRES : pour aider l'auditeur, des commentaires sont parfois attribués au questionnement pour l'aider dans le recueil des preuves d'audit.

VIII. B. 2) La liste de contrôle à renseigner

On retrouve dans cette feuille EXCEL les rubriques « CRITÈRE ET QUESTIONNEMENT » et « MODE DE PREUVE » (La liste de contrôle à renseigner est présentée en Annexe 2 de ce manuel).
Pour le renseignement de la liste qui a lieu lors de la revue documentaire et du sous-processus de réalisation de l'audit, suivre les figures 7 et 8.

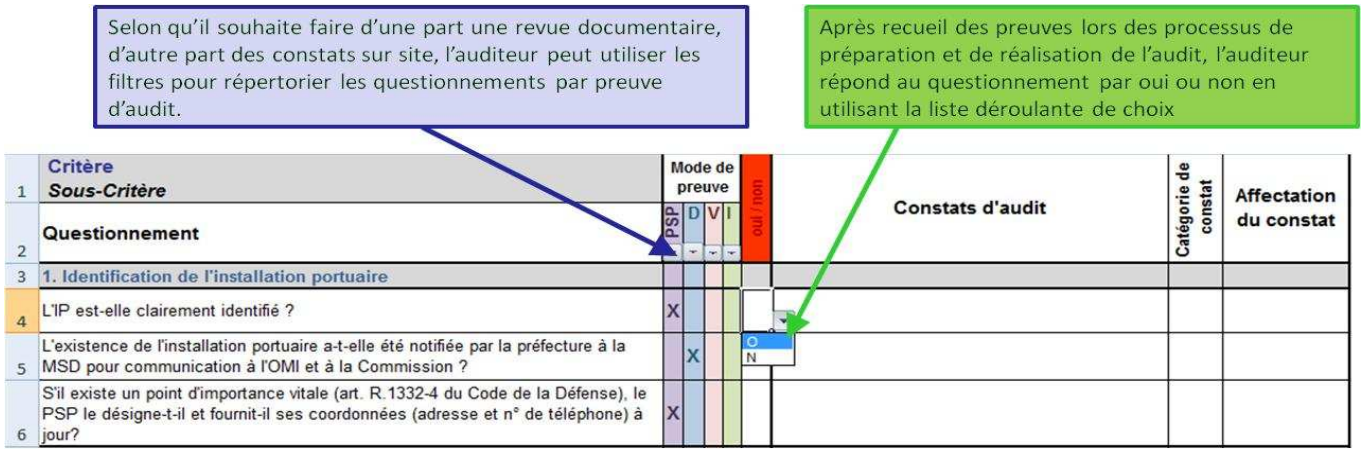

Figure 7 : Guide pour le renseignement de la liste de contrôle.

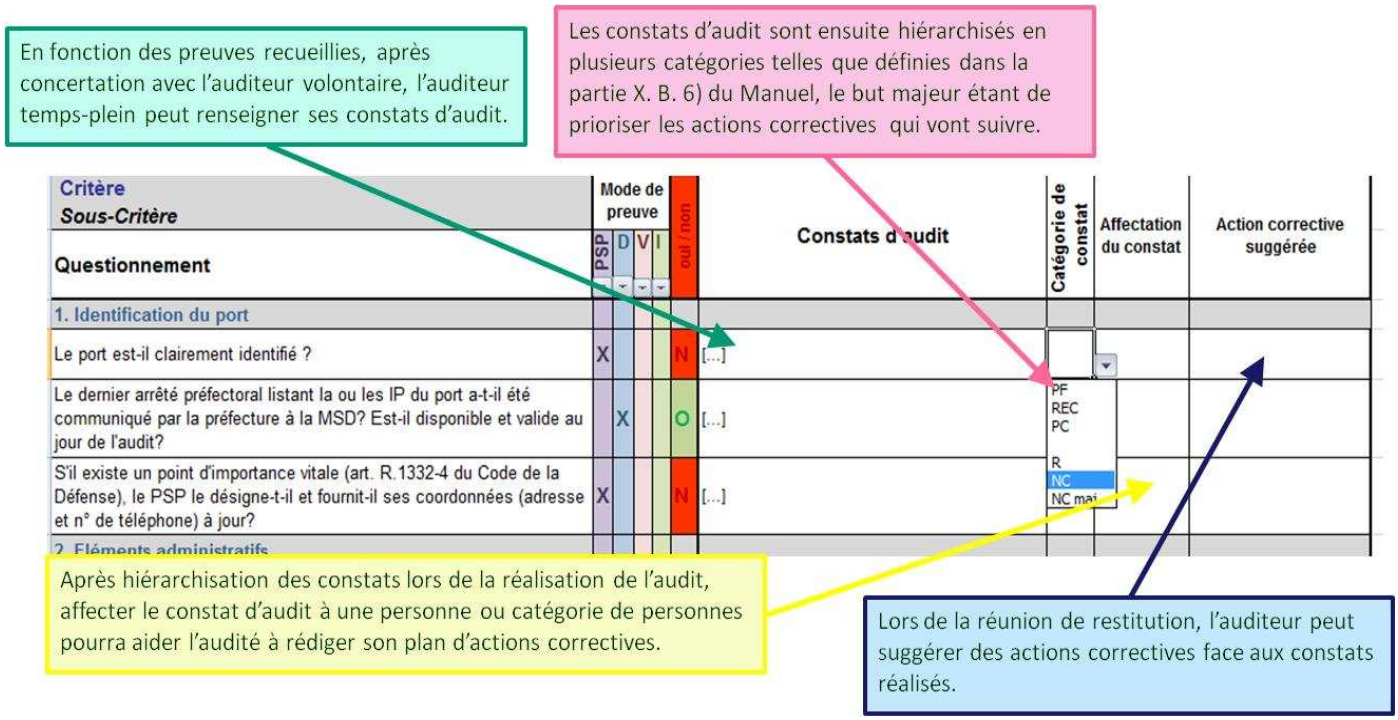

Figure 8 : Guide pour le renseignement de la liste de contrôle.

Afin que les audités aient connaissance de ce que l'on attend d'eux lors d'un audit de sûreté, la liste de contrôle pourra leur être envoyée une fois et dès qu'elle sera modifiée.

IX. Sous-processus « Préparation de l'audit »

IX. A. Présentation générale du sous-processus « Préparation de l'audit »

Ce sous-processus est déterminant pour l'efficacité et l'efficience de la réalisation de l'audit sur site. En maîtrisant les documents de sûreté relatifs à l'installation avant l'audit, l'équipe d'audit aura davantage de temps pour recueillir d'autres preuves d'audit sur site (registres de sûreté, entretiens et observation des activités et des moyens techniques).
Trois activités principales sont à réaliser :

- La revue documentaire des documents de sûreté de l'installation ;
- La préparation de l'échantillonnage prévisionnel des preuves sur site et la préparation les documents de travail ;
- Le contact avec l'audité pour organiser les activités d'audit sur site.

IX. B. Méthodologie de préparation de l'audit

IX. B. 1) Activités du sous-processus « Préparation de l'audit »

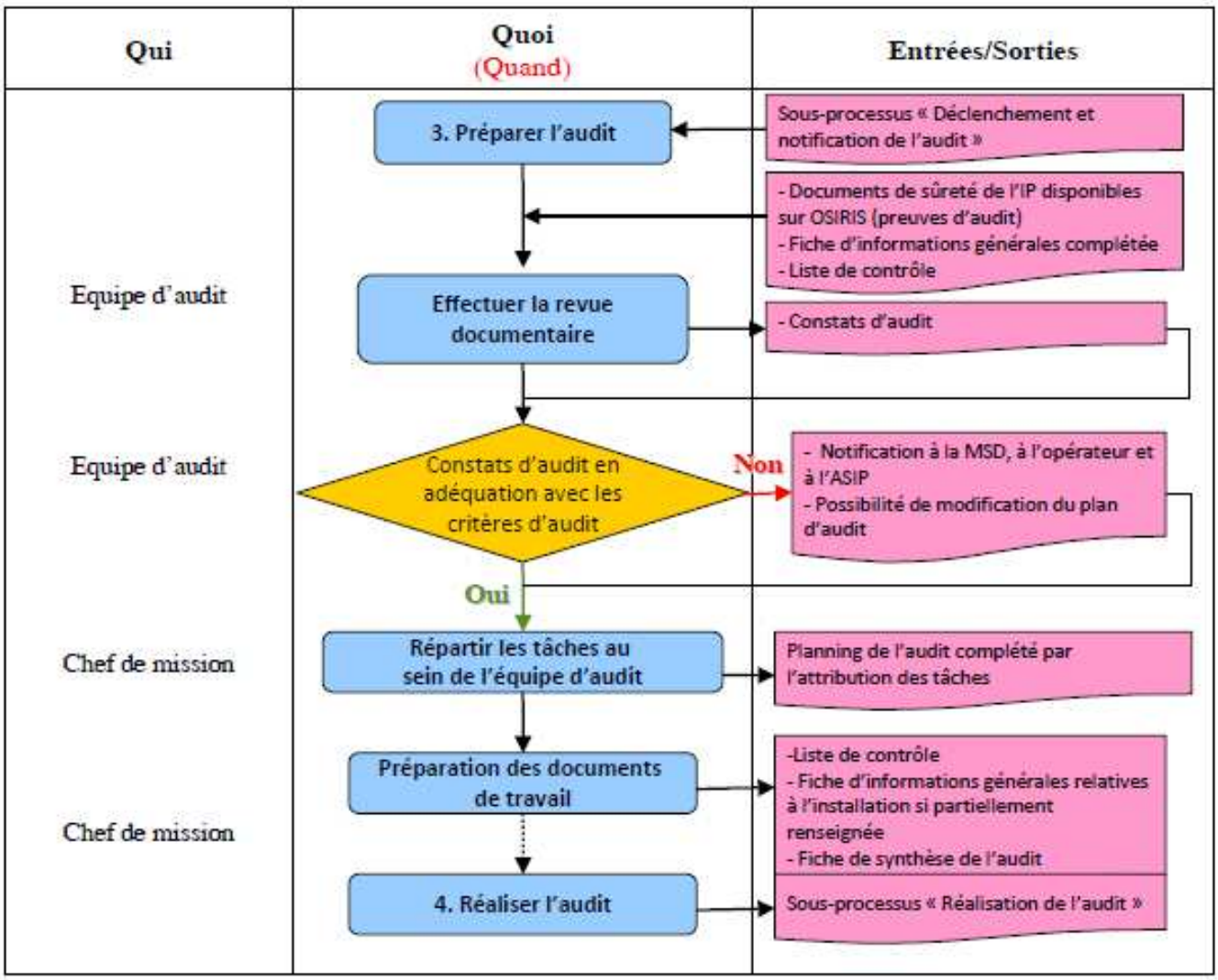

Figure 9 : Logigramme présentant les liens organisationnels entre les activités du sous-processus "Préparation de l'audit"

IX. B. 2) Responsabilités

L'équipe d'audit.

IX. B. 3) Déroulement

- ***Revue documentaire :***

Les membres de l'équipe d'audit effectuent la revue des documents de sûreté recueillis sur OSIRIS (voir partie II. D. du manuel) ou auprès du préfet. Ces documents constituent les premières preuves d'audit recueillies par l'équipe. Les auditeurs devront tenir compte des objectifs et du champ de l'audit définis dans la lettre de notification et vérifier la conformité des documents aux critères d'audit.

Dans le cas d'un audit inopiné, le temps de préparation étant limité, la revue documentaire pourra se limiter uniquement à la revue du plan de sûreté de l'installation.

- ***Préparation d'un échantillonnage prévisionnel et des documents de travail :***

La « Liste de contrôle » et notamment les questionnements peuvent alors être partiellement renseignés par les premiers constats d'audit obtenus lors de la revue des documents et plus précisément du plan de sûreté de l'installation.
En fonction de ces constats, le chef de mission peut commencer à orienter son échantillonnage de preuves d'audit sur site selon les premiers constats qui ne sembleraient pas satisfaire les critères d'audit.
A ce stade, la « Fiche d'informations générales relatives au port ou à l'IP » doit être complétée par l'audité. Si cela n'est pas le cas, les parties qui n'ont pas été renseignées devront l'être le jour de l'audit.
La « Fiche de synthèse de l'audit » peut être partiellement renseignée par le chef de mission.

