Conduite des évaluations de la sécurité informatique dans les installations nucléaires

IAEA
Agence internationale de l'énergie atomique

COLLECTION SÉCURITÉ NUCLÉAIRE DE L'AIEA ET PUBLICATIONS CONNEXES

Les orientations de l'AIEA sur les questions de sécurité nucléaire liées à la prévention, la détection et l'intervention en cas d'actes criminels ou d'actes non autorisés délibérés, mettant en jeu ou visant des matières nucléaires, d'autres matières radioactives, des installations associées ou des activités associées, sont traitées dans la **collection Sécurité nucléaire de l'AIEA**. Ces publications sont conformes aux instruments internationaux relatifs à la sécurité nucléaire, notamment à la Convention sur la protection physique des matières nucléaires telle qu'amendée, à la Convention internationale pour la répression des actes de terrorisme nucléaire, aux résolutions 1373 et 1540 du Conseil de sécurité des Nations Unies et au Code de conduite sur la sûreté et la sécurité des sources radioactives, et elles les complètent.

Les publications de la collection Sécurité nucléaire de l'AIEA se répartissent entre les catégories suivantes :

- Les **Fondements de la sécurité nucléaire**, qui portent sur les objectifs et les éléments essentiels d'un régime national de sécurité nucléaire. Ils servent de base à l'élaboration des recommandations en matière de sécurité nucléaire.
- Les **Recommandations en matière de sécurité nucléaire**, qui prévoient des mesures que les États devraient prendre pour établir et maintenir un régime national de sécurité nucléaire efficace conforme aux Fondements de la sécurité nucléaire.
- Les **Guides d'application**, qui fournissent des orientations sur les moyens dont disposent les États Membres pour appliquer les mesures prévues dans les Recommandations en matière de sécurité nucléaire. À ce titre, ils s'intéressent à la mise en application des recommandations relatives à de grands domaines de la sécurité nucléaire.
- Les **Orientations techniques**, qui fournissent des orientations sur des sujets techniques particuliers et complètent les orientations figurant dans les Guides d'application. Elles exposent de manière détaillée comment mettre en œuvre les mesures nécessaires.

D'autres publications sur la sécurité nucléaire, qui ne contiennent pas d'orientations de l'AIEA, paraissent en dehors de la collection Sécurité nucléaire de l'AIEA.

PUBLICATIONS CONNEXES

L'AIEA établit également des normes de sûreté destinées à protéger la santé et à réduire au minimum les dangers auxquels sont exposés les personnes et les biens, qui paraissent dans la collection **Normes de sûreté de l'AIEA**.

L'AIEA prend des dispositions pour l'application des orientations et des normes, et favorise l'échange d'informations sur les activités nucléaires pacifiques et sert d'intermédiaire entre ses États Membres à cette fin.

Les rapports sur la sûreté et la protection dans le cadre des activités nucléaires sont publiés dans la collection **Rapports de sûreté**. Ils donnent des exemples concrets et proposent des méthodes détaillées à l'appui des normes de sûreté.

Les autres publications de l'AIEA concernant la sûreté paraissent dans les collections **Préparation et conduite des interventions d'urgence**, **Rapports techniques** et **TECDOC**. L'AIEA édite aussi des rapports sur les accidents radiologiques, des manuels de formation et des manuels pratiques, ainsi que d'autres publications spéciales concernant la sûreté et la sécurité.

La collection **Énergie nucléaire de l'AIEA** est constituée de publications informatives dont le but est d'encourager et de faciliter le développement et l'utilisation pratique de l'énergie nucléaire à des fins pacifiques, ainsi que la recherche dans ce domaine. Elle comprend des rapports et des guides sur l'état de la technologie et sur ses avancées, ainsi que sur des données d'expérience, des bonnes pratiques et des exemples concrets dans les domaines de l'électronucléaire, du cycle du combustible nucléaire, de la gestion des déchets radioactifs et du déclassement.

CONDUITE DES ÉVALUATIONS DE LA SÉCURITÉ INFORMATIQUE DANS LES INSTALLATIONS NUCLÉAIRES

Les États ci-après sont Membres de l'Agence internationale de l'énergie atomique :

AFGHANISTAN
AFRIQUE DU SUD
ALBANIE
ALGÉRIE
ALLEMAGNE
ANGOLA
ANTIGUA-ET-BARBUDA
ARABIE SAOUDITE
ARGENTINE
ARMÉNIE
AUSTRALIE
AUTRICHE
AZERBAÏDJAN
BAHAMAS
BAHREÏN
BANGLADESH
BARBADE
BÉLARUS
BELGIQUE
BELIZE
BÉNIN
BOLIVIE, ÉTAT PLURINATIONAL DE
BOSNIE-HERZÉGOVINE
BOTSWANA
BRÉSIL
BRUNÉI DARUSSALAM
BULGARIE
BURKINA FASO
BURUNDI
CAMBODGE
CAMEROUN
CANADA
CHILI
CHINE
CHYPRE
COLOMBIE
CONGO
CORÉE, RÉPUBLIQUE DE
COSTA RICA
CÔTE D'IVOIRE
CROATIE
CUBA
DANEMARK
DJIBOUTI
DOMINIQUE
ÉGYPTE
EL SALVADOR
ÉMIRATS ARABES UNIS
ÉQUATEUR
ÉRYTHRÉE
ESPAGNE
ESTONIE
ÉTATS-UNIS D'AMÉRIQUE
ÉTHIOPIE
FÉDÉRATION DE RUSSIE
FIDJI
FINLANDE
FRANCE
GABON
GÉORGIE
GHANA
GRÈCE
GUATEMALA
GUYANA
HAÏTI
HONDURAS
HONGRIE
ÎLES MARSHALL
INDE
INDONÉSIE
IRAN, RÉP. ISLAMIQUE D'
IRAQ
IRLANDE
ISLANDE
ISRAËL
ITALIE
JAMAÏQUE
JAPON
JORDANIE
KAZAKHSTAN
KENYA
KIRGHIZISTAN
KOWEÏT
LESOTHO
LETTONIE
L'EX-RÉPUBLIQUE YOUGOSLAVE DE MACÉDOINE
LIBAN
LIBÉRIA
LIBYE
LIECHTENSTEIN
LITUANIE
LUXEMBOURG
MADAGASCAR
MALAISIE
MALAWI
MALI
MALTE
MAROC
MAURICE
MAURITANIE
MEXIQUE
MONACO
MONGOLIE
MONTÉNÉGRO
MOZAMBIQUE
MYANMAR
NAMIBIE
NÉPAL
NICARAGUA
NIGER
NIGERIA
NORVÈGE
NOUVELLE-ZÉLANDE
OMAN
OUGANDA
OUZBÉKISTAN
PAKISTAN
PALAOS
PANAMA
PAPOUASIE-NOUVELLE-GUINÉE
PARAGUAY
PAYS-BAS
PÉROU
PHILIPPINES
POLOGNE
PORTUGAL
QATAR
RÉPUBLIQUE ARABE SYRIENNE
RÉPUBLIQUE CENTRAFRICAINE
RÉPUBLIQUE DE MOLDOVA
RÉPUBLIQUE DÉMOCRATIQUE DU CONGO
RÉPUBLIQUE DÉMOCRATIQUE POPULAIRE LAO
RÉPUBLIQUE DOMINICAINE
RÉPUBLIQUE TCHÈQUE
RÉPUBLIQUE-UNIE DE TANZANIE
ROUMANIE
ROYAUME-UNI DE GRANDE-BRETAGNE ET D'IRLANDE DU NORD
RWANDA
SAINT-MARIN
SAINT-SIÈGE
SÉNÉGAL
SERBIE
SEYCHELLES
SIERRA LEONE
SINGAPOUR
SLOVAQUIE
SLOVÉNIE
SOUDAN
SRI LANKA
SUÈDE
SUISSE
SWAZILAND
TADJIKISTAN
TCHAD
THAÏLANDE
TOGO
TRINITÉ-ET-TOBAGO
TUNISIE
TURKMÉNISTAN
TURQUIE
UKRAINE
URUGUAY
VANUATU
VENEZUELA, RÉP. BOLIVARIENNE DU
VIET NAM
YÉMEN
ZAMBIE
ZIMBABWE

