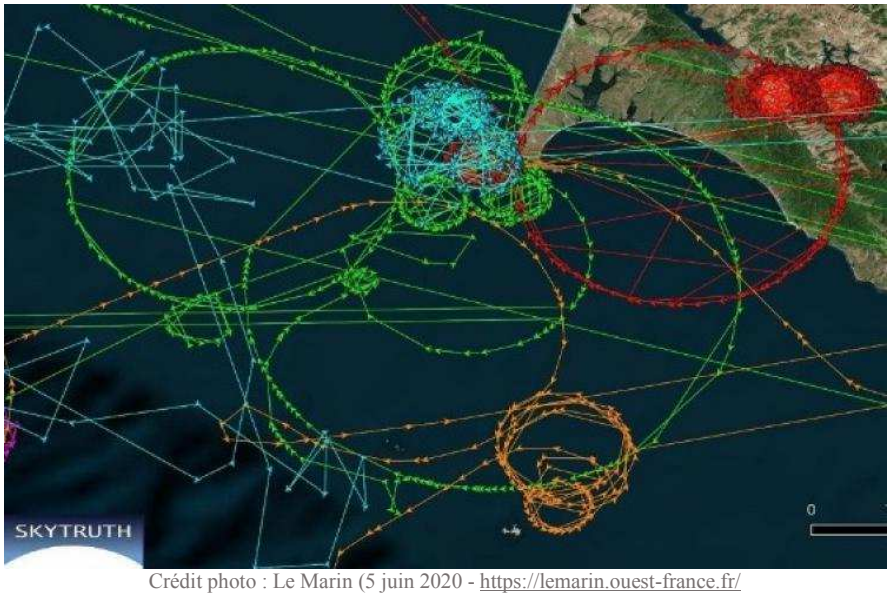
Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

MINISTÈRE DE LA TRANSITION ÉCOLOGIQUE ET SOLIDAIRE

Direction générale des infrastructures, des transports et de la mer

CYBERSÉCURITÉ DES NAVIRES

RECOMMANDATIONS DESTINÉES AUX COMPAGNIES MARITIMES POUR L'INTÉGRATION DE LA CYBERSÉCURITÉ DANS LES SYSTÈMES DE GESTION DE LA SÉCURITÉ



Crédit photo : Le Marin (5 juin 2020 - https://lemarin.ouest-france.fr/

SOMMAIRE

I. INTRODUCTION

I.1. Contexte et position du problème

La résolution MSC.428(98) adoptée le 16 juin 2017 préconise l'intégration des cyber-risques maritimes dans les systèmes de gestion de la sécurité gérés dans le cadre des dispositions du Code ISM. La résolution précise qu'il s'agira de s'assurer que ces risques sont pris en compte au plus tard à la date de la première vérification annuelle du document de conformité délivré à la compagnie après le 1er janvier 2021.

Les termes de cette résolution créent deux ensembles de responsabilités nouvelles :

1. Pour les armateurs : mettre en place les dispositifs et mesures aptes à traiter convenablement les cyber-risques et les intégrer de manière appropriée dans leurs systèmes de gestion de la sécurité ;

2. Pour les administrations – et pour les sociétés de classification habilitées le cas échéant : établir un référentiel pertinent pour l'évaluation de la conformité des dispositions établies par les armateurs et déterminer le cadre et les méthodes à appliquer par les inspecteurs chargés des évaluations.

I.2. Objectifs du guide

Décrire les principes généraux et établir le référentiel qui servira de base pour la prise en compte par les compagnies maritimes de la cybersécurité dans les manuels de gestion de la sécurité (en référence au code ISM).

I.3. Domaine d'application

La résolution MSC.428(98) est adossée au Code ISM. Elle s'applique donc à toutes les compagnies maritimes exploitant des navires relevant des dispositions de ce Code.

Note 1 : il importe donc de noter que le domaine d'application de cette résolution est bien celui des navires relevant du Code ISM et non celui, plus restreint, de l'ISPS.

I.4. Textes de référence pour l'établissement des recommandations

La rédaction de ce guide s'appuie sur deux types de textes :

1. Textes juridiques applicables à tous les navires concernés

Conventions internationales

- Convention internationale pour la sauvegarde de la vie humaine en mer (SOLAS 1974) ;
- Code international de gestion de la sécurité (ISM)

Circulaires de l'OMI

- Circulaire MSC-FAL.1/Circ.3 du 5 juillet 2017 : Directives sur la gestion des cyber risques maritimes
- Résolution MSC.428(98) du 16 juin 2017

2. Documents utilisés comme sources mais non prescriptifs en général

Textes nationaux

- Arrêté du 14 septembre 2018, pris en application de l'article 10 du décret n° 2018-384 du 23 mai 2018 (règles de cybersécurité des opérateurs de services essentiels)

Note 2 : Cette référence, qui ne vaut comme obligation au sens strict que pour les opérateurs de services essentiels (OSE) au sens de la directive NIS, est donnée à titre indicatif. Toutefois, elle est utile pour connaître les principes essentiels de mise en place de la cybersécurité (voir ci-après)

Guides et recommandations

Documentation éditée par l'ANSSI

- Maîtrise du risque numérique – L'atout confiance (https://www.ssi.gouv.fr/administration/guide/maitrise-du-risque-numerique-latout-confiance/
- De manière générale, le site de l'ANSSI comporte nombre de guides et de recommandations utiles aux opérateurs

Guides publiés par la Direction des affaires maritimes du MTES

- Guide 1 - Cybersécurité Évaluer et protéger le navire
- Guide 2 - Cybersécurité - Renforcer la protection des systèmes industriels du navire
- Guide 3 - Guide des bonnes pratiques de sécurité informatique à bord des navires https://www.ecologique-solidaire.gouv.fr/surete-maritime]
- Guide 4 – Recommandations pour le signalement d'incidents de cybersécurité – guide destiné aux armateurs exploitant des navires sous pavillon français (diffusé en juillet 2019).

Guides publiés par les sociétés de classification

- Recommandations publiées par l'Association international des sociétés de classification (IACS) (http://www.iacs.org.uk/news/12-iacs-recommendations-on-cyber-safety-mark-step-change-in-delivery-of-cyber-resilient-ships/)
- Rules on Cyber Security for the Classification of Marine Units - NR 659 DT R00 [section Cyber managed] – Bureau Veritas

Guides publiés par les opérateurs

- The Guidelines on Cyber Security Onboard Ships (v3)- BIMCO, CLIA, ICS, INTERCARGO, INTERMANAGER, INTERTANKO, IUMI, OCIMF and WORLD SHIPPING COUNCIL

Documentation de normalisation

- Management du risque : une approche stratégique, AFNOR édition, 2018
- Norme ISO/IEC 27000:2018 : Technologies de l'information — Techniques de sécurité — Systèmes de management de la sécurité de l'information — Vue d'ensemble et vocabulaire

Note 3 : Le tableau figurant en **annexe I** met en correspondance plusieurs de ces sources de référence pour la mise en place de la cybersécurité des navires. Il pourra être utilement consulté pour trouver la référence utile dans les documents cités pour chaque aspect important de la cybersécurité des navires.

II. RAPPEL DES OBJECTIFS DU CODE ISM

II.1. Objectifs du Code

La traduction des objectifs de cybersécurité dans le code ISM doit s'articuler avec les objectifs généraux de ce code, énoncés dans son paragraphe 1.2, et notamment :

Pour la compagnie :

1. évaluer tous les risques identifiés pour ses navires, son personnel et l'environnement et établir des mesures de sécurité appropriées ; et
2. améliorer constamment les compétences du personnel à terre et à bord des navires en matière de gestion de la sécurité, et notamment préparer ce personnel aux situations d'urgence (…).

Pour le système de gestion de la sécurité :

1. que les règles et règlements obligatoires soient observés ; et
2. que les recueils de règles, codes, directives et normes applicables, recommandés par l'Organisation, les Administrations, les sociétés de classification et les organismes du secteur maritime soient pris en considération.

II.2. Démarche générale

La mise en place de mesures de cybersécurité pourra s'appuyer sur le principe bien connu de la roue de DEMING. Ce principe est général et appliqué dans de nombreux domaines. Il est à la base de toute politique de gestion de la sécurité.

Quatre étapes le composent :

1. Préparer : définition des objectifs, de la planification
2. Mettre en œuvre : appliquer les principes définis dans la phase de préparation
3. Contrôler : vérifier que les actions atteignent leurs objectifs
4. Ajuster : en fonction des résultats obtenus à l'étape 3, reprendre l'étape 1 et corriger l'ensemble du dispositif

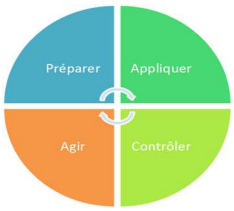


Figure 1 : roue de Deming

La démarche globale de mise en place de dispositions visant à traiter le risque, quel que soit le domaine – ici la cybersécurité mais ces principes sont inchangés pour le traitement des risques physiques, qu'ils soient accidentels ou volontaires – repose sur trois axes-clés :

1. Mesurer les risques
2. Mettre en place un dispositif de prévention adapté
3. Se préparer à réagir

En outre, une politique globale de la compagnie, conçue pour répondre efficacement selon ces trois axes aux risques identifiés, doit nécessairement inclure trois types de composantes :

1. Organisationnelles (ex. politique de la compagnie, définition des rôles à bord)
2. Techniques et opérationnelles (ex. mesures de prévention, hygiène informatique, formation, exercices)
3. Humaines (ex. sensibilisation, formation)

Autrement dit, l'objectif ne peut être atteint que par la combinaison judicieuse de règles d'organisation, de moyens techniques et opérationnels et de moyens humains.

Le chapitre suivant expose comment ces principes généraux vont être appliqués pour mettre en place une politique de cybersécurité du navire.