- ***Contacter l'audité pour l'organisation des activités d'audit sur site :***

L'auditeur temps-plein doit contacter l'audité pour organiser les horaires approximatives des activités d'audit sur site, et cela deux semaines minimum avant l'audit. En effet, si l'auditeur prévoit d'interviewer du personnel présent sur l'installation, l'audité peut souhaiter prendre certaines dispositions pour que les personnes à interviewer soient disponibles.

IX. C. Indicateurs de performance

Un meilleur renseignement de la liste de contrôle implique davantage de preuves d'audit et donc des constats d'audit plus objectifs. L'organisation et l'efficacité lors du sous-processus de préparation permettront de passer moins de temps sur la revue du plan de sûreté de l'installation lors de la réalisation de l'audit sur site et donc de renseigner davantage la liste de contrôle par des preuves d'audit recueillies lors de la visite de l'installation.
Ainsi, pour évaluer la performance de la préparation de l'audit, on pourra regarder si l'auditeur a recueilli un maximum de preuves d'audits.

X. SOUS-PROCESSUS « RÉALISATION DE L'AUDIT »

X. A. Présentation générale du sous-processus « Réalisation de l'audit »

- ✓ Les auditeurs doivent respecter les principes de l'audit (Voir ***V. A. 2)***) dans les différentes phases constituant le sous-processus « réalisation de l'audit ».
- ✓ L'approche lors de la réalisation de l'audit est documentaire (restitution des constats d'audit aux audités et audit des registres de sûreté) mais s'appuie également sur le rapport aux hommes, aux femmes et aux faits.
- ✓ Les preuves d'audit recueillies lors de la visite sur site (étude des registres, observation des faits, entretiens, etc.) devraient converger avec les constats d'audit réalisés lors de la revue documentaire.
- ✓ L'équipe d'audit vérifie si les contre-mesures définies dans l'ESP sont reprises dans le plan de sûreté et appliquées sur site.

X. B. Méthodologie de réalisation de l'audit

X. B. 1) Activités du sous processus « réalisation de l'audit »

Les différentes phases constituant ce sous-processus sont les suivantes (voir Figure 8) :

- Réunion d'ouverture,
- Recueil et vérification des informations,
- Etablissement des constats d'audit et hiérarchisation de ceux-ci,
- Concertation de l'équipe d'audit concernant les constats,
- Réunion de restitution.

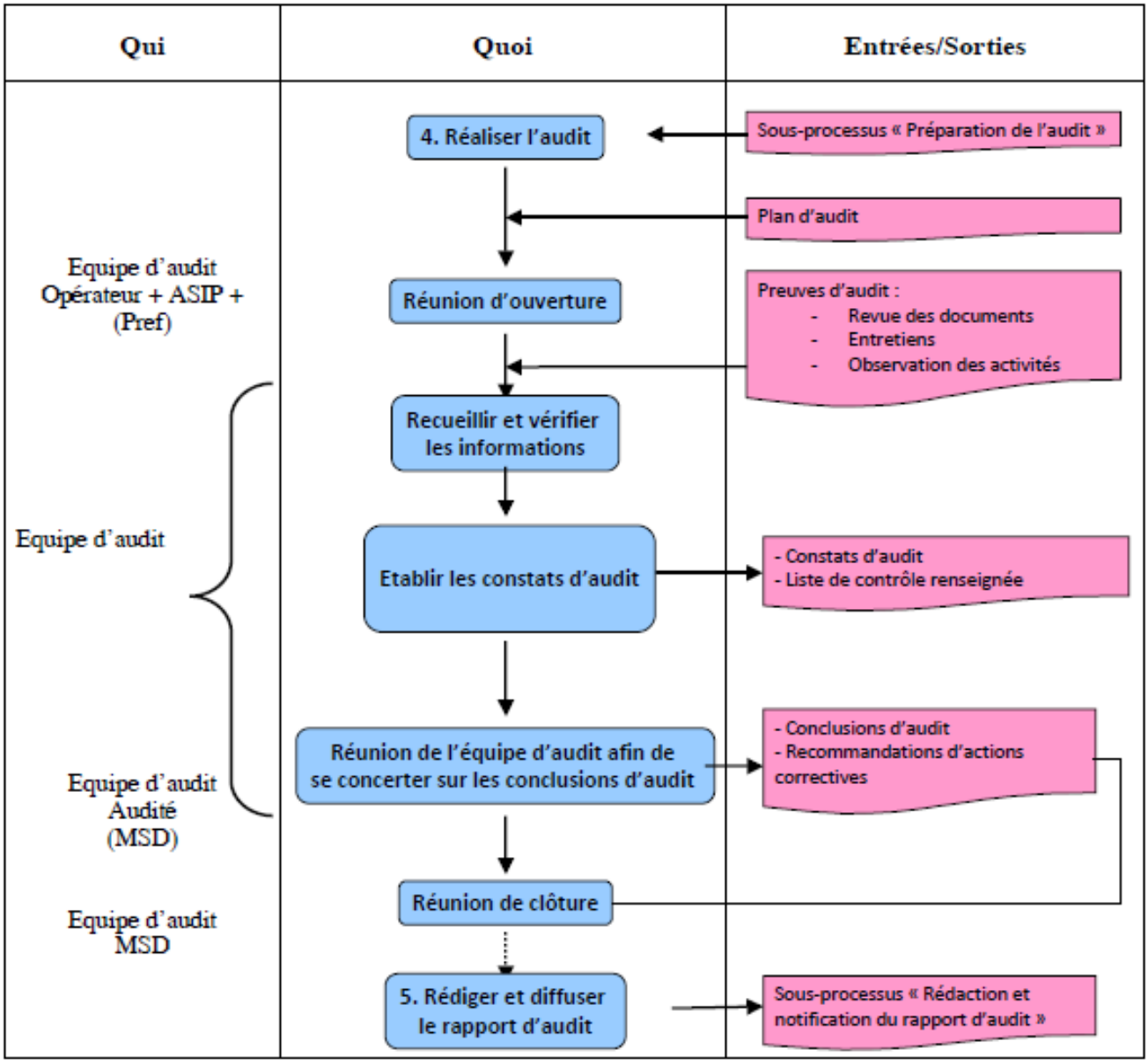

Figure 10 : Logigramme présentant les liens organisationnels entre les activités du sous-processus "Réalisation de l'audit"

X. B. 2) Responsabilités

Tout au long de ce sous-processus, le chef de mission doit mener les activités en veillant à ce que l'échantillonnage préparé soit suivi. Il doit veiller à la bonne avancée des activités d'audit et prendre les décisions concernant la modification inopinée de l'organisation des activités d'audit sur site.

X. B. 3) Réunion d'ouverture

- ***Buts :***

✓ Confirmer les éléments contenus dans le « Plan d'audit » (type d'audit, objectifs et critères de l'audit, champ d'application de l'audit, présentation des membres de l'équipe d'audit, nom et prénoms, programme des activités d'audit sur site) ;

✓ Présenter brièvement la manière dont les activités d'audits seront menées ;

- ✓ Offrir la possibilité à l'audité de poser des questions.

- ***Personnes présentes :***

- ✓ Audités dont l'ASIP (ASP)
- ✓ Auditeurs temps-plein et volontaires ;
- ✓ Présence possible de l'ASP ;
- ✓ Présence possible et recommandée de la préfecture de département ;
- ✓ Présence possible de sous-traitants ;
- ✓ Des observateurs peuvent accompagner l'équipe d'audit mais sans en faire partie. Ces premiers ne doivent exercer aucune influence ou ingérence dans la réalisation de l'audit. Ces observateurs peuvent être nommés par l'audité.

- ***Déroulement :***

Le chef de la mission ouvre la réunion. Il veille à ce que les éléments principaux suivants soient revus succinctement :

- ✓ Eléments notifiés dans la lettre de notification de l'audit ;
- ✓ Méthodes et procédures utilisées pour réaliser l'audit en précisant l'élément d'incertitude que comportent les constats d'audit ;
- ✓ Disponibilité des ressources et de la logistique nécessaire à l'équipe d'audit ;
- ✓ Règles de confidentialité ;
- ✓ Règles de sécurité et procédures d'urgence et de sûreté applicables lors de la visite ;
- ✓ Méthodes de compte-rendu d'audit, dont la hiérarchisation des constats ;
- ✓ Moyens d'intervention, d'appel dans la réalisation ou les conclusions de l'audit.

X. B. 4) Recueil et vérification des informations

- ***Buts :***

Les auditeurs doivent collecter, selon un échantillonnage approprié, des informations et les vérifier afin qu'elles constituent des preuves d'audit solides pour renseigner la liste de contrôle. Ces preuves permettent de mesurer si les points évalués respectent ou non les critères d'audit.

- ***Sources d'informations :***

L'auditeur doit au fur et à mesure de l'audit, renseigner objectivement chaque point à évaluer de la liste de contrôle en recueillant des preuves d'audit de quatre types tels que définis dans la partie *VIII. B. 1)*.

X. B. 5) Etablissement des constats d'audit et hiérarchisation des constats

- ***Buts :***

Etablir des constats d'audit conduisant à un plan d'actions correctives qui permettra une amélioration continue du système de sûreté portuaire ;

- ***Déroulement :***

La formulation des constats d'audit est conduite au fur et à mesure de l'avancement des activités d'audit, du sous-processus « préparation de l'audit » jusqu'au sous-processus « réalisation de l'audit » au cours desquels seront collectées les quatre types de preuves d'audit.

Dans la liste de contrôle, les auditeurs notifient les constats d'audit en face du questionnement correspondant. Les constats relevant des écarts seront exprimés à la forme négative afin de traduire les carences relevées le plus fidèlement possible.

X. B. 6) Concertation de l'équipe d'audit et hiérarchisation des constats d'audit

- ***Buts :***

✓ Se concerter afin de préparer les constats d'audit et leur hiérarchisation avant la réunion de restitution.

✓ Hiérarchiser les constats permettra de prioriser les actions en affectant des délais de mise en œuvre pertinents.

- ***Déroulement :***

Les membres de l'équipe d'audits effectuent principalement la revue des éléments suivants :

✓ Constats d'audit par rapport aux objectifs et critères d'audit ;

✓ Hiérarchisation des constats d'audit (voir tableau 6) ;

✓ Préparation des recommandations d'actions correctives éventuelles ;

✓ Modalités de suivi de l'audit ;

✓ Renseignement de la « Fiche de synthèse de l'audit » quasi final.

- ***Hiérarchisation des constats :***

Les constats n'ayant pas tous la même incidence sur la sûreté de l'installation, il convient de les hiérarchiser selon le tableau 6 ci-après.

Tableau 5 : Hiérarchisation des constats d'audit

Types de constat			Priorité de l'action corrective
Points forts	PF	Bonnes pratiques, qui répondent bien aux exigences de la réglementation et aux mesures spécifiées dans le plan de sûreté approuvé	
Ecarts	Non-respect des exigences réglementaires ou des dispositions du plan de sûreté approuvé. Les exigences en écart sont précisées et hiérarchisées en recommandations et non-conformités comme ci-après :		
Recommandations	REC	Pistes d'amélioration : le critère d'audit est mis en œuvre mais avec des lacunes observées révélant trop peu de pilotage ou de suivi. La recommandation peut concerner un défaut dans la sémantique du plan de sûreté approuvé, reflétant alors mal la pratique.	**3**
Non-conformités	NC	L'écart est avéré. La mise en œuvre du critère d'audit évalué est insuffisante.	**2**
Non-conformités majeures	NC maj	La non-conformité majeure remet en cause à elle-seule la sûreté du système et donc sa viabilité. Elle devra être résolue en priorité, dans les plus	**1**

		brefs délais car elle met en péril la sûreté de l'installation de manière certaine OU immédiate.	