Le Statut de l'Agence a été approuvé le 23 octobre 1956 par la Conférence sur le Statut de l'AIEA, tenue au Siège de l'Organisation des Nations Unies, à New York ; il est entré en vigueur le 29 juillet 1957. L'Agence a son Siège à Vienne. Son principal objectif est « de hâter et d'accroître la contribution de l'énergie atomique à la paix, la santé et la prospérité dans le monde entier ».

CONDUITE DES ÉVALUATIONS DE LA SÉCURITÉ INFORMATIQUE DANS LES INSTALLATIONS NUCLÉAIRES

AGENCE INTERNATIONALE DE L'ÉNERGIE ATOMIQUE
VIENNE, 2017

NOTE CONCERNANT LE DROIT D'AUTEUR

CONDUITE DES ÉVALUATIONS DE LA SÉCURITÉ INFORMATIQUE DANS LES INSTALLATIONS NUCLÉAIRES

IAEA-TDL-006
ISBN 978-92-0-206517-8

Imprimé par l'AIEA en Autriche, Décembre 2017

AVANT-PROPOS

La sécurité nucléaire a pour but de prévenir les actes malveillants mettant en jeu des matières nucléaires, d'autres matières radioactives ou des installations et activités associées, de les détecter et d'intervenir s'il s'en produit. Les ordinateurs, les systèmes informatiques et les composants numériques jouent un rôle de plus en plus important dans la gestion des informations sensibles, la sûreté nucléaire, la sécurité nucléaire ainsi que la comptabilité et le contrôle des matières dans ces installations. Une compromission des systèmes informatiques pourrait nuire à la sécurité nucléaire, tant directement qu'indirectement, et favoriser des actes malveillants.

La collection Sécurité nucléaire de l'AIEA est consacrée aux questions de sécurité nucléaire relatives à la prévention des actes malveillants mettant en jeu des matières nucléaires, d'autres matières radioactives ou des installations associées, y compris le vol, le sabotage, l'accès non autorisé et le transfert illégal, à leur détection et aux interventions s'il s'en produit. À l'appui des orientations faisant l'objet d'un consensus international qu'elle publie dans sa collection Sécurité nucléaire, l'AIEA produit également des publications donnant des conseils d'experts supplémentaires sur des sujets particuliers.

Le n° 17 de la collection Sécurité nucléaire de l'AIEA, intitulé « La sécurité informatique dans les installations nucléaires », donne des orientations concernant l'établissement d'un programme de sécurité informatique dans une installation nucléaire ou radiologique. En se fondant sur les orientations fournies dans le n° 17 de la collection Sécurité nucléaire de l'AIEA, la présente publication expose une méthodologie pour la conduite des évaluations de la sécurité informatique dans les installations nucléaires. Pour protéger les ordinateurs et les actifs informatiques, il est essentiel de procéder périodiquement à de telles évaluations et, le cas échéant, de mettre en œuvre des mesures correctives sans délai. La méthodologie décrite ici peut être appliquée à la fois pour les autoévaluations internes et les évaluations externes. La présente publication est destinée à être utilisée par les évaluateurs pour la planification et la conduite d'évaluations sur mesure de différents organismes et installations.

Elle a été établie avec le concours de plus de 30 experts lors de trois réunions de consultation et d'un certain nombre de réunions d'experts supplémentaires, et plus de dix États Membres y ont contribué.

NOTE DE L'ÉDITEUR

La présente publication a été élaborée à partir de documents originaux soumis par les personnes ayant contribué à sa rédaction. Elle n'a pas été éditée par l'équipe rédactionnelle de l'AIEA. Les opinions exprimées relèvent de la responsabilité de ces personnes et ne représentent pas nécessairement celles de l'AIEA ni de ses États Membres.

Ni l'AIEA ni ses États Membres n'assument une quelconque responsabilité pour les conséquences éventuelles de l'utilisation de la présente publication. La présente publication ne traite pas des questions de la responsabilité, juridique ou autre, résultant d'actes ou omissions imputables à une quelconque personne.

L'emploi d'appellations particulières pour désigner des pays ou des territoires n'implique de la part de l'éditeur, l'AIEA, aucune prise de position quant au statut juridique de ces pays ou territoires, ou de leurs autorités et institutions, ni quant au tracé de leurs frontières.

La mention de noms de sociétés ou de produits particuliers (qu'ils soient ou non signalés comme marques déposées) n'implique aucune intention d'empiéter sur des droits de propriété et ne doit pas être considérée non plus comme valant approbation ou recommandation de la part de l'AIEA.

Les termes relatifs à la sécurité ont le sens donné dans la publication où ils figurent, ou dans les orientations de niveau supérieur que la publication soutient. Autrement, les termes ont le sens qui leur est communément donné.

Un appendice est réputé faire partie intégrante de la publication. Les informations données dans un appendice ont le même statut que le corps du texte. Les annexes ont pour objet de donner des exemples concrets ou des précisions ou explications. Elles ne sont pas considérées comme faisant partie intégrante du texte principal.

L'AIEA n'assume aucune responsabilité quant à la persistance ou à l'exactitude des adresses URL de sites Internet externes ou de tiers mentionnées dans la présente publication et ne peut garantir que le contenu desdits sites est ou demeurera exact ou approprié.