Note 4: Pour un exposé simple et didactique des principes de mise en place d'une politique de gestion du risque numérique, on pourra consulter utilement le guide coédité par l'ANSSI et l'AMRAE[1]: Maîtrise du risque numérique – L'atout confiance (https://www.ssi.gouv.fr/administration/guide/maitrise-du-risque-numerique-latout-confiance/).
Les principes et règles qui sont exposées dans la suite du document sont en cohérence avec ceux décrits dans ce guide.

III. PRINCIPES DE VERIFICATION DE CONFORMITE PAR L'ADMINISTRATION

La vérification de la conformité des compagnies maritimes aux obligations nées de la Résolution MSC.428(98) du 16 juin 2017 se fait selon les mêmes modalités générales que celles qui s'appliquent à la fois à l'émission du document de conformité de la compagnie et à la délivrance du certificat ISM pour chaque navire. Seul diffère le contenu des vérifications, qui s'appuie sur les recommandations présentées dans le présent document et en particulier sur le tableau figurant en **annexe II**.

La vérification de la prise en compte adéquate de la cybersécurité dans le système de gestion de la sécurité de la compagnie (SMS) se fait dans le cadre général de la certification ISM de la compagnie et des navires qu'elle exploite. Cette vérification sera conduite à la fois lors des audits de siège et des audits de navires, en suivant les mêmes méthodes, à savoir :

- Des vérifications documentaires : consultation des documents de politique générale de cybersécurité, gestion et contrôle des procédures, journaux d'incidents, suivi des actions correctives, etc.;
- Des entretiens avec les personnes désignées au sein de la compagnie et des équipages, ainsi qu'avec des membres d'équipage pour s'assurer de leur connaissance des risques et des procédures de la compagnie ;

[1] Association pour le Management des Risques et des Assurances de l'Entreprise

- Des vérifications techniques plus détaillées si besoin.

Le cadre général de la certification ISM s'applique en totalité au cas particulier de la cybersécurité.

IV. LES OBJECTIFS ESSENTIELS DE LA CYBERSECURITE

La prise en compte de la cybersécurité dans le système de gestion de la sécurité des compagnies consiste à appliquer les principes décrits précédemment à la sécurité des systèmes d'information et aux données qu'ils traitent. Il s'agit de répondre aux objectifs essentiels décrits ci-après.

De manière générale, une politique de cybersécurité, quelle que soit la taille ou la complexité des systèmes d'information à protéger, comprendra toujours quatre grandes composantes :

1. **Gouvernance (politique de cybersécurité)**
2. **Protection des réseaux et des systèmes d'information**
3. **Détection et gestion des incidents**
4. **Gestion de crise**

Note 5: Il s'agit d'une traduction, sous forme simplifiée, des objectifs assignés aux opérateurs de service essentiels, tels que décrits dans l'arrêté du 14 septembre 2018, pris en application de l'article 10 du décret n° 2018-384 du 23 mai 2018, textes pris dans le cadre de la transposition par la France de la directive NIS. Ce texte définit les principes essentiels de la cybersécurité que tout opérateur devrait mettre en application, à travers une série de règles que l'on peut regrouper comme suit :

1. Règles de gouvernance (politique de cybersécurité)
2. Règles de protection des réseaux et des systèmes d'information
3. Règles de défense des réseaux et des systèmes d'information
4. Règles de résilience des activités

A travers ces quatre composantes, on s'assure de répondre aux objectifs énoncés au point 3.5 de la circulaire MSC-FAL.1/Circ.3 du 5 juillet 2017 : *Directives sur la gestion des cyber risques maritimes,* à savoir :

1. L'identification des systèmes à protéger et de l'organisation à instaurer
2. La protection des systèmes face aux menaces
3. La détection des incidents
4. La réponse aux incidents
5. Le rétablissement de l'activité

V. LES QUATRE COMPOSANTES DU DISPOSITIF A METTRE EN PLACE

REGLES DE GOUVERNANCE

Avant toute mise en place de moyens techniques de protection, la cybersécurité repose sur deux piliers essentiels :

1. **L'analyse du risque** ; et
2. **Une politique générale de la compagnie**, définissant les responsabilités et les fonctions liées à la cybersécurité.

ANALYSE DU RISQUE

1ère étape : analyse des menaces :

Pour évaluer le risque, il s'agit d'abord de savoir à quelles menaces les systèmes sont exposés. En matière de cybersécurité, on se trouve au croisement de deux sources possibles : les menaces involontaires (ou accidentelles, résultant par exemple d'erreurs ou de mauvais usages des systèmes) et les menaces intentionnelles – on parlera alors de cyberattaques. Précisions que le terme de cyberattaques déborde celui des attaques via internet (infection par un virus présent sur un site malveillant par exemple). On y inclura les attaques portées par tout vecteur comme par exemple via une clé USB infectée, voire les attaques physiques contre les systèmes (destruction physique d'un serveur ou de supports de données par exemple).

Dans le cas des attaques malveillantes, la gravité de la menace se caractérise par la conjonction de trois critères :

1. L'intention : volonté d'une personne ou d'un groupe de personnes de mener une attaque
2. La capacité technique : moyens et compétences des attaquants pour mener leur action
3. Les conséquences potentielles (appelé aussi impact) : résultat d'une attaque réussie sur le fonctionnement du(es) système(s) et sur les fonctions qu'ils remplissent pour le navire

La menace se caractérise par la conjonction simultanée de ces trois critères. Ainsi, une forte motivation dépourvue de moyens techniques de réalisation est impuissante et ne représente pas de risque. A l'opposé, une grande capacité potentielle en l'absence de motivation est inoffensive.
La menace est extérieure à la cible. Elle doit être estimée aussi précisément que possible, mais on ne peut agir dessus.

Note 6: L'analyse de la menace, dans le cas de la cybersécurité, suppose des connaissances techniques très précises et une veille experte, compétences dont ne disposent pas, en principe, les compagnies maritimes[2]. En effet, une chose est de s'informer auprès des autorités compétentes du risque de piraterie, par exemple, dans une certaine zone de navigation, une autre serait de se tenir à jour de manière permanente des nouvelles attaques pouvant viser un système d'exploitation. L'analyse des points 1 et 2 excède les compétences que l'on peut attendre d'une compagnie maritime.

Toutefois, on conserve comme absolument nécessaire l'analyse par la compagnie des conséquences possibles (point 3) d'une attaque réussie sur chacun des systèmes pris en compte. Cette analyse s'inscrit pleinement dans les compétences de la compagnie qui connait les systèmes qui équipent ses navires.

D'autre part, sans nécessairement disposer d'une connaissance détaillée des différentes méthodes d'attaque, il demeure essentiel que l'opérateur travaille à partir de scénarios de référence – considérés comme les plus graves vis-à-vis des conséquences possibles sur le navire – pour déterminer son degré de vulnérabilité (voir ci-après).

Note 7: Un panorama – non exhaustif – des différents types de menaces est donné à titre d'information en page 10 du guide BIMCO ; on trouve un exposé plus détaillé sur le site de l'ANSSI : https://www.ssi.gouv.fr/entreprise/principales-menaces/

2ème étape : analyse des vulnérabilités

Les vulnérabilités sont par définition les **failles intrinsèques des systèmes**. Chacune d'elle représente un risque potentiel en tant que porte ouverte pouvant faciliter une attaque. Exemple : un port (informatique) non sécurisé, un logiciel insuffisamment mis à jour, une passerelle entre un réseau protégé et un réseau non protégé, une politique de mot de passe laxiste, etc.
L'accroissement des vulnérabilités du secteur maritime est corrélatif de l'accroissement de la part de numérisation des activités, qu'il s'agisse des systèmes de navigation ou d'exploitation, des systèmes commerciaux mais aussi de l'augmentation des communications entre navire et services à terre : services portuaires, gestion commerciale de la compagnie, télémaintenance, etc. De ceci résulte l'augmentation toujours croissante de ce qu'on appelle la « surface d'attaque ou surface d'exposition», c'est-à-dire les possibilités d'accéder aux fonctions essentielles du navire pour les perturber ou les endommager.

L'analyse des vulnérabilités comporte deux étapes :

1. **L'inventaire des systèmes à inclure dans l'analyse**
2. **L'identification des vulnérabilités proprement dites, incluant la connaissance des mesures de protection déjà en place au moment de l'analyse**

Pour l'étape 1 :

Il s'agit d'abord de connaitre précisément les systèmes du navire et les données qu'ils traitent, pertinents pour l'analyse du risque. En général, il s'agira notamment – mais la liste n'est pas exhaustive et doit être précisée individuellement (voir point 2.1.1 de la circulaire MSC-FAL.1/Circ.3) :

- Les systèmes de passerelle et notamment ceux concernant la navigation (GNSS, ECDIS, AIS, système de positionnement dynamique, etc.), ainsi que le traitement des signaux radar ;

[2] Toutefois, les compagnies qui ont (ou auront) le statut d'OSE seront dans l'obligation de mener une analyse de risques cyber complète. Elles pourront à cette fin se faire aider par une société de conseil mais devront évaluer leurs risques résiduels et les accepter (principe de l'homologation).

- Les systèmes liés à la gestion, au chargement et au contrôle de la cargaison, notamment dans leurs interfaces avec les systèmes portuaires ; les systèmes de suivi des conteneurs via internet sont notamment à considérer avec attention ;
- Les systèmes de gestion de la propulsion et des machines et les systèmes de contrôle de l'énergie ;
- Les systèmes de contrôle de l'accès;
- Les systèmes de service aux passagers et de gestion des passagers;
- Les réseaux publics destinés aux passagers;
- Les systèmes administratifs et systèmes récréatifs des membres d'équipage; et
- Les systèmes de communication.