Elément complémentaire de la liste de contrôle, la rubrique « ACTIONS CORRECTIVES SUGGÉRÉES » est un champ où les auditeurs peuvent suggérer, notamment par la discussion avec l'audité, des actions correctives pour lever chaque écart signalé. La priorité des actions correctives est cotée de 1 à 3. Plus cette cotation est faible plus le délai de mise en œuvre de l'action devra être court ou même immédiat si l'écart rencontré engendre un risque grave et imminent pour l'installation. L'exploitant tiendra compte de ces discussions et suggestions pour mettre en place son plan d'actions correctives sur lequel le Préfet statuera en finale.

X. B. 7) Réunion de restitution

- ***Buts :***

✓ Présenter oralement les constats et conclusions de l'audit ;
✓ Recommander des actions correctives aux audités et se mettre d'accord sur les délais de mise en œuvre ;
✓ Discuter de toute opinion divergente entre auditeurs et audités et, si possible, la résoudre.

- ***Personnes présentes :***

✓ Equipe d'audit, dont le chef de mission qui préside la réunion ;
✓ Exploitant ;
✓ ASIP et, dans le cas d'un audit d'installation portuaire, l'ASP, ou l'un de ses suppléants ;
✓ Présence hautement souhaitable de la préfecture de département ;
✓ Observateurs si existants.

- ***Déroulement :***

Le chef de mission fait part oralement à l'audité des constats de l'audit de façon à ce qu'il les comprenne et les accepte. Cette réunion donne globalement la configuration du rapport d'audit.
En évoquant les points critiques et écarts détectés, le chef de mission peut proposer pour chacun les actions correctives et les délais de mises en œuvre qui auront été suggérés lors de la concertation de l'équipe d'audit.
En cas de désaccord entre les auditeurs et les audités, il conviendra de trouver rapidement un terrain d'entente afin de fixer des objectifs spécifiques, mesurables, atteignables, réalistes et définis dans le temps.
Dans le cas où le désaccord ne serait pas résolu, l'équipe d'audit doit enregistrer toutes les opinions.
Le chef de mission doit finir son discours en mettant en avant les points forts qui ont été repérés et en précisant que ces derniers devraient être généralisés.

XI. Sous-Processus « Rédaction et Diffusion du rapport d'audit »

XI. A. Présentation générale du sous-processus « Rédaction et diffusion du rapport d'audit »

L'objectif est de fournir un enregistrement complet, précis, concis et clair de l'audit pour les parties concernées.

XI. B. Méthodologie de rédaction et diffusion du rapport d'audit

XI. B. 1) Responsables

Les membres de l'équipe d'audit rédigent conjointement la fiche d'informations générales relatives à l'installation et la fiche de synthèse de l'audit.
Le chef de mission :

- ✓ Rédige les conclusions de l'audit ;
- ✓ Supervise le rendu final lors de la constitution du dossier « Rapport d'audit » à rendre à la MSD (Voir trame de rapport Annexe 3 du Manuel) ;
- ✓ Prépare la lettre de notification du rapport d'audit.

La DGITM/DST/MSD est responsable de la diffusion du rapport.

XI. B. 2) Activités relatives au sous-processus « Rédaction et diffusion du rapport d'audit »

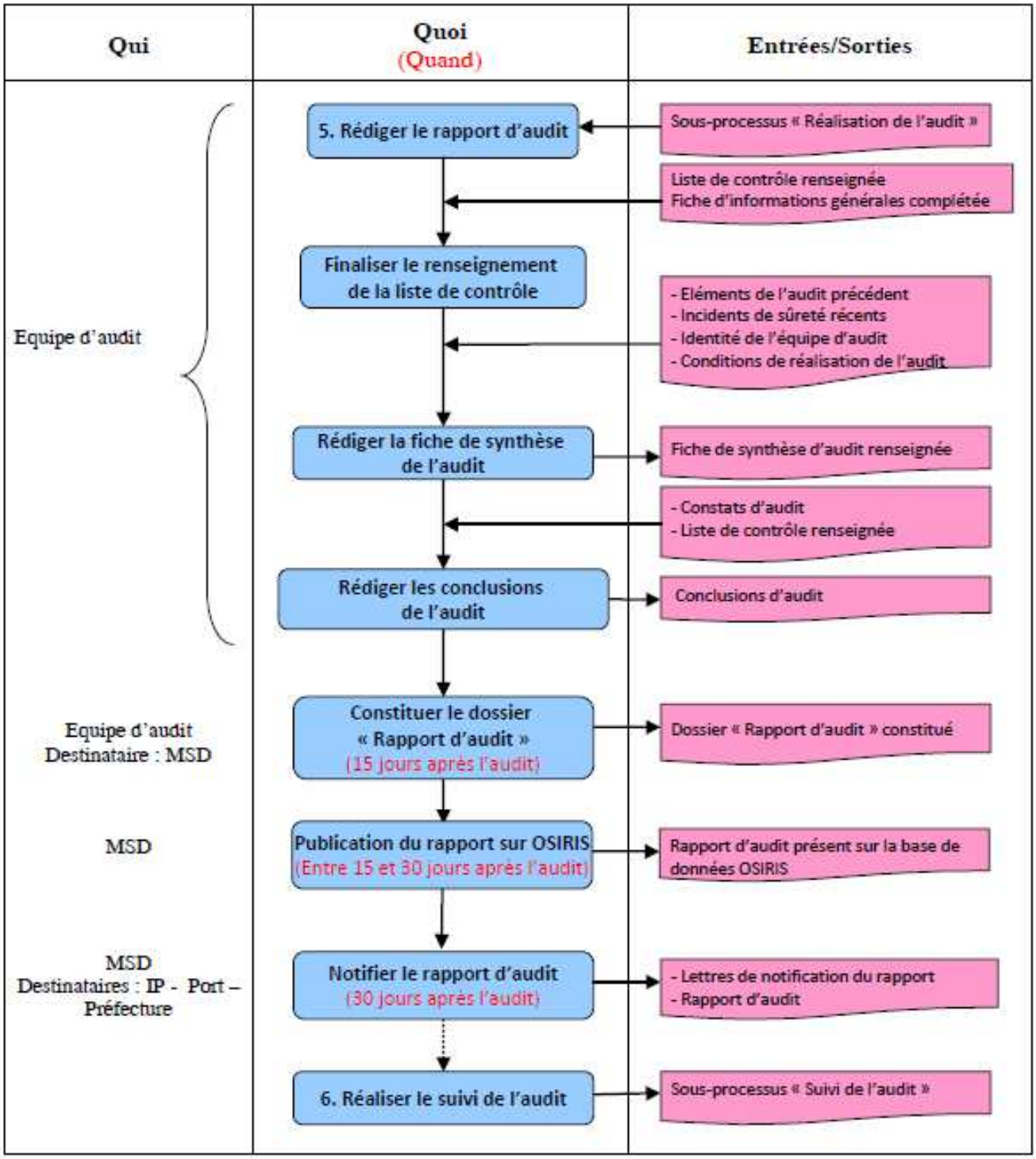

Figure 11 : Logigramme présentant les liens organisationnels entre les activités du sous-processus "Rédaction et diffusion du rapport d'audit"

XI. B. 3) Rédaction du rapport

Afin de fournir un rapport de qualité, les auditeurs devront veiller aux paramètres suivants :

- ✓ clarté,
- ✓ couverture complète du domaine,
- ✓ échéancier réaliste des actions correctives,
- ✓ distinction claire entre les exigences relatives à de réels écarts constatés et les recommandations qui sont des pistes d'amélioration.

Le rapport est constitué de trois parties (Voir Annexe 3) définies ci-après :

I. Fiche d'informations générales relatives à l'installation ;
II. Fiche de synthèse de l'audit ;
III. Conclusions de l'audit.

Les auditeurs s'assurent que la « Fiche d'informations générales sur l'installation » est complète.
Ils finalisent le renseignement de la liste de contrôle si cela n'a pas été fait durant la réalisation de l'audit.
En s'aidant des éléments notifiés dans la lettre de notification de l'audit et des prises de notes réalisées pendant l'audit, les auditeurs peuvent renseigner la « Fiche de synthèse de l'audit » (Voir Annexe 3 du Manuel).
Grâce à la liste de contrôle dûment renseignée et donc aux constats d'audit, le chef de mission rédigent les « Conclusions de l'audit » (Voir Annexe 3 du Manuel).
Le chef de mission doit avoir constitué le rapport d'audit, préparé la lettre de notification du rapport d'audit (des lettres de notification types sont disponibles au sein de la MSD) et envoyé ceux-ci à la MSD dans un délai maximum de 15 jours après l'audit.

XI. B. 4) Diffusion du rapport d'audit

Après avoir effectué les corrections nécessaires au rapport d'audit et à la lettre de notification du rapport préparée reçus, l'autorité compétente valide ces documents et signe la lettre de notification. Elle les envoie aux parties suivantes :

- ✓ Exploitant ;
- ✓ Préfet ;
- ✓ Destinataires en copie : membres de l'équipe d'audit, autorité portuaire.

Les critères de confidentialité précisés dans la partie **IV. B.** doivent être respectés.
Concernant la liste de contrôle renseignée, le chef de mission l'archive pour le prochain audit.

XII. Sous-Processus « Suivi des audits »

XII. A. Présentation générale du sous-processus « Suivi des audits »

Les objectifs de ce sous-processus sont les suivants :

- ✓ Validation par le préfet des actions correctives proposées par l'exploitant pour supprimer les écarts constatés lors de l'audit ;
- ✓ S'assurer que les actions correctives validées ont effectivement été mises en œuvre dans les délais fixés.

XII. B. Méthodologie du sous-processus « Suivi des audits »

XII. B. 1) Responsabilités

- ✓ Préfet de département,
- ✓ DGITM/DST/MSD,
- ✓ Exploitant,
- ✓ Auditeurs temps-plein.

XII. B. 2) Activités relatives au sous-processus « suivi des audits »

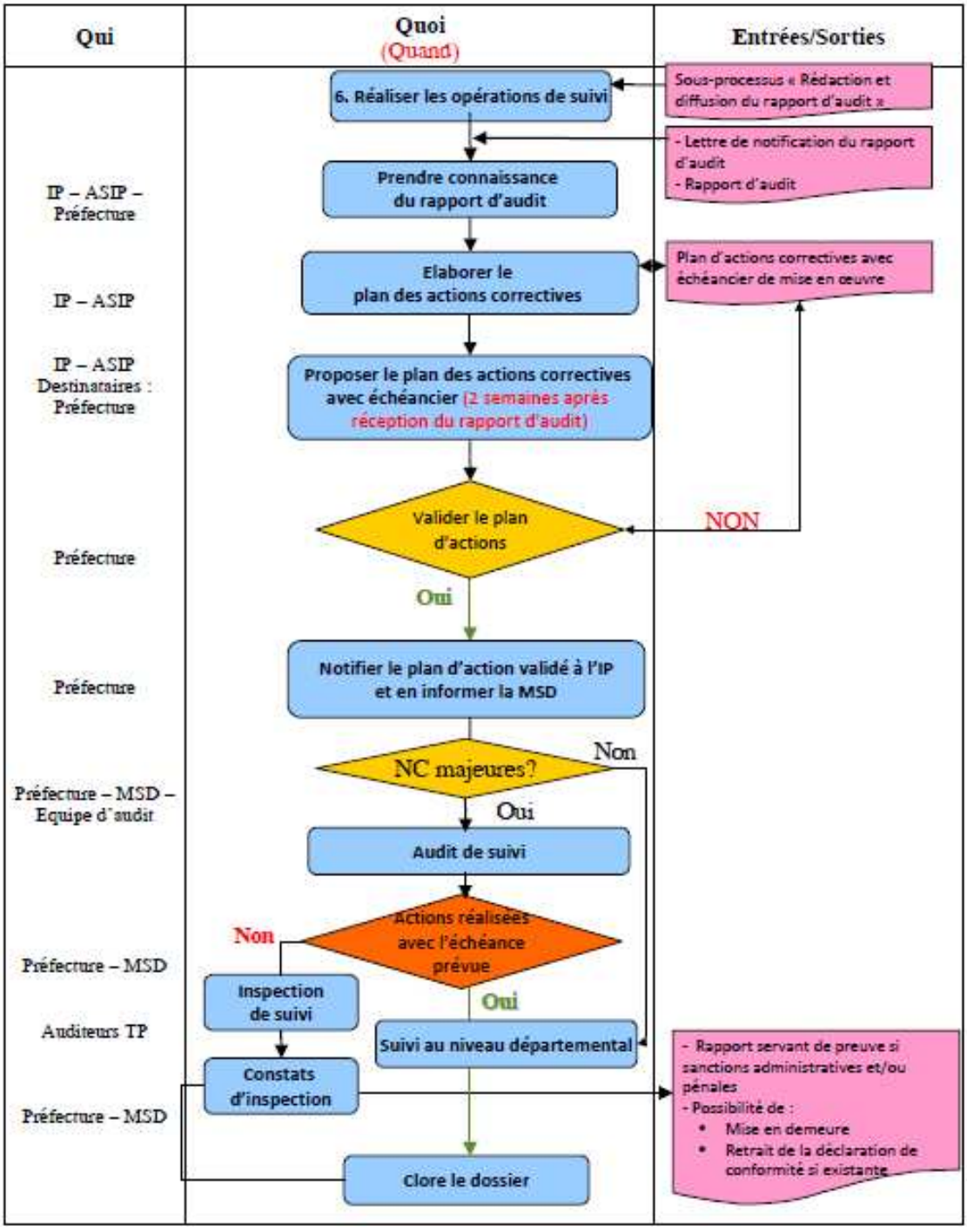

Figure 12 : Logigramme présentant les liens organisationnels entre les activités du sous-processus "Suivi d'audit"