SOMMAIRE

1. INTRODUCTION 1
1.1. Contexte 1
1.2. Objet 1
1.3. Champ d'application 2
1.4. Structure 3

2. APERÇU GÉNÉRAL DE LA MÉTHODOLOGIE ET DU PROCESSUS D'ÉVALUATION 5
2.1. Objectifs 5
2.2. Considérations relatives à la réglementation 5
2.3. Processus d'évaluation 6
2.4. Domaines d'évaluation 7
2.5. Techniques d'évaluation 9
2.6. Extensibilité 12
2.7. Considérations relatives à la sécurité de l'information 12

3. ACTIVITÉS PRÉPARATOIRES 14
3.1. Champ de l'examen 14
3.2. Réunion préparatoire 14
3.3. Obligations de l'hôte 15
3.4. Constitution de l'équipe 16
3.5. Réunion de l'équipe préalablement à l'évaluation 19
3.6. Calendrier de l'évaluation 19

4. MÉTHODOLOGIE D'ÉVALUATION 21
4.1. Aperçu général de la méthodologie 21
4.2. Évaluation du programme général de sécurité informatique 21
4.3. Matrice d'évaluation 23

5. ORIENTATIONS POUR L'ÉVALUATION PAR DOMAINE DE SÉCURITÉ 27
5.1. Aperçu général 27
5.2. Politique de sécurité 27
5.3. Gestion de la sécurité informatique 28
5.4. Gestion des actifs 30
5.5. Sécurité des ressources humaines 32
5.6. Protection physique 34
5.7. Gestion des communications et des opérations informatiques 36
5.8. Contrôles des accès aux ordinateurs 39
5.9. Acquisition, développement et maintenance des systèmes informatiques 42
5.10. Gestion des incidents de sécurité informatique 43
5.11. Gestion de la continuité 45
5.12. Conformité 47

6. RAPPORT FINAL ET ACTIVITÉS POST-ÉVALUATION 49
6.1. Élaboration du rapport final 49
6.2. Éléments pour l'établissement du rapport 51
6.3. Réunion de clôture 52

RÉFÉRENCES 53

GLOSSAIRE 55

ANNEXE I INDICATIONS POUR L'ÉVALUATION DES SYSTÈMES DE CONTRÔLE-COMMANDE 57

ANNEXE II MODÈLE POUR LES OBSERVATIONS 63

ANNEXE III MODÈLE POUR LE RAPPORT FINAL 66

ANNEXE IV CONSIDÉRATIONS RELATIVES À L'EXAMEN DES RÉSULTATS DU RAPPORT 68

1. INTRODUCTION

1.1. CONTEXTE

Il est de plus en plus admis que la sécurité informatique est un élément essentiel de la sécurité nucléaire. Avec les progrès de la technologie, le recours aux ordinateurs et aux systèmes informatiques dans tous les aspects de l'exploitation des centrales, y compris les systèmes de sûreté et de sécurité, devrait s'accroître. Le n° 20 de la collection Sécurité nucléaire, intitulé « Objectif et éléments essentiels du régime de sécurité nucléaire d'un État », souligne l'importance des activités d'assurance de la cybersécurité menées pour déterminer les problèmes et les facteurs susceptibles de nuire à la capacité d'assurer une sécurité nucléaire adéquate et pour y remédier [1]. Il est aussi question de cela dans le n° 13 de la collection Sécurité nucléaire, intitulé « Recommandations de sécurité nucléaire sur la protection physique des matières nucléaires et des installations nucléaires (INFCIRC/225/Révision 5) » [2], dans lequel il est dit ceci :

> « Les systèmes informatisés utilisés pour la protection physique, la sûreté nucléaire et la comptabilité et le contrôle des matières nucléaires devraient être protégés contre la compromission (cyberattaque, manipulation ou falsification, par exemple) conformément à l'évaluation de la menace ou à la menace de référence. » (Réf. [2], par. 4.10/5.19)

Un processus d'évaluation rigoureux et exhaustif peut aider à renforcer l'efficacité du programme de sécurité informatique d'une l'installation (et de l'État). Le n° 17 de la collection Sécurité nucléaire, intitulé « La sécurité informatique dans les installations nucléaires » [3], fournit des orientations au sujet de l'élaboration et de la gestion d'un tel programme. De nombreuses autres publications sont consacrées à la sécurité de l'information et des ordinateurs et à la conduite des audits/évaluations, par exemple :

- La suite ISO/CEI 27000 [4–8] pour la gestion de la sécurité de l'information ;
- La norme ISO 19011:2011 [9], qui fournit un cadre pour les audits ;
- La publication spéciale 800–115 du NIST, intitulée « Technical Guide to Information Security Testing and Assessment » [10].

La présente publication a été rédigée pour répondre à la nécessité d'orientations spécifiques au domaine nucléaire qui soient conformes aux normes internationales, aux orientations de l'Agence internationale de l'énergie atomique (AIEA) et à la bonne pratique reconnue.

1.2. OBJET

La présente publication expose une méthodologie pour la conduite des évaluations de la sécurité informatique dans les installations nucléaires. Cette méthodologie peut aisément être adaptée pour les évaluations dans les installations contenant d'autres matières radioactives.

Les orientations ont été rédigées de manière à pouvoir être appliquées dans de multiples contextes, par exemple aux fins :

- D'une mission de service consultatif spéciale sur la sécurité informatique organisée par l'AIEA à la demande d'un État Membre ;
- De la sécurité informatique en tant que module spécial d'autres missions organisées par l'AIEA, par exemple d'une mission du Service consultatif international sur la protection physique (IPPAS) pour laquelle le sujet de l'évaluation est le domaine de la protection physique ;

— Des évaluations effectuées par une autorité compétente nationale sur des sites et dans des installations de l'État ;
— Des autoévaluations effectuées au niveau d'une installation ou d'un organisme ;
— D'une évaluation de la sécurité informatique des vendeurs et des tiers qui fournissent un appui à des installations nucléaires.

Cette méthodologie permet d'évaluer les pratiques en vigueur dans une installation en vue de renforcer l'organisme et ses procédures et pratiques. Elle tient compte des orientations de l'AIEA sur la sécurité nucléaire, des normes internationales et de la bonne pratique bénéficiant du soutien de la communauté internationale. Sa structure est celle d'un examen de haut niveau du cadre de sécurité informatique qui comporte une analyse fonctionnelle des mesures et procédures en place pour la mise en œuvre de ce cadre, une attention particulière étant accordée aux fonctions de sûreté et de sécurité nucléaires remplies par les systèmes informatiques.

Il peut être nécessaire d'adapter chaque évaluation aux besoins et d'en cerner clairement les résultats escomptés. Dans le cas, par exemple, d'une évaluation effectuée par une autorité compétente, les résultats escomptés pourront être constitués par un rapport sur la façon dont l'exploitant s'est conformé à ses obligations réglementaires et juridiques. Ce rapport ne proposera vraisemblablement pas de pistes de solution, mais il pourra demander que des mesures soient prises conformément aux priorités fixées par l'autorité compétente ainsi qu'une évaluation de suivi. À l'inverse, il peut être demandé à une équipe consultative effectuant une évaluation de recommander des solutions possibles tout en dressant la liste de ses constatations. Il est en outre probable que les équipes consultatives se pencheront sur les priorités et les activités de suivi ; il se peut aussi que dans le champ de l'évaluation il soit stipulé que l'équipe d'évaluation et l'hôte collaborent dans la conduite de l'analyse et l'élaboration d'un plan d'action.

Il est important que les objectifs et les résultats escomptés de l'évaluation soient énoncés et convenus clairement lors de la réunion préparatoire.