Cette analyse relève entièrement de la compétence de la compagnie qui exploite le navire, seule habilitée à connaître ses systèmes et surtout les conséquences possibles d'une défaillance.

Note 8: Sur la manière de réaliser un inventaire efficace des systèmes, on pourra consulter utilement la recommandation de l'IACS : *Inventory List of computer based systems – Rec.161-Septembre 2018 (http://www.iacs.org.uk/media/5324/rec-161-new-sep-2018.pdf)*

Note 9: **L'importance particulière des systèmes industriels**

Les navires de commerce comportent tous des systèmes industriels pilotés par des automates régissant la propulsion, la sécurité et les opérations commerciales du navire. Or ces systèmes industriels sont désormais connectés à des systèmes d'information et cette interconnexion croissante engendre de nouveaux risques, portant sur la sécurité de fonctionnement des systèmes (incluant notamment les systèmes de supervision de type SCADA (Supervisory control and data acquisition). Les failles de sécurité intrinsèques des systèmes industriels présentent des risques spécifiques pour les différentes fonctions essentielles qu'ils remplissent pour le navire. Or il se trouve que ces systèmes font l'objet de menaces récurrentes (Advanced persistent threat) et qu'ils présentent des vulnérabilités spécifiques telles que l'absence de développement sécurisé (pas de prise en compte de la cybersécurité dans leur conception), les passerelles possibles avec les autres systèmes d'information, les faiblesses intrinsèques de leurs protocoles de gestion, etc.
Par conséquent, l'analyse du risque devra traiter avec une attention toute particulière ces systèmes.

Pour un exposé plus détaillé sur ces questions, on pourra se reporter au guide publié en janvier 2017 par la Direction des affaires maritimes : *Cybersécurité - Renforcer la protection des systèmes industriels du navire* ou encore au chapitre 4 (Assess risk exposure) du document *The Guidelines on Cyber Security Onboard Ships* de BIMCO.

Pour l'étape 2, on sera attentif :

- Aux systèmes en réseau et tout particulièrement les systèmes qui communiquent avec l'extérieur (ex. télémaintenance)
- Aux systèmes susceptibles d'être vus par des tiers (lors des opérations de maintenance par exemple) ; par conséquent, les vulnérabilités peuvent résulter de failles dans la politique ou les mesures de protection des tiers
- Au type et aux versions des différents logiciels
- Aux points d'entrée possible sur chacun des systèmes : par principe, on considère que tout point d'accès à un système informatique est une vulnérabilité potentielle
- A la redondance des systèmes (i.e. possibilité de transférer les fonctions devenues inopérantes en cas d'incident vers un autre système)
- A la redondance des données exploitées par les systèmes, incluant l'existence de programmes et de données de sauvegarde

Note 10: Comme dit précédemment, une vulnérabilité n'a de sens que vis-à-vis d'un scénario d'attaque. Il s'agit donc dans cette étape de définir un ou plusieurs scénarios jugés les plus dangereux par leurs conséquences sur le navire.
Par exemple, un port non sécurisé sur un poste de travail ouvre la possibilité de prise de contrôle du système ou de vol des données du disque dur. Autre exemple : l'absence de politique de sensibilisation du personnel aux risques liés à l'usage des messageries rend les systèmes d'information qui peuvent y être connectés vulnérables à l'hameçonnage (phishing). **Un scénario de référence consiste à imaginer une attaque de ce type sur un système essentiel à la sécurité du navire ou à son exploitation**.

Il faudra tenir compte de tous les aspects : technique, organisationnel, humain (ex. connaissances et sensibilité des équipages aux règles de base de l'hygiène informatique) pour bien cerner l'efficacité des mesures déjà en place (l'existence d'une procédure ou d'un dispositif de protection ne suffit pas, encore faut-il s'assurer qu'elle remplit bien son objectif par rapport aux scénarios d'attaque envisagés).

Note 11 : Pour une première analyse de risque sommaire, on pourra partir de la liste des questions de base proposée dans le guide BIMCO – chapitre 4 :

Quels sont les systèmes du navire qui présentent un risque ?
Quelles sont les conséquences potentielles d'un incident?
Qui est responsable de la sécurité de ces systèmes?
Est-ce que les systèmes opérationnels – tels que les automates industriels –sont connectés à internet, ou à tout autre réseau extérieur? Sont-ils protégés ?
Même question pour les systèmes informatiques
Quelles sont les mesures de protection déjà établies? Comment sont-elles appliquées ? Sont-elles connues du bord ?
Quel est le degré de connaissance et la formation des membres d'équipage vis-à-vis de ces risques ?

Note 12: La connaissance et les retours d'expérience d'incidents qui se seraient produits dans le passé doit servir à mieux appréhender les failles des systèmes.

Quelques exemples de failles classiques:

Organisation

- Pas d'organisation spécifique de la cybersécurité (conséquence : inefficacité ou inadaptation des circuits de décision)
- Pas de politique structurée de la compagnie (conséquences : dispositif inadapté et inefficace)
- Pas d'analyse de risques formalisée (conséquence : ignorance ou prise en compte incomplète de certains risques)

Formation

- Insuffisance de la formation et de la sensibilisation (conséquence : méconnaissance des risques et des procédures)
- Négligence dans l'emploi des moyens informatiques (conséquence : exposition accrue au risque d'attaque)
- Méconnaissance des équipages sur les conduites à tenir en cas d'incident (conséquence : retard ou inefficacité des actions à effectuer)

Accès aux systèmes

- Politique de mots de passe trop laxiste (conséquence : exposition accrue au risque d'intrusion dans les systèmes)
- Absence d'antivirus, pas de politique de mise à jour des systèmes de protection (idem)
- Systèmes d'exploitation obsolètes, pas de mises à jour (idem)
- Ports insuffisamment sécurisés (ports USB notamment)
- Pas de politique de contrôle des sous-traitants et intervenants (idem)

Porosité des systèmes (conséquence : exposition accrue au risque d'intrusion et d'atteinte au fonctionnement des systèmes et aux données)

- Absence de cloisonnement entre systèmes courants et systèmes critiques (et entre systèmes critiques)
- Connection permanente entre systèmes de bord et systèmes à terre
- Communications des données critiques non chiffrées

Défaut de supervision et de contrôle

- Absence de supervision du système (conséquence : ignorance des incidents ou réponse tardive)
- Pas de journalisation des événements (conséquence : ignorance des incidents ou réponse tardive)

Impréparation en cas d'incident (conséquence : aggravation des conséquences d'une attaque)

- Pas de procédure de traitement des incidents
- Résilience insuffisante des systèmes
- Pas de procédures de crise et de reprise d'activité
- Pas de politique de redondance et de sauvegarde des données

En résumé : pour la conduite de l'analyse du risque, quatre tâches essentielles sont à réaliser

1. Un inventaire des systèmes essentiels
2. Le choix d'un ou plusieurs scénarios d'attaque de référence, c'est-à-dire tels que leur succès entraîne des conséquences inacceptables pour la sécurité ou l'exploitation du navire
3. Une analyse - même simple – des vulnérabilités, incluant :
    i. Le recensement des points d'entrée du système (ports non sécurisés), qui accroissent la probabilité de succès d'une intrusion.
    ii. L'inventaire des mesures déjà en place (exemple : politique de mots de passe, anti-virus, réseaux séparés, communications chiffrées, etc.) à comparer aux mesures jugées nécessaires.

3ème étape : quantification du risque

A **l'analyse du risque** succède la **gestion du risque**. Le risque évalué et **quantifié** (voir ci-dessous) à partir de l'état existant, il doit être ajusté en référence à un **risque résiduel** acceptable (voir 4ème étape).

Il existe plusieurs définitions du risque. Il se définit généralement comme produit de la menace et des vulnérabilités, associé aux impacts de ces menaces, soit : **Risque = menace × impact × vulnérabilité**
Plusieurs méthodes existent – voir ci-dessous - Il n'entre pas dans le propos du présent document de les décrire en détail ou de les comparer.

Au-delà des différences techniques, du degré de sophistication de chaque méthode, les principes demeurent identiques. Il s'agit toujours d'aboutir à une quantification du risque pour disposer d'un critère d'appréciation comparatif, permettant à la fois de :

- Définir les actions à effectuer en priorité ;
- Suivre l'évolution du risque dans le temps ;
- Déterminer l'effet d'une modification d'une ou plusieurs composantes du risque (exemple : probabilité accrue d'une certaine menace, introduction de mesures nouvelles, situation dégradée).

Les compagnies maritimes sont libres d'employer pour ce faire la méthode de leur choix. L'adaptation des méthodes déjà éprouvées dans le domaine de la sécurité ou de la sûreté a le mérite de s'inscrire dans la culture existante de la compagnie.