XII. B. 3) Déroulement des activités

Après réception du rapport d'audit, l'exploitant élabore un plan d'actions correctives en tenant compte des recommandations des auditeurs. Il le soumet au préfet deux semaines au plus tard après réception du rapport, bien que des actions correctives relatives à des non-conformités majeures aient pu être mises en place immédiatement après l'audit faute d'un risque accru pour la sûreté de l'installation.
Le préfet de département se charge de valider le plan d'actions et les échéanciers relatifs à chacune. Si ce plan est insatisfaisant, il le renvoie à l'installation en notifiant les causes de l'insatisfaction. Le port ou l'IP propose alors un nouveau plan d'actions.
Une fois le plan d'actions correctives validé par le préfet, ce dernier le diffuse à l'exploitant.
Seront mis en copie l'autorité compétente et le chef de mission de l'audit.

S'il n'y a pas de NC majeure détectée lors de l'audit programmé, il n'y aura pas d'audit de suivi et le préfet devra suivre les actions correctives concernant les autres types d'écarts. L'audit est alors clos pour les auditeurs temps-plein dès lors que le rapport d'audit est envoyé aux destinataires concernés.

En cas de non-conformité majeure détectée lors de l'audit programmé, un audit de suivi devra être réalisé par une équipe d'audit différente de celle de l'audit programmé, afin de vérifier que les actions correctives ont été réalisées dans les délais fixés dans le plan d'actions correctives validé par le préfet.
Les auditeurs temps-plein prévoiront l'audit de suivi selon les critères de programmation définis dans la partie *VI. B. 4)*.
Si lors de l'audit de suivi, les actions correctives concernant les NC majeures ont été résolues, le suivi des actions correctives concernant les autres constats d'audit revient à la préfecture et l'audit est ainsi clos pour les auditeurs temps plein dès lors que le rapport d'audit de suivi est envoyé aux destinataires concernés.

XII. C. Cas particulier : l'inspection de suivi

Si, lors de l'audit de suivi, les actions correctives de non-conformités majeures qui auraient dû être réalisées à la date prévue dans le plan d'actions validé par le préfet n'ont pas été réalisées ou si elles n'ont démontré aucune progression, l'auditeur temps-plein doit notifier à :

- ✓ à l'exploitant que l'installation va être soumise à une inspection de suivi, faute du non-respect du plan d'actions validé par le préfet ;
- ✓ à la MSD et au préfet de département l'occurrence prochaine d'une inspection de suivi. Ceux-ci doivent par la suite missionner des auditeurs assermentés qui se rendront sur l'installation pour y réaliser une inspection de suivi.

Le responsable de l'inspection de suivi est chargé de contrôler si lesdites actions correctives ont été mises en œuvre à la date de l'inspection. Dans le cas où les constats d'inspection révèlent un manquement à cette obligation, le responsable peut :

- ✓ Dresser un procès verbal à l'installation ;
- ✓ Utiliser les constats d'inspection comme fondement à l'élaboration de sanctions administratives décidées par le préfet. D'autres sanctions peuvent être encourues telles que la restriction de mise en œuvre de l'installation ou le retrait de sa déclaration de conformité.

Suite aux décisions prises par le préfet de département au regard des constats d'inspection, le dossier d'audit sera clos par celui-ci.

ANNEXES

ANNEXE 1 – Fiche d'enregistrement des propositions de modifications du Manuel d'audit des systèmes de sûreté des ports et installations portuaires

- **Auteur de la proposition de modification**

Nom et prénom de la personne proposant la modification :	
Fonction de la personne proposant la modification :	

- **Proposition de modification**

- **Description générale de la modification proposée :**

- **Description de la situation d'audit ou tout autre événement qui motive la proposition :**

Date	Lieu de la situation d'audit ou de l'événement (ville, code postal et nom du port ou de l'IP)	Noms/Prénoms des personnes présentes au moment de la constatation	Version du manuel concernée par la modification	Partie du manuel concernée par la dite modification

- **Amendement rédigé de la partie du manuel :**

- **Evaluation des conséquences de la modification (autre que l'objet de la modification) :**

Date et Signature :

- **Approbation ou refus par MSD**

Proposition de modification approuvée (oui ou non)	
Si non, motif du refus	
Date d'approbation ou de refus	
Numéro de la nouvelle version du manuel d'audit	
Partie(s) du manuel modifiée(s)	

Date et Signature :

ANNEXE 2 – Listes de contrôle

Appendice 2.1 – Liste de contrôle à renseigner pour l'audit du système de sûreté d'un port

Critère ***Sous-Critère***	**Mode de preuve**				oui / non	**Constats d'audit**	**Catégorie de constat**	**Affectation du constat**	**Action corrective suggérée**
Questionnement	ESP-PSP	D	V	I					
1. Identification du port									
Le port est-il clairement identifié ?	X								
Le dernier arrêté préfectoral listant la ou les IP du port a-t-il été communiqué par la préfecture à la MSD? Est-il disponible et valide au jour de l'audit?		X							
S'il existe un point d'importance vitale (art. R.1332-4 du Code de la Défense), le PSP le désigne-t-il et fournit-il ses coordonnées (adresse et n° de téléphone) à jour?	X								
2. Eléments administratifs									
2.1 Structure et diffusion du PSP									
Le PSP est-il composé de 2 volumes physiquement dissociés et faisant l'objet d'un régime de diffusion distinct justifié par une liste de diffusion exhaustive pour chacun des 2 volumes?	X								
2.2 Modifications du PSP									
En cas de modifications du PSP postérieures à son approbation par le préfet, les modifications ont-elles été communiquées à la préfecture et les membres de la liste de diffusion du PSP ont-ils bien la version à jour du PSP?	X		X	X					
2.3 Identification des auteurs									
Les auteurs du PSP sont-ils clairement identifiés?	X								

Si le PSP a été réalisé par les membres d'un OSH, l'AM portant habilitation de cet organisme et les arrêtés portant agrément individuel des auteurs du plan sont-ils mentionnés?	X	X							
2.4. Processus d'élaboration et d'approbation du PSP									
Le PSP a-t-il été rédigé en suivant le plan et le contenu donnés en Annexe 3 de l'Arrêté ministériel du 22 avril 2008 définissant les modalités d'établissement des évaluations et des plans de sûreté portuaires et des installations portuaires?	X								
Le CLSP a-t-il émis un avis sur le PSP avant approbation préfectorale?	X	X							
Le PSP est-il formellement approuvé par arrêté préfectoral ?	X	X							
Le PSP est-il valide au jour de l'audit?	X	X							
Une déclaration de conformité du port a-t-elle été délivrée par le préfet?	X	X							
2.5 Identification et coordonnées des personnes responsables en matière de sûreté au sein du port									
L'autorité portuaire est-elle clairement identifiée?	X								
Le PSP comprend-il l'identification du concessionnaire le cas échéant?	X								
Le PSP comprend-il l'identité et les coordonnées (numéro de téléphone, fax, courriel) :									
- de l'ASP et de ses suppléants?	X			X					
- des personnes spécifiquement chargées de tâches de sûreté au sein du port?	X			X					
2.6 Identification et coordonnées des personnes ressources en matière de sûreté									
- des personnes ressources en matière de sûreté (préfecture, forces de police et/ou gendarmerie, affaires maritimes, etc.)?	X			X					
2.7 Identification et coordonnées au niveau de chaque IP									
- de chacun des ASIP du port et de leurs suppléants?	X			X					

3. Evaluation de la sûreté du port (ESP)[14]									
3.1 Elaboration de l'ESP									
L'ESP a-t-elle été réalisée conformément à l'Annexe 1 de l'arrêté ministériel du 22 avril 2008 ?	X	X							
L'ESP précise-t-elle quels sont les auteurs de l'ESP?	X								
Dans le cas où l'ESP a été réalisée par un OSH, les références de l'AM d'habilitation et celles de l'arrêté portant agrément individuel des auteurs de l'ESP sont elles disponibles et valides au moment de la réalisation de l'ESP?	X	X							
Données d'entrée de l'ESP :									
Les données d'entrées de cette évaluation sont-elles : - pertinentes ? - complètes ? - et fiables?	X	X	X						
Une liste des exigences réglementaires et autres est-elle constituée, appliquée et tenue à jour?	X	X							
L'ESP a-t-elle pris en compte le contexte géopolitique du pays dans lequel se trouve le port (problème de corruption, d'enlèvement, d'agression, d'attentat, etc.) ?	X	X							
Le périmètre de l'évaluation a-t-il été précisé (le périmètre de la ZPS, le port dans ses limites administratives et les zones terrestres contigües intéressant les opérations portuaires et toute zone adjacente à la ZPS)?	X	X	X						
L'ESP a-t-elle pris en compte la configuration et la localisation physique du port, son environnement ainsi que ses contraintes opérationnelles ?	X	X	X						
L'ESP décrit-elle l'activité du port ?	X								

[14] L'établissement de l'ESP/ESIP est de la responsabilité du préfet. Il n'y aura donc pas d'écart spécifié au port ou à l'IP mais une interrogation faite à l'encontre du préfet.