La présente publication a avant tout pour objet d'aider une équipe d'évaluation à établir un plan d'évaluation adapté à une installation particulière. Elle n'est pas destinée à constituer une liste de contrôle complète en soi, mais compte plutôt sur l'expérience de l'équipe d'évaluation pour qu'elle utilise ces orientations de façon que son examen soit très complet et effectué conformément aux buts de l'évaluation et aux ressources allouées.

1.3. CHAMP D'APPLICATION

La présente publication est axée sur l'évaluation de la pratique en matière de sécurité nucléaire dans les installations nucléaires de tous types, telles que les centrales nucléaires, les installations du cycle du combustible, les réacteurs de recherche, etc. Bien que la gestion des autres matières radioactives, le transport et les opérations associées ne soient pas traités explicitement dans la présente publication, les principes et les processus décrits ici peuvent aisément être adaptés à l'évaluation de ces activités.

La présente publication porte exclusivement sur les aspects de la sécurité de l'information qui ont trait aux ordinateurs. Elle ne traite pas, par exemple, des prescriptions concernant la classification, le marquage et le traitement des informations.

L'évaluation se fonde sur des examens, des entretiens et des observations et ne comporte normalement pas d'essais actifs d'un système. En particulier, l'évaluation décrite en détail dans les présentes orientations ne comporte pas de test d'intrusion ou de connexion de

dispositifs d'essai au système. Les membres de l'équipe d'évaluation ne feront pas fonctionner des équipements sur le site de l'évaluation, mais l'équipe peut demander à consulter les journaux ou les fichiers de configuration de systèmes actifs sur un système de production en service. Au besoin et dans les limites du champ de l'évaluation, l'équipe d'évaluation demandera à l'installation d'effectuer des tâches opérationnelles particulières, et des tests actifs pourront être exécutés dans le cadre d'une autoévaluation ou de services fournis sur demande par un organisme extérieur. Les tests actifs sur tout système de production en service doivent être effectués avec le plus grand soin.

La méthodologie décrite dans la présente publication a été conçue pour une situation idéale dans laquelle une équipe de trois ou quatre évaluateurs peut séjourner sur place pendant une à deux semaines pour effectuer l'évaluation. Toutefois, la façon dont la méthodologie pourrait être adaptée si des contraintes de temps et de ressources ne permettent pas un tel niveau d'effort est également prise en considération.

1.4. STRUCTURE

La présente publication consiste en un aperçu général de la méthodologie suivi d'orientations détaillées pour les diverses étapes de l'évaluation. Elle comprend les sections suivantes :

- La section 2 donne un aperçu général de la méthodologie d'évaluation en décrivant les grandes étapes qui pourraient être suivies.
- La section 3 décrit plus en détail les activités préparatoires qui pourraient être menées préalablement à une évaluation.
- La section 4 précise la méthodologie d'évaluation.
- La section 5 fournit des orientations détaillées sur la conduite de l'évaluation, et notamment des exemples de questions à poser et d'informations à examiner au cours du processus.
- La section 6 porte sur les activités qui seraient menées en général lors de la clôture et du suivi de l'évaluation.
- L'annexe I donne des indications et expose la bonne pratique pour la conduite d'évaluations portant sur des systèmes de contrôle industriel.
- L'annexe II fournit un modèle pour la prise de notes sur le terrain par les membres de l'équipe.
- L'annexe III fournit un modèle pour le rapport final.
- L'annexe IV énumère les considérations à prendre en compte par l'organisme hôte lors de l'examen des résultats du rapport.

La figure 1 indique les grandes étapes de la planification de l'évaluation et le calendrier prévu.

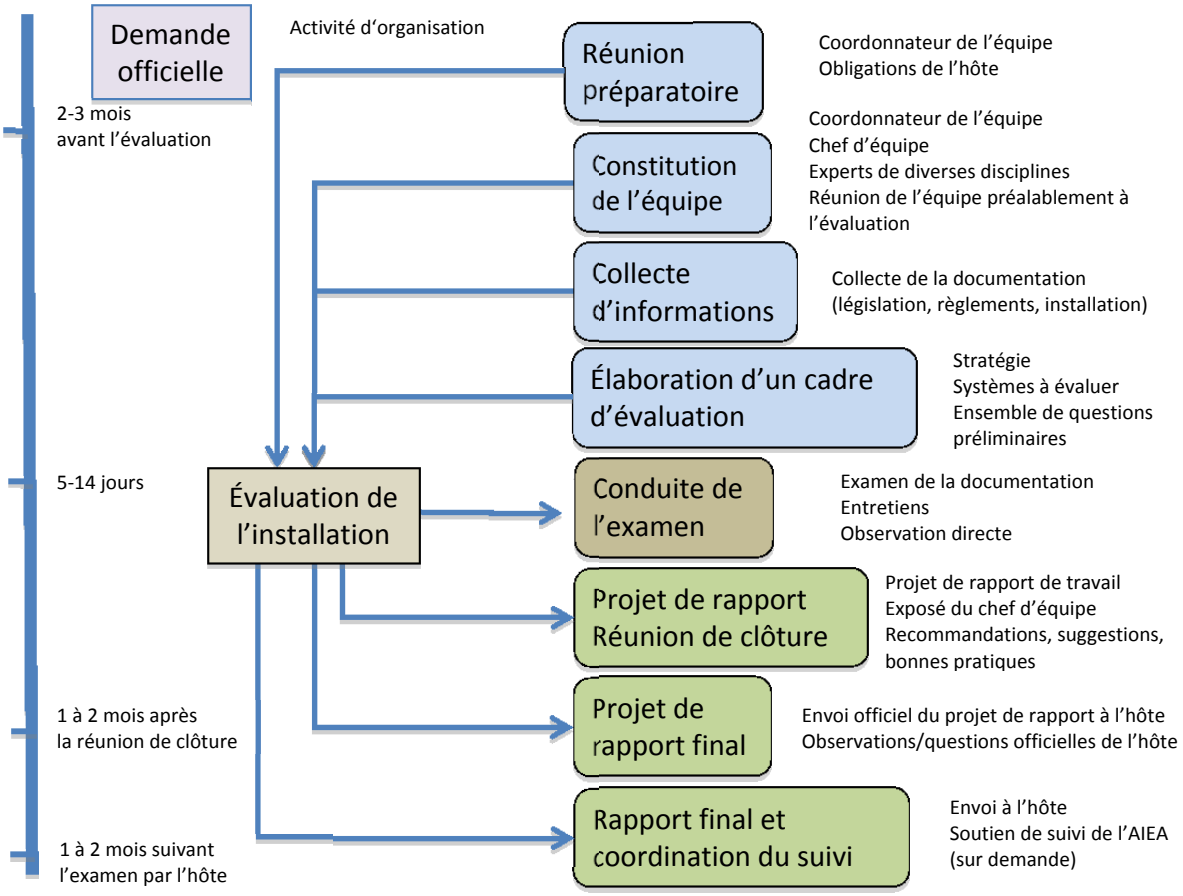

FIG. 1. Étapes et calendrier de l'évaluation. Le calendrier peut être ajusté en fonction des contraintes de ressources et de temps.