Quelle que soit la méthode retenue, elle devra tenir compte des points suivants :

1) Une liste de systèmes à protéger en priorité
2) Les scénarios d'attaque possibles pour chaque système
3) Les vulnérabilités de chaque système
4) Les conséquences d'une attaque réussie sur :
    a) Le fonctionnement de chaque système
    b) Les données traitées par ce système (vis-à-vis de leur disponibilité, confidentialité et intégrité)
    c) Les fonctions qu'il assure pour le navire ou la compagnie

4ème étape : ajustement du dispositif en fonction du risque résiduel acceptable

Le risque résiduel est le risque subsistant à l'issue de l'analyse de risque, une fois que les mesures d'atténuation qui ont été vues comme nécessaires ont été mises en place. Le risque résiduel est un compromis entre le besoin du plus haut niveau de sécurité et le coût acceptable des mesures à mettre en place pour y arriver. Le risque résiduel est donc défini par la compagnie. C'est une décision de politique prise au plus haut niveau. La politique de la compagnie doit le définir explicitement.
Le guide édité par l'ANSSI : *Maîtrise du risque numérique – L'atout confiance* (cité supra) en donne la définition suivante (en utilisant le terme d'appétence au risque, dérivé de l'anglais « risk appetite ») :

L'appétence aux risques est le niveau de risque qu'un dirigeant accepte de prendre pour soutenir les activités et le développement de son organisation. Elle appuie les décisions stratégiques et oriente les opérations

Note 13: La définition du risque résiduel ne peut pas être imposée de manière réglementaire par une autorité extérieure. C'est une responsabilité de la compagnie, qui est évaluée vis-à-vis de sa politique plus générale de risque, qui intéresse sa politique commerciale, sa relation avec les assureurs, ses clients, etc.
On pourra utilement se reporter aux documents *Management du risque : une approche stratégique, AFNOR édition, 2018* et *Maîtrise du risque numérique – L'atout confiance* (ANSSI/AMRAE)

Méthodes de référence

Il existe plusieurs méthodes de référence pour la conduite de l'analyse du risque. Ces méthodes peuvent être appliquées tout ou partie pour effectuer l'analyse du risque de cybersécurité des navires. Il est aussi possible de s'inspirer de leurs principes, le but restant de s'assurer d'aboutir à une analyse crédible sur laquelle établir les règles de cybersécurité minimales.

On peut citer :

- La méthode EBIOS Risk Manager de l'ANSSI (pour en savoir plus :EBIOS Risk Manager)
- ISO/IEC 27005:2011 Information security risk management (Pour en savoir plus https://www.iso.org/fr/standard/42107.html)
- NIST SP 800-39 Managing Information Security Risk.
- La méthode décrite au chapitre 1-section 2 du document *Rules on Cyber Security for the Classification of Marine Units - NR 659 DT R00 [section Cyber managed]* – Bureau Veritas

POLITIQUE DE CYBERSECURITE

Objectif : définir les fonctions et responsabilités du personnel en matière de gestion des cyber-risques. La compagnie élabore, tient à jour et met en œuvre une politique de sécurité de ses systèmes d'information (PSSI). Celle-ci décrit l'ensemble des procédures et des moyens organisationnels et techniques mis en œuvre. La PSSI couvre à la fois la protection des systèmes d'information de la compagnie et ceux de ses navires (systèmes embarqués).

Elle définit au minimum :

- Les objectifs et les orientations stratégiques en matière de cybersécurité ;
- L'organisation mise en place pour satisfaire les objectifs de cybersécurité et notamment les rôles et les responsabilités du personnel interne et du personnel externe (prestataires, fournisseurs, etc.);
- Une politique de contrôle des prestataires et intervenants extérieurs ;
- L'organisation de la sensibilisation et de la formation du personnel à terre comme de celles des équipages ;
- Le système qualité, incluant les procédures internes de contrôle et d'audit ;
- Les mesures générales de cybersécurité, notamment en matière de gestion et de sécurité des ressources matérielles et logicielles des systèmes d'information, de contrôle d'accès, d'exploitation et d'administration, de sécurité des réseaux, des postes de travail et des données ;
- Les procédures de gestion de crise en cas d'incident affectant un système critique ;
- Les procédures de continuité et de reprise d'activité.

POINT IMPORTANT : les vérifications qui seront effectuées par l'administration dans le cadre de la certification ISM porteront essentiellement sur l'examen de la politique de cybersécurité mise en place par la compagnie. C'est donc un point-clé de la mise en conformité de la compagnie avec la résolution MSC428(98).
La compagnie tiendra à disposition des inspecteurs de l'administration l'ensemble des documents constituant cette politique de cybersécurité. Cette documentation devra pouvoir être consultée lors des audits effectués à bord des navires dans le cadre de leur certification ISM.

PROTECTION DES RESEAUX ET DES SYSTEMES D'INFORMATION

La protection des systèmes d'information du navire à pour but de réduire les chances de succès d'une intrusion malveillante résultant d'une action délibérée ou d'un mauvais usage de ces systèmes. Elle combine essentiellement des mesures techniques et procédurales. Les premières consistent à agir sur les systèmes, en renforçant les barrières techniques existantes ou en ajoutant des dispositifs de protection. Les secondes portent sur le bon usage des moyens numériques. L'ensemble des deux types de procédures est souvent désigné sous l'appellation d'hygiène numérique.

Parmi les principales **règles techniques**[3], on retient notamment :

- La tenue à jour d'un inventaire des systèmes, des systèmes d'exploitation et des logiciels autorisés, avec leurs versions ;
- L'emploi de matériels et de logiciels garantis et régulièrement mis à jour par leurs fournisseurs ;
- Installation et mise à jours régulières de logiciels anti-virus sur tous les postes ;
- La suppression ou l'isolement des matériels ou logiciels non autorisés ;
- La sécurisation des configurations des systèmes d'exploitation et des logiciels ;
- Le cloisonnement – autant que possible – des systèmes critiques, c'est-à-dire ceux qui sont essentiels pour la navigation et l'exploitation du navire (i.e. isolation par rapport aux réseaux distants)[4] ;
- La limitation au maximum des connexions sans fil aux réseaux du bord et leur cryptage quand elles sont indispensables ;
- La protection physique des équipements (postes, serveurs, routeurs, etc.) : les locaux concernés doivent bénéficier des mesures de sûreté du navire (zones d'accès restreint, accès verrouillés, surveillance, etc.)

Au plan **procédural**, les règles essentielles comprennent notamment :

- Un programme de sensibilisation - et au besoin de formation - du personnel – à terre comme à bord aux risques liés aux usages du numériques, ainsi qu'aux procédures de signalement des incidents ;

Note 14: Voir à ce sujet le guide BIMCO - point 5.3 – concernant les thèmes à traiter dans le cadre de la sensibilisation du personnel.

- La tenue à jour et la gestion des comptes et en particulier les comptes d'administration des systèmes ;
- Le renforcement des méthodes d'authentification aux comptes d'administration ;
- L'application d'une politique rigoureuse de mots de passe : changement des mots de passe par défaut, modifications régulières, choix de mots de passe robustes ;
- Une politique restrictive de droits d'accès et d'écriture, déterminée strictement par les besoins ;
- Des règles d'hygiène de base pour l'usage des messageries : prudence lors de l'ouverture des pièces jointes, vérification d'identité des expéditeurs, désactivation de l'exécution automatique des fichiers exécutables, etc.
- Des mesures de restrictions concernant les accès par des tiers et les accès à distance: visiteurs, techniciens de maintenance, personnel des ports, autorités, etc. ; exemple : réserver un poste isolé, non connecté aux réseaux du bord, qui jouera le rôle de sas avant toute connexion d'un appareil mobile (clé USB, téléphone mobile ou ordinateur portable) ;

GESTION DES INCIDENTS (RÉPONSE)

Note 15: **Rappel qu'est-ce qu'un incident de cybersécurité?**

La norme ISO IEC/27001 donne une définition du terme d'incident lié à la sécurité de l'information : « un ou plusieurs événements liés à la sécurité de l'information, indésirables ou inattendus, présentant une probabilité forte de compromettre les opérations liées à l'activité de l'organisme et de menacer la sécurité de l'information. »
La définition qu'en donne ANSSI est la suivante : un incident de sécurité est un événement qui porte atteinte à la disponibilité, la confidentialité ou l'intégrité d'un bien.

Il faut donc préciser ce qu'on entend par disponibilité, confidentialité et intégrité :

1. Disponibilité : propriété d'être accessible et utilisable à la demande. Par exemple : le brouillage (d'un GPS par exemple), le rançonnement ou le déni de service sont deux types d'attaques qui visent à rendre indisponibles les données (à des fins d'extorsion dans le cas des logiciels de rançonnement)
2. Confidentialité : Propriété d'une information qui n'est ni disponible, ni divulguée aux personnes, entités ou processus non autorisés La perte de confidentialité peut se produire à chaque fois qu'une intrusion se produit dans un système traitant ou stockant des informations de nature confidentielle (comme des données commerciales ou des secrets industriels).
3. Intégrité : Garantie que le système et l'information traitée ne sont modifiés que par une action volontaire et légitime. De nombreux types d'attaque ont pour résultat la corruption (c'est-à-dire la perte d'intégrité)

[3] Il ne s'agit évidemment là que d'exemples de règles parmi les plus essentielles. Pour aller plus loin, on se reportera aux documents de référence déjà cités

[4] Possibilité de plus en plus rare notamment du fait de l'extension de la télémaintenance

des données. Le fait de leurrer un GPS est un exemple de perte d'intégrité des données (des données erronées sont traitées par le système).

D'autres critères peuvent être considérés, comme celui de la traçabilité des données (garantie que les accès et tentatives d'accès aux éléments considérés sont tracés et que ces traces sont conservées et exploitables), l'authentification (preuve d'identité des utilisateurs de données) ou encore l'imputabilité des actions, c'est-à-dire l'impossibilité de contester qu'une certaine action a été effectuée sur un système d'information.

La gestion des incidents comporte deux aspects essentiels :

- La **surveillance** des activités, basée essentiellement sur la journalisation des événements ;
- La **réponse aux incidents** et notamment les procédures d'alerte

Pour la surveillance des activités – contribuant à la détection d'incidents - le minimum consiste dans la journalisation et l'analyse des événements. La compagnie met en place, au moins sur ses systèmes critiques, un système de journalisation (log en anglais) qui enregistre en continu les événements relatifs notamment à l'authentification des utilisateurs, à la gestion des comptes et des droits d'accès, à l'accès aux systèmes ainsi qu'à leur fonctionnement. Cette journalisation est utile également a posteriori, pour enquêter sur la survenue d'un incident.