L'ESP a-t-elle pris en compte la nature et la valeur des biens "matériels" (équipements et infrastructures) entreposés et des biens "immatériels" détenus (effectifs, savoir-faire, informations confidentielles, brevets, projet de développement, informations à caractère commercial, etc.), qu'ils soient propres au port ou confiés ?	X	X	X	X					
L'ESP a-t-elle pris en compte les pratiques, procédures et moyens matériels existants en matière de sûreté ?	X		X						
La présence d'hommes ou d'équipes clefs dans le port et les responsabilités en matière de sûreté ont-elles été prises en compte?	X		X	X					
Les menaces potentielles sur le port ont-elles été inventoriées?	X	X							
L'ESP comprend-elle formellement un descriptif précisant explicitement les différents intervenants et la méthode utilisée pour son élaboration?	X	X							
Méthode employée :									
A-t-il été établi une procédure/méthode d'évaluation des vulnérabilités?	X	X							
La méthode a-t-elle été appliquée sur l'ensemble du périmètre d'application de l'ESP?	X	X	X						
La méthode est-elle reproductible?	X	X							
Les critères d'évaluation sont-ils pertinents et leur combinaison est-elle fiable?	X	X							
L'évaluation et la hiérarchisation des risques (par définition de l'impact, de la probabilité, et de la vulnérabilité) permettent-elles de prioriser les mesures de sûreté du PSP?	X	X							
3.2 Processus d'approbation de l'ESP									
Le CLSP a-t-il émis un avis sur cette ESP avant approbation par le préfet ?	X	X							
L'arrêté conjoint du préfet de département et du préfet maritime approuvant l'ESP est-il valide au jour de l'audit et disponible au sein du port ? L'ESP et le PSP y font-ils référence?	X	X							

3. 3 Articulation ESP-PSP									
Des objectifs sûreté sont-ils établis ?	X	X		X					
Un programme de management de la sûreté permettant d'atteindre ces objectifs et déclinant les différentes mesures de sûreté à mette en œuvre pour contrer les risques identifiés dans l'ESP est-il établi dans le PSP ?	X	X	X						
Les mesures de sûreté pour faire face aux risques identifiés dans l'ESP sont-elles définies dans le PSP ?									
- port, y compris le plan d'eau ?	X	X	X						
- la ou les IP composant le port?	X	X	X						
- Zone portuaire de Sûreté (art. L.321-1 du CPM)?	X	X	X						
- Zones terrestres contiguës intéressant la sûreté du port?	X	X	X						
- toute zone adjacente à la zone portuaire de sûreté?	X	X	X						
- toute zone adjacente à la zone portuaire de sûreté?	X	X	X						
Les arrêtés préfectoraux suivants sont-ils disponibles au sein du port, valides au jour de l'audit et communiqués à la MSD :									
- Liste des IP composant le port?	X	X							
- Délimitation de la ZPS?	X	X							
4. Organisation générale de la sûreté du port									
4.1 Organisation de l'autorité portuaire en matière de sûreté									
Le PSP comporte-t-il un organigramme détaillant la structure sûreté de l'AP?	X								
L'organigramme est-il diffusé ?		X	X	X					
L'organigramme est-il nominatif, à jour et indique-t-il les délégations en matière de sûreté?	X		X						
Le PSP comprend-il l'identification du concessionnaire le cas échéant?	X								
L'exploitant a-t-il désigné un ASP (correspondant sûreté du concessionnaire) au sein du port et cet ASP possède un certificat encore valide au jour de l'audit?	X	X							

Les missions de cet ASP permettent-elles un suivi du système de sûreté du port?	X			X					
Le PSP précise-t-il les effectifs de l'AP affectés à des tâches de sûreté par fonction (équipes de protection et de gardiennage, etc.), nature des tâches et niveau de sûreté ISPS et ceux-ci sont-il sur le site lors de la visite ?	X		X						
Le PSP précise-t-il les modalités d'astreinte et de permanence?	X	X	X	X					
Le PSP décrit-il les ressources dédiées à la sûreté (locaux, moyens de transmissions) et celles-ci sont-elles effectives sur site ?	X		X						
Ces ressources sont-elles adaptées aux menaces et vulnérabilités identifiées dans l'ESP ?	X		X						
Le PSP décrit-il :									
- les modalités de coordination entre l'ASP, l'AIPPP et les services de l'Etat?	X			X					
- après leur accord, les tâches effectuées dans le port par ces services?	X		X	X					
- les modalités de coordination de l'ASP avec le concessionnaire?	X			X					
- les modalités de communication avec les navires en matière de renseignements de sûreté préalables à l'arrivée (voir circulaire 236 DGITM/MSD du 02 juillet 2008)?	X	X		X					
- les moyens déployés et les prestations assurées par les sous-traitants à chaque niveau de sûreté? Le cahier des charges des sous-traitants comprenant les effectifs et les tâches de sûreté effectuées est-il annexé au PSIP ?	X		X	X					
- la procédure interne de changement de niveau ISPS à réception de la consigne ?	X	X		X					
- les mesures additionnelles nécessaires lors de l'escale d'un navire de croisière?	X	X		X					
Les effectifs sont-ils adaptés aux menaces et vulnérabilités identifiées dans l'ESP ?	X		X						

Les informations "sûreté" sont-elles remontées à la direction du port? Au préfet?	X	X		X					
En cas de désignation de PIV au sein du port, le PSP définit-il les éléments suivants: - l'organisation hiérarchique ? - l'identité du délégué hiérarchique ? - le fonctionnement du PIV ? - l'effectif des personnels travaillant dans le PIV ?	X		X	X					
4.2 Coordination avec les installations portuaires									
Le PSP comprend-il explicitement les modalités de coordination à chaque niveau de sûreté avec les ASIP?	X	X		X					
Le PSP précise-t-il les modalités d'information mutuelle ASP-A-SIP aux niveaux de sûreté 1, puis 2 et 3 ?	X			X					
Le PSP décrit-il les modalités de suivi des échéances des PSIP pendant sa période de validité?	X			X					
Le PSP comprend-il des procédures de coordination des mesures de sûreté entre les exploitants d'IP et l'AP?	X		X	X					
4.3 Articulation avec les autres plans et procédures									
Le PSP comprend-il les modalités d'interaction avec les autres activités faisant l'objet d'une planification (POI, PPI, plan de secours, plan de bouclage, etc.)?	X			X					
4.4 Gestion documentaire et protection du PSP									
Le PSP comporte-il des mesures visant à en assurer sa confidentialité?	X			X					
Le PSP identifie-t-il les personnes ayant accès aux informations de sûreté protégées et les responsables du système de protection ?	X			X					
Des engagements de confidentialité ont-ils été signés par des agents? Le PSP le précise-t-il ?	X	X		X					
Le PSP identifie-t-il les mesures et les moyens de protection des données, des documents, des communications, des informations liées à la sûreté ? Ceux-ci sont-ils adaptés au niveau de confidentialité établi face aux vulnérabilités identifiées ?	X		X	X					
5. Protection des plans d'eau									

Le PSP précise-t-il les modalités de coordination des mesures opérationnelles de protection des plans d'eau entre le préfet de département, le préfet maritime, l'AP, l'AIPPP et les exploitants d'IP?	X			X					
La coordination des services de l'Etat en la matière fait-elle l'objet de l'arrêté conjoint prévu à l'art. R.321-48 du CPM?	X	X		X					
Le PSP comprend-il des mesures de restriction de circulation sur les plans d'eaux en fonction du niveau de sûreté?	X		X	X					
Le PSP comprend-il des procédures et mesures applicables aux navires et bateaux hors champ ISPS (navires de pêche, de plaisance, barges et péniches)?	X		X	X					
6. Accès et circulation dans le port									
6.1 Dispositions prises pour les ZAR et les ZNPL en cas de présence d'un PIV									
Le PSP détaille-t-il :									
- les équipes de protection et de gardiennage employées ?	X		X	X					
- les systèmes d'astreinte et de permanence ?	X	X	X	X					
- les dispositifs de sûreté?	X		X						
- la protection des systèmes de sûreté?	X		X						
6. 2 Inventaire des zones d'accès restreint (ZAR)									
Le PSP fait-il référence à l'arrêté préfectoral créant la ou les ZAR relevant du port?	X	X							
Le PSP comprend-il un plan réaliste faisant apparaître les limites des ZAR, l'emplacement des points d'inspection filtrage (PIF) et les éventuelles séparations en secteurs spécifiques ?	X		X	X					
Le PSP précise-t-il les flux d'entrées dans les ZAR du port et le nombre de titres de circulation délivrés par catégorie définie à l'art. R. 321-34 ?	X		X	X					
Le PSP comporte-t-il un schéma de circulation en ZAR mis en pratique sur le terrain, en particulier pour les ZAR extérieures aux IP et les ZAR situées dans les IP auxquelles elles donnent accès?	X		X	X					

6. 3 Protection et contrôle des accès en ZAR									
Le PSP décrit-t-il :									
- les caractéristiques des clôtures, des dispositifs de fermeture des accès et de tout autre équipement de protection périmétrique ? Sont-ils mis en place sur le terrain et conformes à l'usage prévu (vérification de leur intégrité et de leur continuité) ?	X		X						
- les modalités adoptées pour l'entrée de véhicules en ZAR ?	X		X	X					
- le système informant de l'interdiction de pénétrer en ZAR (panneaux)?	X		X						
- les règles de fonctionnement des différents PIF selon les niveaux ISPS (horaires, effectifs, procédures d'exploitation des équipements, etc.)?	X		X	X					
- les modalités de répartition des contrôles d'accès entre les exploitants des IP et l'autorité portuaire, pour les ZAR d'IP auxquelles une ZAR portuaire donne accès?	X	X	X	X					
- les modalités adoptées pour la surveillance des ZAR pour chaque niveau ISPS (vidéosurveillance, rondes, etc.) ?	X	X	X	X					
- les procédures d'entretien de tout matériel de sûreté et d'inspection filtrage (clôtures incluses) ?	X	X	X	X					
- les procédures appliquées en cas d'incidents de sûreté (accès non autorisé, panne des équipements, etc.)	X	X		X					
Le circuit de vidéosurveillance est-il entièrement opérationnel?			X	X					
La veille vidéo est-elle permanente et attentive?			X	X					
Les lecteurs de badges, clôtures détectrices, dispositifs de communication internes et externes au port (Services de l'Etat) et autres dispositifs de sûreté éventuellement répertoriés dans le PSP sont-ils opérationnels?			X						

Les règles de gestion des clefs sont-elles définies? L'organisation offre-t-elle une garantie sur : - la traçabilité des clefs remises et rendues ? - la protection des réserves de clefs et de badges?	X	X		X					
6. 4 Gestion des titres de circulation									
Le PSP comprend-il des procédures :									
- de délivrance et de restitution des titres de circulation?	X								
- de coordination et la répartition des tâches avec d'autres IP ou avec l'autorité portuaire en cas de mutualisation de la délivrance des titres?	X								
- destinées à protéger les systèmes d'information et les équipements de fabrication des titres de circulation?	X								
Et ces procédures sont-elles effectives sur site et appliquées telles que définies dans le PSP?			X	X					
Les badges sont-ils portés de manière apparente (et par toutes les catégories de personnes présentes sur le site)?			X						
6. 5 Zones non librement accessibles au public (ZNLP hors ZAR)									
Existe-il des ZNLP en dehors des ZAR? Si oui, le PSP comprend-il :									
- un plan réaliste permettant de localiser ces zones et comprenant les points d'accès?	X		X						
- les règles de fonctionnement applicables à ces zones (contrôle d'accès et circulation)?	X		X	X					
- la définition de l'articulation avec les ZAR adjacentes?	X			X					
7. Conduite à tenir en cas d'alerte, d'incident de sûreté avéré ou de sinistre									
Le PSP décrit-il :									
- les moyens de communication et les systèmes d'alerte, tant internes au port (sirènes, interphone, téléphones) qu'externes (forces de l'ordre, préfecture, capitainerie, pompiers)?	X		X	X					

- les mesures prévues à chacun des niveaux de sûreté pour faire face à une menace ou à une atteinte en cours contre la sûreté et pour maintenir les opérations essentielles dans le cas des PIV?	X			X					
Le PSP comprend-il :									
- des exigences précises de notification obligatoire de tous les incidents de sûreté à l'ASP?	X	X		X					
- une procédure d'évacuation?	X			X					
- une procédure permettant d'accueillir un navire faisant l'objet d'une alerte de sûreté (SSAS)?	X			X					
- une procédure applicable en cas de déclenchement du SSAS d'un navire se trouvant hors d'une IP?	X			X					
- des fiches réflexes pour chaque type d'incident : intrusion ; colis ou véhicule suspect ; appel menaçant ; prise d'otage ?	X			X					
Le PSP prévoit-il :									
- la coordination des mesures de sûreté entre l'ASP et l'ASIP en cas d'incident de sûreté survenant sur un navire amarré dans une IP?	X			X					
- les mesures applicables en cas d'intervention d'urgence des services de secours?	X			X					
Des exercices et entraînements sont-ils réalisés afin de mettre en œuvre les procédures de situation d'urgence et le registre de sûreté contient-il l'enregistrement des exercices et entraînements réalisés?	X	X		X					
Le retour d'expérience suite à la réalisation d'exercices et entraînements est-il analysé?	X	X		X					
Les agents de surveillance à l'entrée des ZAR ou des ZNLP ont-ils à leur disposition la partie du PSP comprenant les consignes opérationnelles (chapitre 11 du plan type selon l'arrêté du 22 avril 2008) ?			X	X					
Connaissent-ils la conduite à tenir en cas d'incidents de sûreté (intrusion, colis, ou véhicules suspects, etc.) ?				X					
Le ou les agents responsables de la vidéosurveillance connaissent-ils la conduite en cas d'intrusion ou d'incidents de sûreté?				X					