2. APERÇU GÉNÉRAL DE LA MÉTHODOLOGIE ET DU PROCESSUS D'ÉVALUATION

2.1. OBJECTIFS

Cette méthodologie d'évaluation a pour objectif d'aider les États Membres et les exploitants à instaurer, mettre en œuvre, maintenir et, s'il y a lieu, renforcer la sécurité informatique de leurs installations, ainsi que leurs autorités compétentes à évaluer l'efficacité des mesures prises. La présente publication donne des orientations de haut niveau pour la conception et la conduite d'une évaluation dans des installations nucléaires ou d'autres installations contenant des matières radioactives, mais elle n'est pas censée fournir une liste de contrôle complète pour la conduite de l'évaluation. Elle a principalement pour objet de donner des conseils à une partie ou à l'ensemble :

— Des exploitants d'installations sur la façon dont leur programme de sécurité informatique peut leur permettre de faire face aux cybermenaces pertinentes et de le structurer pour l'adapter à l'évolution de celles-ci ;

— Des autorités nationales sur la façon de traduire les recommandations internationales en prescriptions précises concernant le système de sécurité informatique de l'État pour les installations contenant des matières nucléaires ou d'autres matières radioactives ;

— Des exploitants d'installations au sujet des diverses méthodes permettant de se conformer aux recommandations internationales et à la bonne pratique ;

— Des autorités nationales compétentes et des exploitants d'installations sur la façon de procéder à une évaluation objective de l'état de leur cadre de sécurité informatique et de la mise en œuvre des orientations internationales et de la bonne pratique ;

— Des principaux membres du personnel de l'autorité compétente nationale et des exploitants d'installations en leur offrant l'occasion de se pencher sur leur pratique avec des experts ayant l'expérience de la pratique suivie ailleurs dans le même domaine ;

— Des spécialistes de la sécurité informatique des États Membres en leur offrant des possibilités d'élargir leur expérience et leurs connaissances dans leur domaine de compétence.

L'évaluation peut en outre servir à déterminer la bonne pratique qui pourrait alors être portée à la connaissance d'autres installations et/ou États Membres aux fins de leur amélioration à long terme.

2.2. CONSIDÉRATIONS RELATIVES À LA RÉGLEMENTATION

La présente publication peut servir de guide de référence aux autorités compétentes dans l'exécution de leurs évaluations sur site de la sécurité informatique. En outre, l'autorité compétente peut reconnaître à une installation le mérite d'avoir procédé à une autoévaluation ou exiger que des autoévaluations soient effectuées périodiquement. L'autorité compétente peut demander qu'une évaluation du site soit effectuée par une entité indépendante et/ou un tiers.

Le processus préparatoire définit les normes et règlements particuliers à utiliser pour parvenir aux constatations, aux recommandations et aux suggestions. L'autorité compétente peut demander les informations ci-après dans le cadre de l'évaluation et du rapport final :

— Liste des constatations ;
— Plan d'action de l'installation pour donner suite aux constatations, y compris les mesures et les délais ;
— Preuve qu'il existe un système de traçage permettant de contrôler et de surveiller la suite donnée aux différentes constatations ;
— Au besoin, rapports périodiques sur la situation en ce qui concerne les mesures prises pour donner suite à des constatations particulières.

L'autorité compétente peut utiliser ces résultats d'inspection comme point de départ pour des inspections futures sur site.

2.3. PROCESSUS D'ÉVALUATION

Les éléments et le schéma du processus d'évaluation sont illustrés dans la fig. 2. Ce processus sera examiné en détail.

La présente publication fournit des orientations et des recommandations concernant la façon de planifier une évaluation et de constituer une équipe d'évaluation. Une bonne évaluation suppose l'allocation de ressources adéquates, une solide équipe d'évaluation et une coopération de la part de l'installation.

La présente publication indique ensuite des domaines d'évaluation représentatifs et fournit des orientations pour la collecte d'informations sur la base du concept des domaines fonctionnels et des domaines de sécurité. L'équipe d'évaluation crée un cadre d'évaluation — plan d'évaluation systématique de l'installation — conforme aux objectifs de planification, aux orientations de l'AIEA, aux normes de l'industrie, aux guides réglementaires, à la bonne pratique, etc. Nous ne fournissons pas de liste de contrôle particulière pour cela, étant donné que chaque évaluation est unique et doit être adaptée individuellement.

Suivant la nature de l'évaluation et le temps disponible, les membres de l'équipe d'évaluation pourront ajuster le champ de l'évaluation à la situation et aux exigences particulières de l'installation. Une évaluation approfondie de tous les aspects de la sécurité informatique relevant du champ de l'évaluation doit être envisagée afin de porter un jugement en connaissance de cause sur l'état actuel du programme de sécurité informatique.

Lors de la conduite d'une évaluation, l'équipe doit rassembler suffisamment d'informations pour évaluer les pratiques de l'installation en matière de sécurité informatique au niveau pertinent. Les orientations fournissent des indications pour le rassemblement des informations ainsi que des recommandations sur les points essentiels.

L'équipe d'évaluation doit faire preuve de sens critique dans l'évaluation du cadre de sécurité informatique de l'installation, et son jugement doit se fonder sur des observations étayées et non sur des hypothèses. L'équipe peut aussi recommander et suggérer des améliorations et prendre acte de la bonne pratique de l'installation. Il est important que l'équipe admette que diverses approches de la mise en œuvre de la sécurité peuvent être acceptables (sauf si l'autorité compétente a imposé une approche particulière).

L'évaluation donne lieu à un rapport final et, normalement, à une réunion de clôture. Outre qu'il contient les constatations faites durant l'évaluation, le rapport d'évaluation formule des recommandations ou des suggestions susceptibles de contribuer à l'amélioration des systèmes ou des processus examinés. Le rapport peut aussi examiner l'impact des constatations sur la

sécurité et la sûreté générales de l'installation. Il est recommandé de déterminer la bonne pratique et de la porter à la connaissance d'autres installations et/ou États Membres.

Lors de la réunion de clôture, le chef d'équipe présentera les constatations de l'évaluation et, en particulier, les recommandations et suggestions éventuelles. Il est important que le chef d'équipe définisse le contexte des constatations et de toute information connexe pertinente. Il est conseillé de présenter toujours les résultats, en particulier les « rapports gradués », avec leur contexte et leur justification.

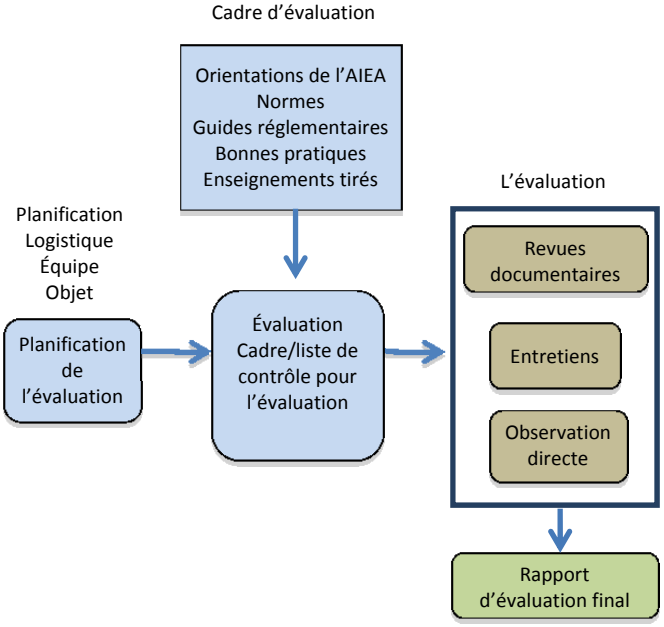

Fig.2. Composantes de l'évaluation.