Note 16: la mise en place de dispositifs de détection telles que des sondes, capables d'identifier des événements caractéristiques d'un incident de sécurité en cours ou à venir, est considérée comme excédant les exigences de base pour une compagnie maritime. En effet, la détection relève de l'activité de ce que l'on désigne généralement par l'acronyme SOC (Security operational centre) qui est un métier d'experts et requière de lourds investissements pour se maintenir à l'état de l'art dans le domaine de la cybersécurité. Les prestataires de SOC sont généralement qualifiés par l'ANSSI sur la base d'un référentiel exigeant (référentiel PDIS). On considère donc qu'on ne saurait exiger de la majorité des compagnies d'aller au-delà de règles de base de journalisation.

Le point essentiel concerne celui des **procédures de signalement des incidents**.

Il est essentiel que la compagnie définisse les responsabilités et établisse des procédures de réponse aux incidents et en premier lieu des procédures de signalement, à la fois en interne – au sein du bord et/ou de la compagnie - et auprès des autorités compétentes en cas d'incident le nécessitant. Ces procédures doivent faire partie intégrante de la politique de la compagnie et feront donc l'objet d'une vérification lors des audits menés par l'administration.

Note 17: la mise en place de procédures de gestions de crise est réputée faire partie intégrante de la politique de sécurité de la compagnie – par exemple pour le traitement des avaries ayant des conséquences sur la sécurité ou l'exploitation - et en tant que telle être inscrite dans le manuel de gestion de la sécurité. L'intégration des cyber-risques dans ce dispositif en constitue une extension naturelle.

Cette procédure pourra s'appuyer notamment sur le guide produit par la Direction des affaires maritimes - *Recommandations pour le signalement d'incidents de cybersécurité – guide destiné aux armateurs exploitant des navires sous pavillon franç*ais - diffusé en juillet 2019. Ce guide remplit quatre objectifs :

1. Recenser les informations utiles à rassembler et à fournir en cas d'incident sur le navire et ses systèmes d'information ;
2. Préciser les types d'incidents considérés ;
3. Préparer l'équipage du navire à réagir de manière adéquate à un incident de cybersécurité ;
4. Décrire la chaîne d'alerte et de réponse

Il comporte un formulaire-type à remplir en cas d'incident.

GESTION DE CRISE (RESILIENCE)

La compagnie maritime établit et met en œuvre, conformément à sa politique de cybersécurité inscrite dans sa politique générale de gestion de la sécurité, une procédure de gestion de crises en cas d'incidents de sécurité ayant un impact majeur sur ses fonctions essentielles, à terre comme en mer.

A ce titre, la politique de sécurité de la compagnie inclut un **Plan de continuité et de reprise de l'activité**, destiné à assurer la résilience des systèmes et des fonctions essentielles qu'ils servent.
Le but est de disposer d'une organisation et de mesures permettant de redémarrer aussi vite que possible les activités – i.e. la sécurité de la navigation et l'efficacité des opérations commerciales - avec le minimum de perte d'informations,

avec ou sans l'assistance d'un prestataire et de viser, dans le délai le plus court possible, une restauration complète des fonctions et des données essentielles.

Comme pour la protection des systèmes et plus généralement pour la prévention des accidents, les procédures de gestion de crise combinent :

- Des mesures techniques : sauvegarde des données, isolement des systèmes infectés, etc.
- Des mesures d'organisation : répartition des rôles et des tâches

Une des conditions-clés de la gestion de crise est la préparation. Cela inclut notamment la redondance des systèmes et des données – avec l'existence de sauvegardes hors-lignes – dont la restauration aura été testée - permettant la restauration rapide des fonctions assurées par les systèmes d'information – et la réalisation régulière d'exercices de gestion de crise pour s'assurer de son efficacité.

Le Plan de continuité/reprise de l'activité constitue un chapitre essentiel de la politique de sécurité de la compagnie et doit être revu, testé et enrichi à intervalles réguliers pour rester efficace.

Note 18: pour la mise en place de procédures de gestions de crise et de plans de continuité d'activité, on pourra s'appuyer notamment sur la norme *ISO 22301 : 2012 Systèmes de management de la continuité d'activité*

VI. TRANSPOSITION DE CES OBJECTIFS DANS LE MANUEL DE GESTION DE LA SECURITE (SMS)

Le code ISM énonce des règles générales de gestion de la sécurité des navires, à l'attention des compagnies maritimes qui les exploitent. Ce sont des principes similaires à ceux exposés en II qui s'appliquent au traitement des risques subis par les systèmes d'information des compagnies et des navires. L'intégration des cyber-risques dans le manuel de gestion de la sécurité de la compagnie en constitue une extension naturelle, appliquant les mêmes principes généraux : politique de sécurité, préparation, mesures de prévention, de contrôle, de réaction et de réponse en cas d'incident.

Le tableau figurant en **Annexe II** décrit, pour chacune des règles du code ISM, sa traduction pour la question spécifique de la cybersécurité, autrement dit ce sur quoi les audits menés par l'administration porteront leur attention. Comme pour toutes les vérifications conduites dans le cadre de la certification ISM, celles portant sur la cybersécurité se baseront essentiellement sur des vérifications documentaires - politique de la compagnie, procédures, mécanismes de contrôle et d'amélioration continue – plus que sur le détail technique des dispositions mises en place. Ces vérifications seront complétées par des entretiens avec le personnel désigné pour l'application de cette politique, y compris le capitaine, ainsi que de manière aléatoire avec des membres du personnel.

VII. SYNTHESE

Objectifs du guide

Décrire les principes généraux et établir le référentiel qui servira de base pour la prise en compte par les compagnies maritimes de la cybersécurité dans les manuels de gestion de la sécurité (en référence au code ISM).

La cybersécurité dans le code ISM

La résolution MSC.428(98) adoptée le 16 juin 2017 préconise l'intégration des cyber-risques maritimes dans les systèmes de gestion de la sécurité gérés dans le cadre des dispositions du Code ISM. Elle s'applique donc à toutes les compagnies maritimes exploitant des navires relevant des dispositions de la Convention internationale pour la sauvegarde de la vie humaine en mer (SOLAS 1974).

Les objectifs à atteindre

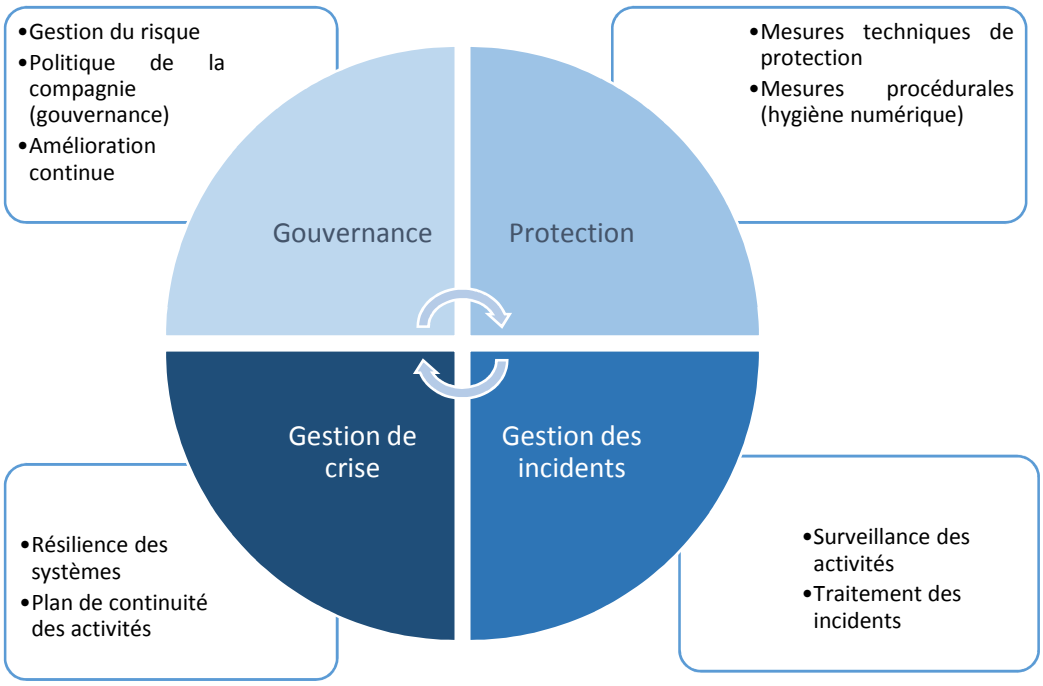
Pour les armateurs, il s'agit de mettre en place les dispositifs et mesures aptes à traiter convenablement les cyber-risques et les intégrer de manière appropriée dans leurs systèmes de gestion de la sécurité, de sorte à se mettre en conformité avec les objectifs posés par le code ISM.

Les règles de cybersécurité à mettre en place

En fonction des capacités organisationnelles, techniques, financières et humaines de la compagnie, les règles de cybersécurité à mettre en place et à traduire dans le manuel de gestion de la sécurité (SMS) de la compagnie doivent comprendre au minimum les éléments suivants :

1. Une politique de cybersécurité à tous les échelons
2. Une analyse de risques régulièrement mise à jour, incluant un inventaire des systèmes et des procédures existantes
3. Des procédures techniques, humaines et organisationnelles
4. Des procédures de suivi au quotidien
5. Des procédures d'alerte et de reprise de l'activité

Schéma général :



La pertinence et la forme pratique des recommandations présentées dans ce guide doit s'apprécier au cas par cas, en fonction des particularités de la compagnie – type d'exploitation, de navigation, de moyens disponibles, etc. – avec une application qui soit la plus adaptée possible à ces particularités.

L'évaluation de conformité par l'administration compétente

En fin de compte, ce qui prévaut – et qui sera examiné lors des audits conduits par l'administration compétente dans le cadre de la certification ISM – est la pertinence des mesures adoptées et la fiabilité de la gestion par la compagnie de son dispositif de cybersécurité à travers son manuel de sécurité.