La personne recevant les appels téléphoniques extérieurs connaît-elle la conduite à tenir en cas d'appel menaçant ?				X					
Le PSP comprend-il les procédures appliquées en cas d'incident de sûreté (accès non autorisé, panne des équipements, etc.)?	X			X					
8. Dispositions visant à réduire la vulnérabilité liée aux personnes									
Le PSP comporte-t-il une procédure visant à sensibiliser le personnel des tiers (clients, fournisseurs)?	X	X		X					
Le PSP comporte-t-il des procédures applicables aux relations avec les prestataires en matière de sûreté?	X			X					
Le PSP comporte-t-il des procédures applicables à l'habilitation (ZAR) et à l'agrément des personnels?	X	X							
9. Audits et contrôles internes, mises à jour du PSP									
Le PSP comprend-il des procédures et une périodicité pour l'entretien, l'étalonnage et la maintenance de tout matériel de sûreté (protection, surveillance, communication) et d'inspection filtrage (clôtures incluses)?	X			X					
Les registres de ces actions d'étalonnage et de maintenance sont-ils complétés et conservés?		X		X					
L'ASP tient-il à jour le registre de sûreté réglementaire, comprenant l'ensemble des évènements relatifs à la sûreté (sensibilisation et formation du personnel, inspections et incidents de sûreté et de suivi des mesures correctives)?		X							
Le PSP comporte-t-il une procédure d'audit interne des mesures de sûreté?	X			X					
Le registre de sûreté contient-il l'enregistrement des inspections et audits internes effectués?		X							
Le PSP comporte-t-il une procédure garantissant la prise en compte de la sûreté dans les aménagements et nouveaux projets d'infrastructures?	X			X					
Le PSP comporte-il une procédure d'analyse de chaque incident de sûreté et de suivi des mesures correctives éventuelles?	X			X					
La traçabilité des actions correctives est-elle garantie par le registre de sûreté ou tout autre document prévu à cet effet?		X							
10. Formation, exercices et entraînements									

Le PSP détaille-t-il les modalités de sensibilisation du personnel en matière de sûreté ? Le personnel de l'exploitant a-t-il reçu une sensibilisation en matière de sûreté conformément aux modalités décrites dans le PSP ?	X			X					
Les obligations de formation initiale et de certification pour les personnels de sûreté par catégorie (ASP, personnes assurant le gardiennage, etc.) sont elles définies dans le PSP et appliquées?	X			X					
Le PSP fait-il référence à un programme d'exercices trimestriels et d'entraînements annuels?	X	X							
Les participations de tout agent à une action de formation ou de sensibilisation à la sûreté ont-elles enregistrées?		X		X					
Les registres de formations, exercices et entraînements réalisés attestent-il que des formations, exercices et entraînements ont été effectuées aux bonnes périodes et catégories de personnes telles que définies dans le PSP ?		X							
Pouvez-vous présenter les supports permettant de réaliser les sensibilisations du personnel aux enjeux de la sûreté et les formations des personnels ayant des tâches liées à la sûreté?		X							
Une organisation est-elle définie et mise en œuvre pour revoir les procédures dont l'exercice a révélé des difficultés de mise en œuvre (retour d'expérience)?	X	X		X					
Les prestataires privés effectuant les visites de sûreté au sens de l'article L. 321-5 sont-ils titulaires du double agrément ?	X	X		X					
11. Information communicables aux personnes chargées d'effectuer les visites de sûreté									
Les informations définies dans la partie 11 du PSP sont-elles celles demandées dans l'annexe 1 de l'arrêté du 22 avril 2008?	X								

Appendice 2. 2 – Liste de contrôle à renseigner pour l'audit du système de sûreté d'une installation portuaire

Critère ***Sous-Critère*** **Questionnement**	**Mode de preuve** ESI P-P-SI P	D	V	I	oui / non	**Constats d'audit**	**Catégorie de constat**	**Affectation du constat**	**Action corrective suggérée**
1. Identification de l'installation portuaire									
L'IP est-elle clairement identifié ?	X								
L'existence de l'installation portuaire a-t-elle été notifiée par la préfecture à la MSD pour communication à l'OMI et à la Commission ?		X							
S'il existe un point d'importance vitale (art. R.1332-4 du Code de la Défense), le PSP le désigne-t-il et fournit-il ses coordonnées (adresse et n°de téléphone) à jour?	X								
2. Eléments administratifs									
2.1 Structure et diffusion du PSIP									
Le PSIP est-il composé de 2 volumes physiquement dissociés et faisant l'objet d'un régime de diffusion distinct justifié par une liste de diffusion exhaustive pour chacun des 2 volumes?	X								
2.2 Modifications du PSIP									
En cas de modifications du PSIP postérieures à son approbation par le préfet, les modifictions ont-elles été communiquées à la préfecture et les membres de la liste de diffusion du PSIP ont-ils bien la version à jour du PSIP?	X		X	X					
2.3 Identification des auteurs									
Les auteurs du PSIP sont-ils clairement identifiés?	X								
Si le PSIP a été réalisé par les membres d'un OSH, l'AM portant habilitation de cet organisme et les arrêtés portant agrément individuel des auteurs du plan sont-ils mentionnés?	X	X							

2.4. Processus d'élaboration et d'approbation du PSIP									
Le PSIP a-t-il été rédigé en suivant le plan et le contenu donnés en Annexe 4 de l'Arrêté ministériel du 22 avril 2008 définissant les modalités d'établissement des évaluations et des plans de sûreté portuaires et des installations portuaires?	X								
Le PSIP est-il formellement approuvé par arrêté préfectoral ?	X	X							
Le PSIP est-il valide au jour de l'audit?	X	X							
Une déclaration de conformité de l'IP a-t-elle été délivrée par le préfet?	X	X							
2.5 Identification et coordonnées des personnes responsables en matière de sûreté									
Le PSIP comprend-il l'identité et les coordonnées (numéro de téléphone, fax, courriel) :									
- de l'ASIP et de ses suppléants?	X			X					
- des personnes spécifiquement chargées de tâches de sûreté au sein de l'IP ?	X			X					
3. Evaluation de la sûreté de l'installation portuaire (ESIP)[14]									
3.1 Elaboration de l'ESIP									
L'ESIP a-t-elle été réalisée conformément à l'Annexe 2 de l'arrêté ministériel du 22 avril 2008 ?	X	X							
L'ESIP précise-t-elle quels sont les auteurs de l'ESIP?	X								
Dans le cas où l'ESIP a été réalisée par un OSH, les références de l'AM d'habilitation et celles de l'arrêté portant agrément individuel des auteurs de l'ESIP sont elles disponibles et valides au moment de la réalisation de l'ESIP?	X	X							
Données d'entrée de l'ESIP :									

[14]L'établissement de l'ESP/ESIP est de la responsabilité du préfet. Il n'y aura donc pas d'écart spécifié au port ou à l'IP mais une interrogation faite à l'encontre du préfet.

Les données d'entrées de cette évaluation sont-elles : - pertinentes ? - complètes ? - et fiables ?	X	X	X						
Une liste des exigences réglementaires et autres est-elle constituée, appliquée et tenue à jour?	X	X							
L'ESIP a-t-elle pris en compte le contexte géopolitique du pays dans lequel se trouve l'IP (problème de corruption, d'enlèvement, d'agression, d'attentat, etc.) ?	X	X							
L'aire géographique à prendre en compte a-t-elle été bien précisée ?	X	X	X						
L'ESIP a-t-elle pris en compte la configuration et la localisation physique de l'IP, son environnement ainsi que ses contraintes opérationnelles ?	X	X	X						
L'ESIP précise-t-il le type d'installation exploitée?	X								
L'ESIP a-t-elle pris en compte la nature et la valeur des biens "matériels" (équipements et infrastructures) entreposés et des biens "immatériels" détenus (effectifs, savoir-faire, informations confidentielles, brevets, projet de développement, informations à caractère commercial, etc.), qu'ils soient propres à l'IP ou confiés à celle-ci ?	X	X	X	X					
L'ESIP a-t-elle pris en compte les pratiques, procédures et moyens matériels existants en matière de sûreté ?	X		X						
La présence d'hommes ou d'équipes clefs dans l'IP et les responsabilités en matière de sûreté ont-elles été prises en compte?	X		X	X					
Les menaces potentielles sur l'installation ont-elles été inventoriées?	X	X							
L'ESIP comprend-elle formellement un descriptif précisant explicitement les différents intervenants et la méthode utilisée pour son élaboration?	X	X							
Méthode employée :									
A-t-il été établi une procédure/méthode d'évaluation des vulnérabilités?	X	X							

La méthode a-t-elle été appliquée sur l'ensemble du périmètre d'application de l'ESIP?	X	X	X						
La méthode est-elle reproductible?	X	X							
Les critères d'évaluation sont-ils pertinents et leur combinaison est-elle fiable?	X	X							
L'évaluation et la hiérarchisation des risques (par définition de l'impact, de la probabilité, et de la vulnérabilité) permettent-elles de prioriser les mesures de sûreté du PSIP?	X	X							
3.2 Processus d'approbation de l'ESIP									
Le CLSP a-t-il émis un avis sur cette ESIP avant approbation par le préfet ?	X	X							
L'arrêté du préfet de département approuvant l'ESIP est-il disponible au sein de l'IP et valide au jour de l'audit? L'ESIP et le PSIP y font-ils référence ?	X	X							
3. 4 Articulation ESIP-PSIP									
Des objectifs sûreté sont-ils établis ?	X	X		X					
Un programme de management de la sûreté permettant d'atteindre ces objectifs et déclinant les différentes mesures de sûreté à mette en œuvre pour contrer les risques identifiés dans l'ESIP est-il établi dans le PSIP ?	X	X	X						
Les mesures de sûreté pour faire face aux risques identifiés dans l'ESIP sont-elles définies dans le PSIP ?	X								
Le périmètre d'application de l'ESIP est-il le même que celui du PSIP ?	X		X						
4. Organisation générale de la sûreté de l'installation portuaire									
4.1 Plans de l'installation portuaire									
Le PSIP comporte-t-il un plan détaillé de l'installation comprenant les dispositifs de protection ?	X		X	X					
4.2 Organisation de l'installation portuaire en matière de sûreté									

Le PSP comporte-t-il un organigramme détaillant la structure sûreté de l'IP?	X								
L'organigramme est-il diffusé ?		X	X	X					
L'organigramme est-il nominatif, à jour et indique-t-il les délégations en matière de sûreté?	X		X						
L'exploitant a-t-il désigné un ASIP et cet ASIP possède-t-il un certificat encore valide au jour de l'audit?	X	X							
Les missions de cet ASIP permettent-elles un suivi du système de sûreté de l'IP?	X			X					
Le PSIP précise-t-il les effectifs de l'exploitant de l'IP affectés à des tâches de sûreté par fonction (équipes de protection et de gardiennage, etc.), nature des tâches et niveau de sûreté ISPS et ceux-ci sont-il sur le site lors de la visite ?	X		X						
Le PSIP précise-t-il les modalités d'astreinte et de permanence?	X	X	X	X					
Le PSIP décrit-il les ressources dédiées à la sûreté (locaux, moyens de transmissions) et celles-ci sont-elles effectives sur site ?	X		X						
Ces ressources sont-elles adaptées aux menaces et vulnérabilités identifiées dans l'ESIP ?	X		X						
Le PSIP décrit-il :									
- les modalités de coordination entre l'ASIP, l'ASP, l'AP, l'AIPPP et les services de l'Etat?	X			X					
- après leur accord, les tâches effectuées dans le port par ces services?	X		X	X					
- les modalités de communication avec les navires en matière de renseignements de sûreté préalables à l'arrivée (voir circulaire 236 DGITM/MSD du 02 juillet 2008)?	X	X		X					
- les moyens déployés et les prestations assurées par les sous-traitants à chaque niveau de sûreté? Le cahier des charges des sous-traitants comprenant les effectifs et les tâches de sûreté effectuées est-il annexé au PSIP ?	X		X	X					
- la procédure interne de changement de niveau ISPS à réception de la consigne ?	X	X		X					