2.4. DOMAINES D'ÉVALUATION

L'approche de l'évaluation de la sécurité informatique comporte deux éléments fondamentaux : un examen du programme général de sécurité informatique et un ou plusieurs examens au niveau de systèmes. L'évaluation donne un aperçu instantané des pratiques de l'installation en matière de sécurité informatique. Le concept exposé dans la présente publication conduit à un examen interdomaines à la fois des opérations fonctionnelles de l'installation et de sa sécurité informatique. Il aide ainsi à assurer la prise en considération des processus et des systèmes qui remplissent les principales fonctions, à savoir notamment les opérations, l'activité commerciale, la sûreté, la sécurité et les interventions d'urgence.

2.4.1. Domaines fonctionnels

D'une manière générale, les systèmes informatiques des installations nucléaires peuvent être associés à un ou plusieurs des cinq domaines fonctionnels décrits dans la présente section. L'évaluation peut être conçue pour couvrir un ou plusieurs de ces domaines fonctionnels (voir la section 2.6 sur l'extensibilité pour plus de précisions). Une évaluation complète de la sécurité informatique couvrirait l'ensemble des cinq domaines :

i. Domaine des opérations : systèmes informatiques utilisés pour faire fonctionner l'entité évaluée. Ceux-ci comprennent les systèmes d'instrumentation, de commande et d'acquisition de données. Les autres systèmes à prendre en considération sont ceux qui sont nécessaires au fonctionnement de l'installation proprement dite, à savoir les systèmes de chauffage, de refroidissement, de ventilation, d'éclairage et d'ascenseurs.

ii. Domaine de l'activité commerciale : systèmes informatiques utilisés pour la gestion et l'activité commerciale de l'entité. Le système d'autorisation de tâches en offre un exemple typique. Dans le domaine commercial, les systèmes sont généralement connectés à des réseaux externes qui pourraient également être importants pour d'autres domaines.

iii. Domaine de la sûreté : systèmes informatiques qui sont vitaux pour assurer la sûreté des installations et la protection des personnes et de l'environnement contre les risques radiologiques et les activités qui pourraient donner lieu à de tels risques. Ces systèmes comprennent, par exemple, les systèmes de protection utilisés pour mettre une centrale nucléaire à l'arrêt.

iv. Domaine de la protection physique : systèmes informatiques utilisés pour protéger et surveiller les matières nucléaires et radiologiques de l'entité. Ces systèmes comprennent les systèmes de contrôle des accès et de protection physique pour la surveillance du périmètre et les systèmes de comptabilité et de contrôle des matières nucléaires.

v. Domaine des interventions d'urgence : systèmes informatiques utilisés pour la détection, l'intervention et l'atténuation en cas d'incident menaçant la sûreté du public, sa santé et l'environnement. Ces systèmes informatiques peuvent, par exemple, être utilisés pour le contrôle radiologique et environnemental, l'alarme incendie et la lutte contre les incendies ainsi que les communications en cas d'urgence.

2.4.2. Domaines de sécurité

Les domaines de sécurité sont ceux sur lesquels l'examen de la sécurité informatique met fortement l'accent. Ils aident l'équipe évaluant un domaine fonctionnel en ciblant globalement leur examen des pratiques en matière de sécurité. Il s'agit de domaines adaptés à partir de ceux qui sont décrits dans la norme ISO/CEI 27002 [6]. Ces domaines sont les suivants :

i. Politique de sécurité ;

ii. Gestion de la sécurité informatique ;

iii. Gestion des actifs ;

iv. Sécurité des ressources humaines ;

v. Protection physique ;

vi. Gestion des communications et des opérations ;

vii. Contrôles des accès aux ordinateurs ;

viii. Acquisition, développement et maintenance des systèmes informatiques ;

ix. Gestion des incidents de sécurité informatique ;

x. Gestion de la continuité ;

xi. Conformité.

Le n° 17 de la collection Sécurité nucléaire de l'AIEA, intitulé « La sécurité informatique dans les installations nucléaires » [3], et la suite ISO/CEI 27000 [4–8] fournissent conjointement une première base pour l'évaluation. Les normes relatives aux systèmes de contrôle industriel, la bonne pratique et les enseignements tirés peuvent également être pris en considération par l'équipe d'évaluation lors de l'établissement de son plan d'évaluation (une liste de contrôle pour l'évaluation, le cas échéant). La section 5 décrit plus en détail chaque domaine de sécurité et fournit des orientations pour son évaluation. L'annexe I cite des exemples d'enseignements tirés de l'évaluation de systèmes de contrôle industriel.

2.5. TECHNIQUES D'ÉVALUATION

Une équipe d'évaluation recourt à l'ensemble ou à certaines des techniques ci-après en vue d'acquérir les informations dont elle a besoin pour formuler ses conclusions et ses recommandations :

- examen de documents et de dossiers, par exemple de la législation, des règlements et de ceux de l'installation.
- entretiens avec le personnel des organismes pertinents, par exemple celui de l'autorité compétente, les opérateurs de l'installation et les représentants d'autres organismes.
- observation directe de l'organisme, de ses pratiques et systèmes ainsi que de la mise en œuvre des mesures de sécurité informatique.

2.5.1. Examen des documents et dossiers

Le processus de collecte d'informations consiste notamment à examiner, étudier ou analyser les documents et les dossiers fournis par l'installation ou rassemblés dans celle-ci. Il a pour objet :

- d'évaluer la conformité des arrangements et de la sécurité informatique aux procédures internes ;
- d'évaluer la conformité aux lois, politiques, prescriptions réglementaires et orientations nationales ;
- de déterminer la compatibilité avec les orientations internationales pertinentes, telles que les orientations de l'AIEA, les normes ISO/CEI et la bonne pratique ;
- de déterminer si les arrangements et les mesures de sécurité informatique correspondent à la bonne pratique établie aux niveaux international et national ;
- d'évaluer la pertinence de l'environnement de sécurité actuel (par exemple la menace de référence) ;
- de déterminer les processus et/ou systèmes à évaluer sur site de manière approfondie dans les domaines fonctionnels retenus/pertinents.