****

VIII. ANNEXES

ANNEXE I **TABLEAU DE CORRESPONDANCE DES TEXTES DE REFERENCE**
ANNEXE II **TABLEAU DE TRADUCTION VERS LE CODE ISM**

ANNEXE I TABLEAU DE CORRESPONDANCE DES TEXTES DE REFERENCE

Principes clés de cybersécurité	MSC FAL1/Circ3	Guide BIMCO	Guides DAM	BV Cyber Managed (659-NR-2018)	Arrêté du 14 septembre 2018
Identifier	3.5. Évaluer de manière complète les niveaux de cybersécurité effectifs et désirés, afin notamment d'en repérer les lacunes et de les traiter dans le meilleur usage des moyens disponibles	CH.2. IDENTIFY THREATS (p9) CH.3. IDENTIFY VULNERABILITIES (incl. list of onboard systems, list of common vulnerabilities (p13-14), (p15), CH.4. ASSESS RISK EXPOSURE list of questions (p16), Relationship with vendors (p8), Third parties access (p18), 4.3 Risk assessment process (p22)	Guide 1-R1 : Réaliser une évaluation de la sécurité des systèmes d'information du navire, incluant : - cartographie logicielle et matérielle, - définition des éléments sensibles, - vulnérabilités des systèmes	Section 2 (et Rec. 161 de l'IACS)	Annexe – Règle 1 : de l'IACS)analyse de risque Annexe – Règle 6 : Cartographie Annexe – Règle 5 : Audits de sécurité
	3.5.1 Définir les fonctions-clés et tâches du personnel	5.3. Procedural protection measures - training and awareness (p29)	Guide 1-R2 : Rédiger une politique de compagnie des systèmes d'information du navire	Section 4 - 2.2-3.1	Annexe – Règle 2 : politique de sécurité
	3.5.1 Identifier les systèmes et données critiques du point de vue des conséquences d'une défaillance	CH.3. IDENTIFY VULNERABILITIES (incl. list of onboard systems, list of common vulnerabilities (p13), (p15), list of questions (p16), risk assesment made by the comany (p21), Risk assessment process (p22)	Guide 1-R1 : Réaliser une évaluation de la sécurité des systèmes d'information du Navire : - cartographie logicielle et matérielle du navire, - définition des éléments sensibles du navire, - vulnérabilités des systèmes	Section 2	Annexe – Règle 1 : analyse de risque Annexe – Règle 6 : Cartographie Annexe – Règle 5 : Audits de sécurité
	2.1.1 Liste des systèmes vulnérables	ANNEX 1 : List of target systems	ANNEXE 1 : Vulnérabilités spécifiques des navires		

Principes clés de cybersécurité	MSC FAL1/Circ3	Guide BIMCO	Guides DAM	BV Cyber Managed (659-NR-2018)	Arrêté du 14 septembre 2018
Protéger	3.3 Implication des niveaux dirigeants : incorporer la culture de cybersécurité dans l'entreprise et établir un mécanisme de gestion du risque appliqué et suivi de manière permanente	CH.4. ASSESS RISK EXPOSURE Cyber risk assessment to start at senior management level (p16)	Guide 1-R2 : Rédiger une politique de compagnie des systèmes d'information du navire	Section 4 – 1.2.1	Annexe – Règle 2 : politique de sécurité
	3.5.2 Mettre en place des processus et des mesures de contrôle/ d'atténuation des risques	CH.5. DEVELOP PROTECTION AND DETECTION MEASURES	Guide 1-R3 : appliquer des mesures d'hygiène (ex. droits d'accès, mots de passe, gestion des privilèges, archivage des données, messagerie sécurisée, mises à jour)	Section 2-Ch2, Section 3	Annexe – Chapitre II : Règles relatives à la protection des réseaux et systèmes d'information – [règles 7 à 17]
		5.1. Defense in-depth and in breadth (p24) 5.2. Technical protection measures - networks (p25-26)-malware detection (p27)-application software security (p28)-data recover capability (p28)-upgrade and software maintenance (p31)	Guide 1-R4 : sécuriser les échanges (droits d'accès aux systèmes, opérations autorisées, contrôle des équipements, traçabilité des accès)	Section 4-3.3 (maintenance)	
		5.2. Technical protection measures – physical security (p26)	Guide 1-R7 : Appliquer les mesures de protections physiques des systèmes d'information du navire	Section 4- Ch 4 Physical security (incl. Removable media)	
	3.7. S'assurer de la sensibilité et de la vigilance en matière de cybersécurité à tous les niveaux de l'organisation	5.3. Procedural protection measures - training and awareness (p29)	Guide 1-R3 : appliquer des mesures d'hygiène (formation et sensibilisation)	Section 4- 2.1.1-3.1.1	
	3.5.2 Mettre en place des plans d'urgence en cas d'événement, afin d'assurer la continuité de la navigation et des opérations	CH.6. ESTABLISH CONTINGENCY PLANS	Guide 1-R2 : Rédiger une politique de compagnie des systèmes d'information du navire	Section 4- 3.4 (incident response)	
		Safety management system (p34)	Guide 1-R5 : mettre en place un plan de continuité de fonctionnement post-incident (système de secours, isolation des systèmes défaillants, essais, restauration des données)	Section 4- 3.4 (incident response) et Rec.155 de l'IACS	

Principes clés de cybersécurité	MSC FAL1/Circ3	Guide BIMCO	Guides DAM	BV Cyber Managed (659-NR-2018)	Arrêté du 14 septembre 2018
Détecter	3.5.3 Mettre en place les dispositifs nécessaires afin de détecter des événements/incidents dans les meilleurs délais	Detection, blocking and alerts (p26)	Guide 1-R6 : Contrôler et gérer les incidents de systèmes d'information du navire	Section 4- 3.2	Annexe – Règle 18 : détection (NB :voir les réserves émises dans le guide) Annexe – Règles 19 et 20 : journalisation et corrélation
Répondre	3.5.4 Mettre en place des dispositifs de résilience/retour à la normale des systèmes critiques affectés par l'incident	CH.7. RESPOND TO AND RECOVER FROM CYBER SECURITY INCIDENTS 7.1. Effective response 7.2. Recovery plan 7.3. Investigating cyber incidents	Guide 1-R5 : mettre en place un plan de continuité de fonctionnement post-incident (système de secours, isolation des systèmes défaillants, essais, restauration des données) Guide 4 - Recommandations pour le signalement d'incidents de cybersécurité – guide destiné aux armateurs exploitant des navires sous pavillon français	Section 4- 3.4 (incident response)	Annexe – Règle 21 : réponse aux incidents Annexe – Règle 22 : traitement des alertes
Rétablir	3.5.5 Etablir des mécanismes de compensation et de restauration des systèmes critiques affectés par l'incident	CH.7. RESPOND TO AND RECOVER FROM CYBER SECURITY INCIDENTS	Guide 1-R5 : mettre en place un plan de continuité de fonctionnement post-incident (système de secours, isolation des systèmes défaillants, essais, restauration des données)	Section 4-3.4 (incident response)	Annexe – Règle 21 : réponse aux incidents Annexe – Règle 22 : traitement des alertes

ANNEXE II TABLEAU DE TRADUCTION VERS LE CODE ISM

Référence Code ISM	Enoncé de la disposition du Code	Application à la cybersécurité	Contrôle par l'administration lors des audits	Méthode de vérification
1.2. Objectifs				
1.2.1.	Les objectifs du Code sont de garantir la sécurité en mer et la prévention des lésions corporelles ou des pertes en vies humaines et d'empêcher les atteintes à l'environnement, en particulier l'environnement marin, ainsi que les dommages matériels.	Inscription des objectifs essentiels de la cybersécurité Les pratiques de cybersécurité doivent faire partie intégrante de la politique de sécurité de la compagnie	Les inspecteurs examineront le manuel de gestion de la sécurité de la compagnie et vérifieront qu'il intègre la cybersécurité ; la prise en compte des objectifs-clés de la cybersécurité dans ce document sera vérifiée	Consultation des documents pertinents (politique de la compagnie, procédures)
	Les objectifs de la compagnie en matière de gestion de la sécurité devraient notamment être les suivants :			Entretien avec les personnes désignées par la compagnie – et identifiées comme telles dans le SMS – pour les questions de cybersécurité
	1 offrir des pratiques d'exploitation et un environnement de travail sans danger ;			
1.2.2	2 évaluer tous les risques identifiés pour ses navires, son personnel et l'environnement et établir des mesures de sécurité appropriées ; et	Analyse spécifique du risque lié à la cybersécurité, comportant cinq phases : 1) cartographie de l'état existant 2)analyse des menaces 3) analyse des vulnérabilités 4) mesures existantes 5) mesure du risque	Les inspecteurs s'assureront de l'existence d'une analyse de risque documentée et de l'application de ses conclusions dans le système de gestion de la cybersécurité	Consultation des documents pertinents (l'analyse de risque doit être formalisée par des documents spécifiques consultables)
	3 améliorer constamment les compétences du personnel à terre et à bord des navires en matière de gestion de la sécurité, et notamment préparer ce personnel aux situations d'urgence, tant sur le plan de la sécurité que de la protection du milieu marin.	Formation et sensibilisation du personnel en cybersécurité : objectifs, méthodes, programmation, personnel concerné ; processus d'amélioration continue inscrit dans la politique de la compagnie	Examen du programme de formation et de sa mise en œuvre	Consultation du programme (contenu, périodicité des formations, personnel formé, méthodes de formation, enregistrements) ; Entretiens avec les personnes désignées et - de manière aléatoire – avec des membres du personnel
1.2.3	Le système de gestion de la sécurité devrait garantir :			
	1 que les règles et règlements obligatoires sont observés ; et	Autorité de la structure responsable en matière de cybersécurité ; doit pouvoir	Examen de la structure mise en place et des circuits de décision	