- les mesures additionnelles nécessaires lors de l'escale d'un navire de croisière?	X	X		X					
- une procédure permettant à l'agent de sûreté du navire de confirmer l'identité de toute personne désirant monter à bord?	X		X	X					
Les effectifs sont-ils adaptés aux menaces et vulnérabilités identifiées dans l'ESP ?	X		X						
Les informations "sûreté" sont-elles remontées à l'exploitant? à la direction du port? Au préfet?	X	X		X					
Si l'IP est désignée comme PIV, le PSIP définit-il les éléments suivants: - l'organisation hiérarchique ? - l'identité du délégué pour la défense et la sécurité ? - le fonctionnement du PIV ? - l'effectif des personnels travaillant dans le PIV ?	X		X	X					
4.3 Coordination avec les installations portuaires adjacentes ou ayant un accès commun.									
Le PSIP comprend-il explicitement les modalités de coordination à chaque niveau de sûreté avec les ASIP des IP adjacentes ?	X	X		X					
Le PSIP comprend-il les procédures de coordination au niveau des accès communs entre des ZAR de l'IP desservies depuis la terre?	X		X	X					
4.4 Articulation avec les autres plans et procédures									
Le PSIP comprend-il les modalités d'interaction avec les autres activités faisant l'objet d'une planification (POI, PPI, plan de secours, plan de bouclage, etc.)?	X			X					
4.4 Gestion documentaire et protection du PSIP									
Le PSIP comporte-il des mesures visant à en assurer sa confidentialité?	X								
Le PSIP identifie-t-il les personnes ayant accès aux informations de sûreté protégées et les responsables du système de protection ?	X			X					
Des engagements de confidentialité ont-ils été signés par des agents? Le PSIP le précise-t-il ?	X	X		X					

Le PSIP identifie-t-il les mesures et les moyens de protection des données, des documents, des communications, des informations liées à la sûreté ? Ceux-ci sont-ils adaptés au niveau de confidentialité établi face aux vulnérabilités identifiées ?	X		X	X					
5. Accès et circulation dans l'installation portuaire									
5.1 Dispositions communes aux ZAR et aux ZNPL en cas de présence dans les IP désignées PIV									
Le PSIP détaille-t-il :									
- les équipes de protection et de gardiennage employées ?	X		X	X					
- les systèmes d'astreinte et de permanence ?	X	X	X	X					
- les dispositifs de sûreté?	X		X						
- la protection des systèmes de sûreté?	X		X						
5. 2 Identification et caractéristiques des zones d'accès restreint (ZAR)									
Le PSIP fait-il référence à l'arrêté préfectoral créant la ou les ZAR contenues dans l'IP? Les arrêtés sont disponibles au sein de l'IP?	X	X							
Le PSIP comprend-il un plan réaliste faisant apparaître les limites des ZAR, l'emplacement des points d'inspection filtrage (PIF) et les éventuelles séparations en secteurs spécifiques ?	X		X	X					
Le PSP précise-t-il les flux d'entrées dans les ZAR du port et le nombre de titres de circulation délivrés par catégorie définie à l'art. R. 321-34 ?	X		X	X					
Le PSP comporte-t-il un schéma de circulation en ZAR mis en pratique sur le terrain, en particulier pour les ZAR extérieures aux IP et les ZAR situées dans les IP auxquelles elles donnent accès?	X		X	X					
5. 3 Protection et contrôle des accès en ZAR									
Le PSIP décrit-t-il :									
- les caractéristiques des clôtures, des dispositifs de fermeture des accès et de tout autre équipement de protection périmétrique ? Sont-ils mis en place sur le terrain et conformes à l'usage prévu (vérification de leur intégrité et de leur continuité) ?	X		X						
- les modalités adoptées pour l'entrée de véhicules en ZAR ?	X		X	X					
- le système informant de l'interdiction de pénétrer en ZAR (panneaux)?	X		X						

- les règles de fonctionnement des différents PIF selon les niveaux ISPS (horaires, effectifs, procédures d'exploitation des équipements, etc.)?	X		X	X					
- les modalités de répartition des contrôles d'accès entre les exploitants des IP et l'autorité portuaire, pour les ZAR d'IP auxquelles une ZAR portuaire donne accès?	X	X	X	X					
- les modalités adoptées pour la surveillance des ZAR pour chaque niveau ISPS (vidéosurveillance, rondes, etc.) ?	X	X	X	X					
- les procédures d'entretien de tout matériel de sûreté et d'inspection filtrage (clôtures incluses) ?	X	X	X	X					
- les procédures appliquées en cas d'incidents de sûreté (accès non autorisé, panne des équipements, etc.)	X	X		X					
Le circuit de vidéosurveillance est-il entièrement opérationnel?			X	X					
La veille vidéo est-elle permanente et attentive?			X	X					
Les lecteurs de badges, clôtures détectrices, dispositifs de communication internes et externes au port (Services de l'Etat) et autres dispositifs de sûreté éventuellement répertoriés dans le PSP sont-ils opérationnels?			X						
Les règles de gestion des clefs sont-elles définies? L'organisation offre-t-elle une garantie sur : - la traçabilité des clefs remises et rendues ? - la protection des réserves de clefs et de badges?	X	X		X					
Dans le cas d'une IP à passagers, vérifier la réalité des mesures prévues par le PSIP en effectuant le trajet d'un passager embarquant. Les mesures et procédures de sûreté mises en œuvre sur l'IP permettent-elles de répondre aux menaces et vulnérabilités identifiées ?			X						
Dans le cas d'une IP accueillant des ferries, vérifier la réalité des mesures prévues par le PSIP en effectuant le trajet d'un véhicule embarquant. Les mesures et procédures de sûreté mises en œuvre sur l'IP permettent-elles de répondre aux menaces et vulnérabilités identifiées ?			X						

Dans le cas d'une IP conteneurs ou marchandises diverses, le contrôle des cargaisons sur ste est-il réellement effectué conformément au PSIP ? Les mesures et procédures de sûreté mises en œuvre sur l'IP permettent-elles de répondre aux menaces et vulnérabilités identifiées ?			X						
5. 4 Gestion des titres de circulation									
Le PSP comprend-il des procédures :									
- de délivrance et de restitution des titres de circulation?	X								
- de coordination et la répartition des tâches avec d'autres IP ou avec l'autorité portuaire en cas de mutualisation de la délivrance des titres, le cas échéant ?	X								
- destinées à protéger les systèmes d'information et les équipements de fabrication des titres de circulation?	X								
Et ces procédures sont-elles effectives sur site et appliquées telles que définies dans le PSP?			X	X					
Les badges sont-ils portés de manière apparente (et par toutes les catégories de personnes présentes sur le site)?			X						
5. 5 Zones non librement accessibles									
En l'absence de ZAR, le PSIP décrit-il :									
- les modalités de surveillance de l'IP à chaque niveau de sûreté (rondes, vidéosurveillance)?	X	X	X	X					
- les modalités retenues pour le contrôle des accès à l'IP et le renforcement éventuel lors d'un changement de niveau ?	X		X	X					
- des procédures pour faciliter les congés à terre pour le personnel du navire ou les changements de personnel, de même que l'accès des représentants des services sociaux et des syndicats des gens de mer ?	X	X		X					
En l'absence de ZAR, le PSIP fait-il référence à des mesures destinées à empêcher l'introduction d'armes (ouverture des bagages et des coffres de voiture sur une base volontaire sans fouille, etc.) ?	X		X	X					
Le PSIP comporte-t-il formellement :									

- des procédures de supervision de la livraison des provisions de bord, pour chaque niveau de sûreté ISPS?	X		X	X					
- des mesures visant à protéger l'intégrité des cargaisons ?	X		X						
6. Conduite à tenir en cas d'alerte, d'incident de sûreté avéré ou de sinistre									
Le PSIP décrit-il :									
- les moyens de communication et les systèmes d'alerte, tant internes à l'IP (sirènes, interphone, téléphones) qu'externes (forces de l'ordre, préfecture, capitainerie, pompiers)?	X		X	X					
- les moyens d'alerter les rondes côté mer et les services spécialisés dans la fouille, y compris pour les inspections sous-marines (démineurs, plongeurs, etc.) ?	X		X	X					
- les mesures prévues à chacun des niveaux de sûreté pour faire face à une menace ou à une atteinte en cours contre la sûreté et pour maintenir les opérations essentielles dans le cas des PIV?	X			X					
Le PSIP comprend-il :									
- des exigences précises de notification obligatoire de tous les incidents de sûreté à l'ASIP?	X	X		X					
- une procédure d'évacuation?	X			X					
- une procédure applicable en cas de déclenchement du SSAS d'un navire amarré ?	X			X					
- des fiches réflexes pour chaque type d'incident : intrusion ; colis ou véhicule suspect ; appel menaçant ; prise d'otage (IP passagers) ?	X			X					
Le PSIP prévoit-il :									
- la coordination des mesures de sûreté entre l'ASP et l'ASIP en cas d'incident de sûreté survenant sur un navire amarré dans une IP?	X			X					
- les mesures applicables en cas d'intervention d'urgence des services de secours?	X			X					

Des exercices et entraînements sont-ils réalisés afin de mettre en œuvre les procédures de situation d'urgence et le registre de sûreté contient-il l'enregistrement des exercices et entraînements réalisés?	X	X		X					
Le retour d'expérience suite à la réalisation d'exercices et entraînements est-il analysé?	X	X		X					
Les agents de surveillance à l'entrée des ZAR ou de l'IP ont-ils à leur disposition la partie du PSIP comprenant les consignes opérationnelles (chapitre 10 du plan type selon l'arrêté du 22 avril 2008) ?			X	X					
Connaissent-ils la conduite à tenir en cas d'incidents de sûreté (intrusion, colis, ou véhicules suspects, etc.) ?				X					
Le ou les agents responsables de la vidéosurveillance connaissent-ils la conduite en cas d'intrusion ou d'incidents de sûreté?				X					
La personne recevant les appels téléphoniques extérieurs connaît-elle la conduite à tenir en cas d'appel menaçant ?				X					
Le PSIP comprend-il les procédures appliquées en cas d'incident de sûreté (accès non autorisé, panne des équipements, etc.)?	X			X					
7. Dispositions visant à réduire la vulnérabilité liée aux personnes									
Le PSIP comporte-t-il une procédure visant à sensibiliser le personnel des tiers (clients, fournisseurs)?	X	X		X					
Le PSIP comporte-t-il des procédures applicables aux relations avec les prestataires en matière de sûreté?	X			X					
Le PSIP comporte-t-il des procédures applicables à l'habilitation (ZAR) et à l'agrément des personnels?	X	X							
8. Audits et contrôles internes, mises à jour du PSIP									
Le PSIP comporte-t-il une procédure garantissant la prise en compte de la sûreté dans les aménagements et nouveaux projets d'infrastructures?	X			X					
Le PSIP comprend-il des procédures et une périodicité pour l'entretien, l'étalonnage et la maintenance de tout matériel de sûreté (protection, surveillance, communication) et d'inspection filtrage (clôtures incluses)?	X			X					
Les registres de ces actions d'étalonnage et de maintenance sont-ils complétés et conservés?		X		X					