Les documents et dossiers peuvent être les suivants (mais sans s'y limiter) :

- Politique ;
- Procédures ;
- Formulaires de l'entreprise ;
- Guides réglementaires/lois ;
- Rapports d'évaluation précédents (externes, autoévaluations, etc.) ;

— Dossiers (par exemple sur la formation, l'inspection, etc.) ;
— Pages Web (internet et intranet) ;
— Matériels de formation (initiation des nouveaux salariés, sécurité informatique, etc.) ;
— Listes d'inventaire concernant les ordinateurs ;
— Listes de contrôle des accès ;
— Fichiers de configuration ;
— Schémas de réseaux ;
— Schémas de l'installation ;
— Journaux des opérations ;
— Ensembles de règles (par exemple pare-feu, système de détection d'intrusion, routeurs, etc.).

La section 5 énumère les documents et les dossiers qu'il est recommandé d'examiner pour chaque domaine de sécurité et donne des indications permettant de se faire une idée des éléments particuliers à rechercher lors de l'examen des documents par rapport à la bonne pratique.

2.5.2. Entretiens

Les entretiens et les discussions avec des individus ou des groupes de l'installation et/ou de l'autorité concernée fournissent un niveau supplémentaire d'information pour l'évaluation. De fait, s'ils sont bien conduits, ces entretiens constituent peut-être la partie la plus importante de l'évaluation. Après l'examen de la documentation pertinente, des entretiens avec le personnel de l'installation peuvent être menés en vue :

— D'obtenir des informations supplémentaires ;
— De vérifier que les procédures écrites sont comprises et suivies à la lettre ;
— De déterminer les problèmes d'évaluation découlant d'actions ou de séances d'information précédentes ;
— De solliciter des opinions individuelles ;
— De former un jugement concernant la base de connaissances, la formation et les ressources de l'entité évaluée ;
— D'étayer, de confirmer ou de contester les constatations faites au cours de l'observation sur site des mesures de sécurité informatique en place ;
— De déterminer les flux et les processus d'information réels dans l'organisme.

Les entretiens offrent en outre l'occasion aux membres de l'équipe d'évaluation et à leurs contreparties de l'installation d'échanger des informations importantes. Un échange de vues représente souvent la meilleure approche pour un entretien. Une approche confrontationnelle peut ne pas être productive. Au besoin, un interprète peut être fourni afin d'éviter les problèmes de communication. Il faut choisir avec soin le personnel approprié pour les entretiens afin d'assurer un échange d'informations au niveau voulu. Par exemple, la direction ne sera pas nécessairement en mesure de traiter des processus de mise en œuvre technique. Le personnel recommandé pour les entretiens comprend les personnes suivantes (mais sans s'y limiter) :

i. Direction

— Chef de site ;
— Responsable(s) de l'installation ;
— Responsable de la sécurité ;
— Responsable de la sûreté ;
— Responsable(s) de la sécurité de l'information/des ordinateurs/de la TI ;
— Chef de la technologie de l'information ;
— Responsable des RH ;
— Responsable des opérations d'urgence ;
— Autres responsables, selon qu'il convient.

ii. Spécialistes techniques

— Administrateurs de systèmes ;
— Superviseur de la maintenance contrôle-commande ;
— Ingénieur système (pour chaque système retenu) ;
— Opérateurs techniques.

iii. Autres membres du personnel

— Personnel d'assurance de la qualité ;
— Opérateurs de pupitres.

Avant l'entretien, l'équipe d'évaluation doit avoir préparé une première série de questions ou de thèmes de discussion. Des questions bien formulées peuvent aider à évaluer :

— La connaissance et le respect de la politique et des procédures ;
— La formation et l'efficacité de la sécurité ;
— L'éducation et la sensibilisation à la sécurité ;
— La perception de la menace et des risques ;
— La capacité d'intervention en cas d'incident ;
— La clarté des rôles et des responsabilités ;
— L'efficacité de la culture de sécurité ;
— La détermination et la notification des problèmes ;
— Les mesures de confidentialité ;
— L'application de la bonne pratique ;
— Le choix des mesures et des solutions techniques à mettre en place.

Plus particulièrement, un questionnement efficace peut permettre de :

— Clarifier les questions découlant de l'examen des documents rassemblés ;
— Vérifier que le personnel chargé ou responsable de la mise en œuvre des procédures comprend les politiques de sécurité qui y sont associées ;
— Vérifier que le personnel comprend les procédures de mise en œuvre et est formé et qualifié comme il se doit pour s'acquitter de ses fonctions et/ou activités.

Les entretiens ouverts et dynamiques laissant la possibilité de poser des questions en sus de celles qui sont prédéfinies et d'échanger des informations de manière spontanée sont encouragés.

La section 5 contient, pour chaque domaine de sécurité, des exemples de questions que l'équipe d'évaluation pourra utiliser et adapter à ses besoins particuliers.

2.5.3. Observation directe

L'observation directe des mesures de sécurité informatique et de la mise en œuvre des procédures dans une installation est un aspect important du processus d'évaluation. Une bonne partie de la période d'évaluation sur site pourra être consacrée à leur observation dans la pratique. Il est suggéré que les observations couvrent l'utilisation des procédures, les plans du site, les instructions, l'établissement de rapports réguliers et particuliers ainsi que les mesures de contrôle de la qualité.

Les activités du site qu'il est recommandé d'observer durant l'évaluation sont notamment les suivantes (mais sans s'y limiter) :

- Gestion de la configuration et des actifs ;
- Durcissement des systèmes ;
- Processus de sécurité ;
- Contrôle des accès physiques et logiques ;
- Séparation des attributions individuelles ;
- Sécurité du personnel ;
- Surveillance et journalisation des événements ;
- Architecture de réseau ;
- Application de la bonne pratique ;
- Inspections visuelles/vérifications des systèmes.

Il est en outre important de se pencher sur l'utilisation éventuelle de contrôles compensatoires lorsqu'un contrôle de sécurité ne peut pas être mis en place et qu'un autre y est substitué pour atteindre le même objectif de sécurité. L'activité observée peut être comparée avec les procédures ou les règles de l'installation, les orientations établies et la bonne pratique de l'industrie. Les observations des membres de l'équipe peuvent servir à juger avec quelle efficacité une installation est capable de mettre en œuvre un programme de sécurité informatique.

La section 5 énumère les activités pertinentes à observer pour chaque domaine de sécurité.

2.6. EXTENSIBILITÉ

La nature de l'évaluation peut être telle qu'il est raisonnable ou souhaitable de la restreindre à certains domaines fonctionnels couverts dans le présent guide. Les orientations données dans la présente publication sont souples et peuvent être modulées en fonction de différentes approches et durées suivant le niveau d'évaluation.

2.7. CONSIDÉRATIONS RELATIVES À LA SÉCURITÉ DE L'INFORMATION

L'évaluation examinera les informations et les actifs d'information sensibles. Les rapports et les documents de travail peuvent contenir des informations sensibles dont la divulgation non autorisée pourrait compromettre la sécurité nucléaire et avoir de graves conséquences. Il est donc impératif que les documents préparatoires, les notes techniques, les projets de rapports et le rapport final soient classifiés, marqués, traités, stockés, transmis et détruits de manière

appropriée conformément aux procédures applicables aux informations sensibles dans l'installation hôte. La question du traitement et de la sécurité de ces informations doit donc être examinée lors de la réunion préparatoire et réglée préalablement à l'évaluation.