		exercer cette autorité pour faire appliquer la politique mise en place, au sein de la compagnie et à bord		Consultation des documents pertinents (politique de la compagnie, procédures), questions au capitaine et aux personnes désignées pour la cybersécurité
	2 que les recueils de règles, codes, directives et normes applicables, recommandés par l'Organisation, les Administrations, les sociétés de classification et les organismes du secteur maritime sont pris en considération	Pas de remarque propre à la cybersécurité		
1.3 Application	Les prescriptions du présent Code peuvent être appliquées à tous les navires	Concerne tous les navires relevant de l'application du Code		
1.4. Modalités pratiques d'un système de gestion de la sécurité	Chaque compagnie devrait établir, mettre en œuvre et maintenir un système de gestion de la sécurité qui comporte les modalités pratiques suivantes			
1.4.1	une politique en matière de sécurité et de protection de l'environnement	Politique de cybersécurité de la compagnie, complétant la politique globale de gestion de la sécurité	Examen de la politique de la compagnie	
1.4.2	des instructions et des procédures propres à garantir la sécurité de l'exploitation des navires et la protection de l'environnement, conformément à la réglementation internationale et à la législation de l'État du pavillon, pertinentes	Procédures de cybersécurité : Protection (hygiène informatique, protection physique, maîtrise des échanges, formation, tests) Surveillance continue (journalisation) Procédures de traitement des incidents Procédures de gestion du risque (continuité et reprise d'activité)	Examen des procédures mises en place (formalisation, pertinence vis-à-vis des objectifs essentiels de cybersécurité)	Consultation des documents pertinents (politique de la compagnie, procédures) Questions aux membres du personnel sur le degré de connaissance des procédures Vérifications aléatoires de l'existence de mesures de protection (hygiène numérique en particulier) sur des postes informatiques
1.4.3	une hiérarchie et des moyens de communication permettant aux membres du personnel de bord de communiquer entre eux et avec les membres du personnel à terre	Définition des rôles en matière de cybersécurité et création d'une structure responsable au niveau de compagnie et à bord de chaque navire. Établissement de circuits de décision spécifiques, cohérents avec ceux établis pour les autres risques décrits dans le manuel ISM	Examen de la politique de la compagnie	Consultation des documents pertinents (politique de la compagnie, procédures) Questions aux membres du personnel sur le degré de connaissance des procédures

1.4.4	des procédures de notification des accidents et du non-respect des dispositions du présent code	Mise en place de procédures de signalement d'incident Inclusion dans le système interne de qualité du traitement des défaillances dans le domaine cybersécurité	Examen des procédures	Vérification documentaire de la procédure de signalement ; questions au personnel concerné sur la connaissance de ces procédures ; si possible : simulation d'alerte
1.4.5	des procédures de préparation et d'intervention pour faire face aux situations d'urgence	Disposer de plans d'urgence, connus de l'ensemble du personnel et régulièrement testés (inclusion des tests dans le plan d'audits internes et d'exercices de la compagnie et du bord)	Consultation des plans d'urgence et de gestion de crise	Vérification documentaire ; questions au capitaine et aux personnes désignées pour la cybersécurité
1.4.6	des procédures d'audit interne et de maîtrise de la gestion	Inclure les audits des procédures de cybersécurité dans le système d'audit interne de la compagnie		
2. Politique en matière de sécurité et de protection de l'environnement				
2.1	La compagnie devrait établir une politique en matière de sécurité et de protection de l'environnement qui décrive comment les objectifs énoncés au paragraphe 1.2 seront réalisés	Politique de cybersécurité de la compagnie, complétant la politique globale de gestion de la sécurité	Examen de la politique de la compagnie	Vérification documentaire ; questions au capitaine et aux personnes désignées pour la cybersécurité
2.2	La compagnie devrait veiller à ce que cette politique soit appliquée à tous les niveaux de l'organisation, tant à bord des navires qu'à terre	Autorité de la structure responsable en matière de cybersécurité ; doit pouvoir exercer cette autorité pour faire appliquer la politique mise en place, au sein de la compagnie et à bord Les procédures de contrôle qualité interne incluent la cybersécurité dans leur domaine d'application	Examen de la politique de la compagnie ; accent sur la politique de contrôle interne	Vérification documentaire ; questions au capitaine et aux personnes désignées pour la cybersécurité
3. Responsabilité et autorité de la compagnie				

3.1	Si la responsabilité de l'exploitation du navire incombe à une entité autre que le propriétaire de ce navire, ce dernier doit faire parvenir à l'administration le nom complet et les détails de cette entité	Pas de remarque propre à la cybersécurité		
3.2	La compagnie devrait définir et établir par écrit les responsabilités, les pouvoirs et les relations réciproques de l'ensemble du personnel chargé de la gestion, de l'exécution et de la vérification des activités liées à la sécurité et à la prévention de la pollution ou ayant une incidence sur celles-ci	Définition des rôles en matière de cybersécurité et création d'une structure responsable au niveau de compagnie et à bord de chaque navire (définition dans la politique de la compagnie)	Examen de la politique de la compagnie ; accent sur la définition des rôles et de l'existence de structures adaptées	Vérification documentaire ; questions au capitaine et aux personnes désignées pour la cybersécurité
3.3	La compagnie doit veiller à ce que des ressources adéquates et un soutien approprié à terre soient fournis pour que la ou les personnes désignées puissent s'acquitter de leurs tâches	La politique de la compagnie décrit les ressources nécessaires à l'application de la politique de cybersécurité– la compagnie s'engage à mettre en adéquation ces ressources avec les besoins identifiés	Examen de la politique de la compagnie ; accent sur la question de l'adéquation des ressources	Vérification documentaire ; questions au capitaine et aux personnes désignées pour la cybersécurité
4. Personne désignée	Pour garantir la sécurité de l'exploitation de chaque navire et pour assurer la liaison entre la compagnie et les personnes à bord, chaque compagnie devrait, selon qu'il convient, de désigner une ou plusieurs personnes à terre ayant directement accès au plus haut niveau de la direction. La responsabilité et les pouvoirs de la ou des personnes désignées devraient notamment consister à surveiller les aspects de l'exploitation de chaque navire, liés à la sécurité et à la prévention de la pollution et veiller à ce que des ressources adéquates et un soutien approprié à terre soient fournis, selon que de besoin	Définition des rôles en matière de cybersécurité et création d'une structure responsable au niveau de compagnie et à bord de chaque navire (définition dans la politique de la compagnie)	Examen de la politique de la compagnie ; accent sur la question de l'adéquation des ressources	Vérification documentaire ; questions au capitaine et aux personnes désignées pour la cybersécurité
5. Responsabilité et autorité du capitaine				
5.1	La compagnie devrait définir avec précision et établir par écrit les responsabilités du capitaine pour ce qui est de	Définition des rôles en matière de cybersécurité et création d'une structure responsable au niveau de compagnie et à bord de chaque navire (définition dans la politique de la compagnie)	Examen de la politique de la compagnie ; accent sur la définition des rôles et de l'existence de structures adaptées	Vérification documentaire ; questions au capitaine et aux personnes désignées pour la cybersécurité
5.1.1	mettre en œuvre la politique de la compagnie en matière de sécurité et de protection de l'environnement			
5.1.2	encourager les membres de l 'équipage à appliquer cette politique			

5.1.3	donner les ordres et les consignes appropriées d'une manière claire et simple			
5.1.4	vérifier qu'il est satisfait aux spécifications			
5.1.5	passer en revue périodiquement le système de gestion de la sécurité et signaler les lacunes à la direction à terre			
5.2	La compagnie devrait veiller à ce que le système de gestion de la sécurité en vigueur à bord du navire mette expressément l'accent sur l'autorité du capitaine. La compagnie devrait préciser, dans le système de gestion de la sécurité que l'autorité supérieure appartient au capitaine et qu'il a la responsabilité de prendre des décisions concernant la sécurité et la prévention de la pollution et de demander l'assistance de la compagnie si cela s'avère nécessaire			
6. Ressources et personnel				
6.1	La compagnie devrait s'assurer que le capitaine :	La politique de la compagnie décrit les ressources nécessaires à l'application de la politique de cybersécurité– la compagnie s'engage à mettre en adéquation ces ressources avec les besoins identifiés	Voir points précédents	
6.1.1	a les qualifications requises pour commander le navire			
6.1.2	connaît parfaitement le système de gestion de la sécurité de la compagnie			
6.1.3	bénéficie de tout l'appui nécessaire pour s'acquitter en toute sécurité de ses tâches			
6.2	La compagnie devrait s'assurer que chaque navire est doté d'un personnel navigant qualifié, breveté et ayant l'aptitude physique requise conformément aux prescriptions internationales et nationales pertinentes. La compagnie devrait s'assurer que chaque navire est : 1. doté d'un personnel navigant ayant les qualifications, les brevets et certificats et l'aptitude physique qu'exigent les prescriptions nationales et internationales; et 2. doté d'effectifs appropriés afin de couvrir toutes les aspects liés au maintien de la sécurité des opérations à bord	Définition dans la politique de la compagnie des besoins et de la mise en œuvre de la formation et de la sensibilisation du personnel en cybersécurité : objectifs, méthodes, programmation, personnel concerné	Examen de la politique de la compagnie ; accent sur la politique de formation et de sa mise en œuvre	Consultation du programme (contenu, périodicité des formations, personnel formé, méthodes de formation, enregistrements) ; Entretiens avec les personnes