L'ASIP tient-il à jour le registre de sûreté réglementaire, comprenant l'ensemble des évènements relatifs à la sûreté (sensibilisation et formation du personnel, inspections et incidents de sûreté et de suivi des mesures correctives)?		X							
Le PSIP comporte-t-il une procédure d'audit interne des mesures de sûreté?	X			X					
Le registre de sûreté contient-il l'enregistrement des inspections et audits internes effectués?		X							
Le PSIP comporte-il une procédure d'analyse de chaque incident de sûreté et de suivi des mesures correctives éventuelles?	X			X					
La traçabilité des actions correctives est-elle garantie par le registre de sûreté ou tout autre document prévu à cet effet?		X							
9. Formation, exercices et entraînements									
Le PSIP détaille-t-il les modalités de sensibilisation du personnel de l'exploitant en matière de sûreté ? Le personnel de l'exploitant a-t-il reçu une sensibilisation en matière de sûreté conformément aux modalités décrites dans le PSIP ?	X			X					
Le PSIP détaille-t-il les obligations de formation initiale et de certification pour les personnels de sûreté par catégorie (ASIP, personnes assurant le gardiennage, etc.) et sont-elles appliquées?	X			X					
Le PSIP fait-il référence à un programme d'exercices trimestriels et d'entraînements annuels?	X	X							
Les participations de tout agent à une action de formation ou de sensibilisation à la sûreté ont-elles enregistrées?		X		X					
Les registres de formations, exercices et entraînements réalisés attestent-il que des formations, exercices et entraînements ont été effectuées aux bonnes périodes et catégories de personnes telles que définies dans le PSIP ?		X							
Pouvez-vous présenter les supports permettant de réaliser les sensibilisations du personnel aux enjeux de la sûreté et les formations des personnels ayant des tâches liées à la sûreté?		X							
Une organisation est-elle définie et mise en œuvre pour revoir les procédures dont l'exercice a révélé des difficultés de mise en œuvre (retour d'expérience)?	X	X		X					
Les prestataires privés effectuant les visites de sûreté au sens de l'article L. 321-5 sont-ils titulaires du double agrément ?	X	X		X					

10. Information communicables aux personnes chargées d'effectuer les visites de sûreté									
Les informations définies dans la partie 11 du PSP sont-elles celles demandées dans l'annexe 4 de l'arrêté du 22 avril 2008?	X								

ANNEXE 3 – Constitution du Rapport d'audit

I Fiche d'informations générales relatives au port audité

I. 1) Présentation générale du port audité

Désignation de l'information	Informations concernant le port audité
Type de port (GPM, port autonome, port décentralisé)	
Nom du port	
Indicatif du port selon l'OMI	
Numéro français du port	
Autorité portuaire (AP) Coordonnées	
Représentant de l'AP pour le port (Nom, prénom)	
Le port est-il soumis aux dispositions de la directive 2005/65/CE et des textes pris pour sa transposition? (OUI/NON)	
Le port (ou une partie du port) est-il un point d'importance vitale? (au sens de l'art R1332-4 du Code de la Défense) (oui/non) Si oui, désignation du PIV et coordonnées (adresse et n° de téléphone)	
Concessionnaire	
Responsable sûreté du concessionnaire (Nom, prénom)	
Agent de sûreté du port (ASP) (Nom, prénom)	
Agent(s) de sûreté du port suppléant(s) (Nom(s), prénom(s))	
Effectif (ensemble du personnel)	
Effectif (personnel ayant des tâches relatives à la sûreté dans le port)	
Le port comporte-t-il une ou plusieurs ZAR ? (oui/non)	
Si oui, Date et références de l'arrêté préfectoral de création de la (ou des) ZAR	
Une déclaration de conformité du port a-t-elle été délivrée par le préfet? (oui/non) Si oui, date de délivrance de la déclaration	

I. 2) Caractéristiques spécifiques du port, le cas échéant, y compris le trafic maritime susceptibles de faire augmenter la probabilité d'incidents de sûreté

Caractéristiques	OUI	NON	Commentaires
Navires à passagers (spécifier le ou les types de navires)			
Terminal roulier/conteneurs			
Terminal pétrolier/gazier			
Autres marchandises dangereuses			
Proximité d'une installation militaire			
Autres (préciser)			
Caractéristiques	**Nombre**		**Commentaires**
Nombre moyen de navires visés par la convention SOLAS qui visitent le port chaque année			

I. 3) Présentation générale de l'activité du port

I. 4) Renseignements généraux concernant l'évaluation de sûreté (ESP) et le plan de sûreté du port (PSP) audité

Désignation de l'information	Information concernant l'ESP ou le PSP
Date d'approbation de l'ESP	
Références de l'arrêté préfectoral approuvant l'ESP	
Le CLSP a-t-il émis un avis sur l'ESP ? (oui/non) Si oui, à quelle date ?	
Auteurs de l'ESP (Noms, Prénoms, Fonctions)	
L'ESP a-t-elle été réalisée par un OSH ? (oui/non) (Si oui, nom de l'organisme et coordonnées)	
Références de l'Arrêté Ministériel d'habilitation de l'OSH	
Date de validité de l'ESP	
Date d'approbation du PSP	
Auteurs du PSP (Noms, Prénoms, Fonctions)	
Le PSP a-t-il été réalisé par un OSH ? (oui/non) (Si oui, nom de l'organisme et coordonnées)	
Références de l'Arrêté Ministériel d'habilitation de l'OSH et références de l'arrêté portant agrément individuel des auteurs du PSP	
Le PSP a-t-il fait l'objet de modifications postérieures à son approbation par le préfet? (OUI/NON)	

I. 5) Description géographique du port et de son environnement

I. 5) a) Description générale (dont photo) :

I. 5) b) Infrastructures et superstructures :

I. 5) c) Personnel du port :

I. 5) d) Liste des installations portuaires ISPS appartenant au port audité :

I. 5) e) Liste des installations portuaires non ISPS appartenant au port audité :

I. 5) f) Définition et délimitation des zones d'accès restreint :

I. Fiche d'informations générales relatives à l'installation portuaire auditée

I.1) Présentation générale de l'installation portuaire auditée

Désignation de l'information	Information concernant l'installation auditée
Nom du port où se trouve l'IP	
Autorité portuaire	
Désignation de l'IP	
N° national de l'IP	
Identification OMI	
Nom ou raison sociale de l'exploitant	
Personne chargée des opérations sur l'installation (Nom, prénom)	
L'installation portuaire est-elle un point d'importance vitale? (au sens de l'art R1332-4 du Code de la Défense) (oui/non) Si oui, désignation du PIV et coordonnées (adresse et n° de téléphone)	
Agent de sûreté de l'installation portuaire (ASIP) (Nom, prénom)	
Agent(s) de sûreté de l'installation portuaire suppléant(s) (Nom(s), prénom(s))	
Effectif (ensemble du personnel)	
Effectif (personnel ayant des tâches relatives à la sûreté dans le port)	
L'IP comporte-t-elle une ou plusieurs ZAR ? (oui/non)	
Date et références de l'arrêté préfectoral de création de la (ou des) ZAR	
Une déclaration de conformité a-t-elle été délivrée par le préfet? (oui/non) Si oui, date de délivrance de la déclaration et date de fin de validité	

I.2) Caractéristiques spécifiques de l'installation portuaire, le cas échéant, y compris le trafic maritime susceptibles de faire augmenter la probabilité d'incidents de sûreté

Caractéristiques	OUI	NON	Commentaires
Navires à passagers (spécifier le ou les types de navires)			
Terminal roulier/conteneurs			
Terminal pétrolier/gazier			
Autres marchandises dangereuses			

Proximité d'une installation militaire			
Autres (préciser)			
Caractéristiques	**Nombre**		**Commentaires**
Nombre moyen de navires visés par la convention SOLAS qui visitent l'IP chaque année			

I. 3) Présentation générale de l'activité de l'installation portuaire

I. 4) Renseignements généraux concernant l'évaluation de sûreté (ESIP) et le plan de sûreté de l'installation portuaire (PSIP) auditée

Désignation de l'information	**Information concernant l'ESP ou le PSP**
Date d'approbation de l'ESIP	
Références de l'arrêté préfectoral approuvant l'ESIP	
Le CLSP a-t-il émis un avis sur l'ESIP ? (oui/non) Si oui, à quelle date ?	
Auteurs de l'ESIP (Noms, Prénoms, Fonctions)	
L'ESIP a-t-elle été réalisée par un OSH ? (oui/non) (Si oui, nom de l'organisme et coordonnées)	
Références de l'Arrêté Ministériel d'habilitation de l'OSH	
Date de validité de l'ESIP	
Date d'approbation du PSIP	
Auteurs du PSIP (Noms, Prénoms, Fonctions)	
Le PSIP a-t-il été réalisé par un OSH ? (oui/non) (Si oui, nom de l'organisme et coordonnées)	
Références de l'Arrêté Ministériel d'habilitation de l'OSH et références de l'arrêté portant agrément individuel des auteurs du PSIP	
Le PSIP a-t-il fait l'objet de modifications postérieures à son approbation par le préfet? (OUI/NON)	

II. 5) Description géographique de l'IP et de son environnement

I. 5) a) Description générale (dont photo) :

I. 5) b) Infrastructures et superstructures :

I. 5) c) Personnel de l'installation portuaire :

I. 5) d) Définition et délimitation des zones d'accès restreint :

II. Fiche de synthèse de l'audit

II. 1) Synthèse de l'audit précédent

Date du dernier audit	
Type du dernier audit	
Nombre de non-conformités majeures constatées	
Nombre de non-conformités majeures encore en cours de redressement	
Nombre de non conformités constatées	
Nombre de non conformités encore en cours de redressement	
Nombre de remarques constatées	
Nombre de remarques encore en cours de redressement	

II. 2) Incidents de sûreté récents (au cours des 5 dernières années)

Incident de sûreté	Date où l'incident a eu lieu	Causes	Actions correctives mises en place suite à l'incident

II. 3) Conditions de réalisation de l'audit

II. 3) a) Date de réalisation et lieu

II. 3) b) Equipe d'audit

[Noms, prénoms et fonctions des membres de l'équipe d'audit]

II. 3) c) Critères de l'audit

II. 3) d) Champs d'application de l'audit

II. 3) e) Type d'audit et Objectifs

II. 4) Déroulement de l'audit

II. 4) a) Liste des documents revus lors de la préparation de l'audit

II. 4) b) Réunion d'ouverture

[Liste des Participants (Noms, Prénoms, Fonctions)]
[Sujets abordés]

II. 4) c) Déroulement de la visite sur site

Date Créneau horaire	Items audités

II. 4) d) Réunion de fin d'audit

[Liste des Participants (Noms, Prénoms, Fonctions)]
[Sujets abordés]

II. 5) Liste de diffusion du rapport d'audit

[Liste des personnes ou catégories de personnes auxquelles est envoyé le rapport d'audit]

III. Conclusions de l'audit

III. 1) Constats d'audit

III. 1) a) Eléments administratifs

[Préciser pour chaque écart :
- ✓ La description de celui-ci-ci ;
- ✓ Le texte réglementaire auquel l'écart est constaté ;
- ✓ L'action corrective recommandée et son délai d'application.]

III. 1) b) L'évaluation de la sûreté de l'installation

[Préciser pour chaque écart :
- ✓ La description de celui-ci ;
- ✓ Le texte réglementaire auquel l'écart est constaté ;
- ✓ L'action corrective recommandée et son délai d'application.]

III. 1) c) Le Plan de Sûreté de l'Installation

[Préciser pour chaque écart :
- ✓ La description de celui-ci ;
- ✓ Le texte réglementaire auquel l'écart est constaté ;
- ✓ L'action corrective recommandée et son délai d'application.]

III. 1) d) L'organisation générale de la sûreté de l'installation

[Préciser pour chaque écart :
- ✓ La description de celui-ci ;
- ✓ Le texte réglementaire auquel l'écart est constaté ;
- ✓ L'action corrective recommandée et son délai d'application.]

III. 1) e) Accès et surveillance de l'installation

[Préciser pour chaque écart :
- ✓ La description de celui-ci ;
- ✓ Le texte réglementaire auquel l'écart est constaté ;
- ✓ L'action corrective recommandée et son délai d'application.]

III. 1) f) Procédure de réponse à une menace ou à un incident de sûreté avéré

[Préciser pour chaque écart :
- ✓ La description de celui-ci ;
- ✓ Le texte réglementaire auquel l'écart est constaté ;
- ✓ L'action corrective recommandée et son délai d'application.]

III. 1) g) Audit, contrôle interne et revue périodique du plan

[Préciser pour chaque écart :
- ✓ La description de celui-ci ;
- ✓ Le texte réglementaire auquel l'écart est constaté ;
- ✓ L'action corrective recommandée et son délai d'application.]

III. 1) h) Formation du personnel – Exercices et entraînements

[Préciser pour chaque écart :
- ✓ La description de celui-ci ;

- ✓ Le texte réglementaire auquel l'écart est constaté ;
- ✓ L'action corrective recommandée et son délai d'application.]

III. 2. Conclusions de l'audit

[Conclusions de l'audit rédigées par le chef de mission de l'audit]