6.3	La compagnie devrait établir des procédures pour garantir que le nouveau personnel et le personnel affecté à de nouvelles fonctions liées à la sécurité et à la protection de l'environnement reçoivent la formation nécessaire à l'exécution de leurs tâches. Les consignes qu'il est essentiel de donner avant l'appareillage devraient être identifiées, établies par écrit et transmises			désignées et - de manière aléatoire – avec des membres du personnel
6.4	La compagnie devrait veiller à ce que l'ensemble du personnel intervenant dans le système de gestion de la sécurité de la compagnie comprenne de manière satisfaisante les règles, règlements, recueils de règles, codes et directives pertinents			
6.5	La compagnie devrait établir et maintenir des procédures permettant d'identifier la formation éventuellement nécessaire pour la mise en œuvre du système de gestion de la sécurité et veiller à ce qu'une telle formation soit dispensée à l'ensemble du personnel concerné			
6.6	La compagnie devrait élaborer des procédures garantissant que le personnel du navire reçoive les renseignements appropriés sur le système de gestion de la sécurité dans une ou plusieurs langue(s) de travail qu'il comprenne			
6.7	La compagnie devrait veiller à ce que les membres du personnel du navire soient capables de communiquer efficacement entre eux dans le cadre de leurs fonctions liées au système de gestion de la sécurité			
7. Établissement de plans pour les opérations à bord	La compagnie devrait établir des procédures, plans et consignes, y compris des listes de contrôle, s'il y a lieu, pour les principales opérations à bord qui concernent la sécurité du personnel et du navire et la protection de l'environnement. Les diverses tâches en jeu devraient être définies et être assignées à un personnel qualifié.	Politique de cybersécurité de la compagnie, complétant la politique globale de gestion de la sécurité Description des mesures essentielles de cybersécurité	Examen des procédures mises en place (formalisation, pertinence vis-à-vis des objectifs essentiels de cybersécurité)	Consultation des documents pertinents (politique de la compagnie, procédures) Questions aux membres du personnel sur le degré de connaissance des procédures Vérifications aléatoires de l'existence de mesures de protection (hygiène numérique en particulier) sur des postes informatiques

8. Préparation aux situations d'urgence				
8.1	La compagnie devrait identifier les situations d'urgence susceptibles de survenir à bord et établir les procédures à suivre pour y faire face.	La compagnie établit un plan de gestion de crise et de continuité/reprise de l'activité	Examen des plans d'urgence et des procédures de gestion de crise spécifiques aux risques cyber	Vérification documentaire ; questions au capitaine et aux personnes désignées pour la cybersécurité
8.2	La compagnie devrait mettre au point des programmes d'exercices préparant aux mesures à prendre en cas d'urgence.	La compagnie met en place des mécanismes de contrôle interne et conduit, à intervalle défini dans le document de politique, des exercices de mise en situation (exercices de gestion de crise)	Examen des registres d'exercices, des comptes rendus et du suivi des actions correctives	Vérifications aléatoires de la correction des écarts constatés
8.3	Le système de gestion de la sécurité devrait prévoir des mesures propres à garantir que l'organisation de la compagnie est à tout moment en mesure de faire face aux dangers, accidents et situations d'urgence pouvant mettre en cause ses navires	La compagnie établit un plan de gestion de crise et de continuité/reprise de l'activité	Examen des plans d'urgence et des procédures de gestion de crise spécifiques aux risques cyber	Vérification documentaire ; questions au capitaine et aux personnes désignées pour la cybersécurité
9. Notification et analyse des irrégularités, des accidents et des incidents potentiellement dangereux				
9.1	Le système de gestion de la sécurité devrait prévoir des procédures garantissant que les irrégularités, les accidents et les incidents potentiellement dangereux sont signalés à la compagnie et qu'ils font l'objet d'une enquête et d'une analyse, l'objectif étant de renforcer la sécurité et la prévention de la pollution.	La politique de la compagnie inclut un dispositif incluant : - La surveillance continue (basé notamment sur la journalisation des événements) - des procédures de réponse aux incidents (incluant leur analyse et la formalisation des dispositions correctives) - Des procédures de signalement et de traitement des alertes	Examen de ces points dans la politique de la compagnie	Vérification documentaire et entretiens avec les personnes désignées ; le cas échéant, consultation de comptes rendus d'incident et de la formalisation des enseignements tirés
9.2	La compagnie devrait établir des procédures pour l'application de mesures correctives, y compris de mesures propres à éviter que le même problème ne se reproduise			

10. Maintien en état du navire et de son armement				
10.1	La compagnie devrait mettre en place des procédures permettant de vérifier que le navire est maintenu dans un état conforme aux dispositions des règles et des règlements pertinents ainsi qu'aux prescriptions supplémentaires qui pourraient être établies par la compagnie			
10.2	Pour satisfaire ces prescriptions, la compagnie devrait veiller à ce que :			
10.2.1	des inspections soient effectuées à des intervalles appropriés	La compagnie inclut la cybersécurité dans son processus d'amélioration continue, incluant des audits internes et des exercices réguliers	Examen de ces points dans la politique de la compagnie	Vérification documentaire et entretiens avec les personnes désignées ; le cas échéant, consultation de comptes rendus d'incident et de la formalisation des enseignements tirés
10.2.2	toute irrégularité soit signalée, avec indication de la cause éventuelle, si celle-ci est connue	Les irrégularités constatées lors des audits internes ou dans l'analyse des incidents de cybersécurité sont documentées et font l'objet d'actions correctives suivies et documentées	Examen des procédures d'audit interne et de la tenue à jour d'un registre	Consultation des rapports d'audits internes et des rapports d'incident ; Vérifications aléatoires de la correction des écarts constatés
10.2.3	les mesures correctives appropriées soient prises			
10.2.4	ces activités soient consignées dans un registre			
10.3	La compagnie devrait identifier le matériel et les systèmes techniques dont la panne soudaine pourrait entraîner des situations dangereuses. Le système de gestion de la sécurité devrait prévoir des mesures spécifiques pour renforcer la fiabilité de ce matériel et de ces systèmes. Ces mesures devraient inclure la mise à l 'essai à intervalles réguliers des dispositifs et du matériel de secours ainsi que des systèmes techniques qui ne sont pas utilisés en permanence	1er temps : Analyse spécifique du risque lié à la cybersécurité, comportant cinq phases : 1) cartographie de l'état existant 2)analyse des menaces 3) analyse des vulnérabilités 4) mesures existantes 5) mesure du risque. La première étape est la plus essentielle : connaître les systèmes et leur caractère critique, fonction de leur vulnérabilité et des conséquences possibles de leur défaillance 2ème temps : mise en place/renforcement de mesures de protection	Examen de ces points dans la politique de la compagnie	Consultation des documents pertinents (politique de la compagnie, procédures) Questions aux membres du personnel sur le degré de connaissance des procédures Vérifications aléatoires de l'existence de mesures de protection (hygiène numérique en particulier) sur des postes informatiques
10.4	Les inspections mentionnées au paragraphe 10.2 ci-dessus ainsi que les mesures visées au paragraphe 10.3 devraient être intégrées dans le programme d'entretien courant			

11. Documents				
11.1	La compagnie devrait élaborer et maintenir des procédures permettant de maîtriser tous les documents et renseignements se rapportant au système de gestion de la sécurité	Politique de cybersécurité de la compagnie (formellement identique dans ses principes à la politique globale de sécurité)	Examen de la politique de la compagnie	Consultation des documents pertinents ; entretiens avec les personnes désignées
11.2	La compagnie devrait s'assurer que :			
11.2.1	des documents en cours de validité sont disponibles à tous les endroits pertinents			
11.2.2	les modifications apportées à ces documents sont examinées et approuvées par le personnel compétent			
11.2.3	les documents périmés sont rapidement retirés			
11.3	Les documents utilisés pour décrire et mettre en œuvre le système de gestion de la sécurité peuvent faire l'objet du "manuel de gestion de la sécurité". Ces documents devraient être conservés sous la forme jugée la plus appropriée par la compagnie. Chaque navire devrait avoir à bord tous les documents le concernant			
12. Vérification, examen et évaluation effectués par la compagnie				
12.1	La compagnie devrait effectuer des audits internes à bord et à terre, à des intervalles ne dépassant pas 12 mois, pour vérifier que les activités liées à la sécurité et à la prévention de la pollution sont conformes au système de gestion de la sécurité. Dans des circonstances exceptionnelles, cet intervalle peut être prolongé de trois mois au plus	Inclusion dans la politique de la compagnie d'audits et d'exercices portant sur la gestion de la cybersécurité (ex. simulation de cyberattaque affectant des systèmes critiques du navire) Enseignements des exercices et des audits portés à la connaissance du personnel à terre et des équipages (formation continue et campagnes de sensibilisation)	Examen de ces points dans la politique de la compagnie ; accent sur les procédures d'audit interne et de la tenue à jour d'un registre	Vérification documentaire et entretiens avec les personnes désignées ; le cas échéant, consultation de comptes rendus d'incident et de la formalisation des enseignements tirés ; Consultation des rapports d'audits internes et des rapports d'incident ; Vérifications aléatoires de la correction des écarts constatés
12.2	La compagnie devrait vérifier périodiquement que tous ceux qui exécutent des tâches liées au Code ISM agissent en conformité avec les responsabilités qui incombent à la compagnie en vertu du Code			
12.3	La compagnie devrait évaluer périodiquement l'efficacité du système de gestion de la sécurité conformément aux procédures qu'elle a établies			

12.4	Les audits ainsi que les éventuelles mesures correctives devraient être exécutés conformément aux procédures établies			
12.5	Le personnel qui procède aux audits ne devrait pas faire partie du secteur soumis à l'audit, à moins que cela soit impossible en raison de la taille et des caractéristiques de la compagnie			
12.6	Les résultats des audits et révisions devraient être portés à l'attention de l'ensemble du personnel ayant des responsabilités dans le secteur en cause			
12.7	Le personnel d'encadrement responsable du secteur concerné devrait prendre sans retard les mesures correctives nécessaires pour remédier aux défectuosités constatées			