Les membres de l'équipe communiquant leurs notes techniques à d'autres membres de l'équipe doivent prendre des précautions particulières pour assurer la sécurité des informations sensibles. Il faut aussi réfléchir avant l'évaluation aux types de dispositifs électroniques ou aux supports de stockage qui seront utilisés pour les prises de notes individuelles et la compilation des projets de rapports et du rapport final.

Il est recommandé de fonder la sécurité de ces documents sur le principe du « besoin d'en connaître »,
c'est-à-dire de restreindre leur accès aux personnes dont l'habilitation et le besoin d'en connaître ont été établis.

Suivant le contexte de l'évaluation, les membres de l'équipe peuvent devoir signer un accord de confidentialité ou de non-divulgation.

3. ACTIVITÉS PRÉPARATOIRES

3.1. CHAMP DE L'EXAMEN

Eu égard au nombre des systèmes informatiques dans les installations nucléaires et à l'étendue des domaines fonctionnels et de sécurité à évaluer, il peut être impossible de procéder à une évaluation complète de l'ensemble du programme de sécurité informatique dans le cadre d'une seule évaluation. L'hôte doit donc commencer par décider du champ et des objectifs de l'évaluation et les expliquer au coordonnateur de l'équipe ou à son chef suivant le cas. La section 4 présente le concept des éléments modulaires pour certains domaines fonctionnels de l'installation. Cette approche permet aux planificateurs de l'évaluation de déterminer les éléments prioritaires pour une évaluation sur mesure.

3.2. RÉUNION PRÉPARATOIRE

La réunion préparatoire, à laquelle participent le coordonnateur et le chef de l'équipe, se tient habituellement deux à trois mois environ avant l'évaluation et dans l'installation hôte afin de permettre à toutes les parties concernées d'y prendre part. Elle devrait aboutir à ce que le processus et la méthodologie d'évaluation, y compris les activités préparatoires, la mécanique du déroulement de l'évaluation et les activités de rapport après l'évaluation, soient compris clairement. Un compte rendu de cette réunion pourra être diffusé.

La réunion examinera :

- Les principaux aspects du programme d'évaluation ;
- L'objectif et le champ de l'évaluation ;
- La forme et le contenu escomptés du rapport ;
- Le champ et le niveau de l'analyse à inclure dans le rapport ;
- Les exigences relatives au traitement et à la sécurité des informations pour le rapport et les notes techniques ;
- La préparation de l'évaluation, y compris une liste des documents requis ;
- La préparation d'un dossier d'information préalable à l'intention de l'équipe d'évaluation ;
- Le soutien logistique requis (par exemple bureau pour l'équipe, imprimante, photocopieuse et transports locaux) ;
- La fourniture de services de traduction/interprétation ;
- Le traitement des documents confidentiels émanant de l'installation considérée ;
- Les procédures à suivre par l'équipe d'évaluation — y compris les mesures qu'elle doit prendre immédiatement et le point de contact de l'organisme hôte qu'elle doit aviser — au cas où l'un quelconque des événements ci-après est décelé :
  - compromission effective ou potentielle d'un système,
  - négligence volontaire,
  - problème de sûreté majeur,
  - problème de sécurité majeur ;
- La mise au point définitive du calendrier d'évaluation ;
- La composition potentielle de l'équipe d'évaluation ;
- Les activités de suivi possibles.

3.3. OBLIGATIONS DE L'HÔTE

L'hôte est considéré comme le parrain de l'activité. Il peut s'agir de la direction d'une installation ou d'un organisme gouvernemental dans le cas de l'examen d'une installation, ou d'un organisme gouvernemental si l'activité d'évaluation est centrée sur un examen au niveau de l'État. Dans le cadre des discussions lors de la réunion préparatoire, le coordonnateur et le chef de l'équipe prendront des dispositions avec l'hôte pour assurer la fourniture des moyens de soutien nécessaires là où aura lieu l'évaluation. Dans le cas d'une mission internationale, les évaluations de la sécurité informatique se déroulent habituellement en anglais. L'hôte doit assurer l'interprétation nécessaire le cas échéant pour que les membres de l'équipe puissent faire leur travail.

Il est important que l'hôte mette à la disposition exclusive de l'équipe un lieu de réunion sécurisé pendant toute la durée de l'évaluation. Ce lieu de réunion sécurisé doit être de dimensions suffisantes pour que l'équipe puisse raisonnablement travailler et tenir des discussions en privé. Un accès internet peut également être souhaité, mais il faut en discuter lors de la réunion préparatoire initiale. Il est recommandé de mettre une imprimante et une photocopieuse à la disposition des membres de l'équipe. Les documents pertinents à examiner lors de la réunion préparatoire doivent être fournis dans une langue convenue entre l'hôte et l'équipe d'évaluation. L'équipe a besoin, pendant la durée de l'évaluation, d'un conteneur, ou d'un local dans lequel des mesures de protection physique supplémentaires sont en place, pour stocker en toute sécurité les documents ou les actifs qui peuvent contenir des informations confidentielles ou sensibles.

Afin de gagner du temps lors de l'évaluation et de permettre aux membres de l'équipe de bien comprendre le contexte de l'évaluation et les prescriptions réglementaires, il est souhaitable que l'hôte fournisse les documents pertinents pour communication aux membres de l'équipe au moins deux mois avant la visite de l'équipe, étant donné que certains documents pourraient ne pas être faciles à obtenir à leur arrivée dans l'installation. Tous les documents émanant de l'hôte devraient être traités comme convenu entre lui et l'équipe.

Suivant le champ de l'évaluation, ces documents pourraient comprendre ce qui suit :

i. Législation nationale :
   - Loi(s) régissant la sécurité informatique des installations nucléaires ; aperçu général des responsabilités et de la structure (avec indications des départements pertinents) des divers organismes gouvernementaux qui s'occupent des questions de sécurité informatique et
     des liens entre eux ;
   - Règlements relatifs à la sécurité informatique des installations nucléaires ;
   - Orientations réglementaires pertinentes concernant les installations nucléaires ;
   - Caractéristiques de la menace de référence.

ii. Organisation et procédures des autorités compétentes :
   - Structure, organisation et effectifs ; description des procédures d'autorisation le cas échéant ;
   - Pratiques en matière d'inspection ;
   - Liste des règlements, guides réglementaires, codes et normes applicables.

iii. Description, organisation et procédures de sécurité informatique de l'installation :
   - Politique générale de sécurité (ou parties pertinentes de celle-ci) ;

— Plans de sécurité informatique ;
— Rôles et responsabilités en matière de sécurité ;
— Programme de formation et de sensibilisation à la sécurité ;
— Inventaire des actifs numériques et description du comment et du pourquoi ces actifs entrent dans le cadre du programme de sécurité informatique de l'installation ;
— Interventions de tiers ;
— Évaluation du risque, y compris une description de la façon dont les contrôles de sécurité sont sélectionnés ;
— Catégorisation des systèmes de sûreté ;
— Procédures de sûreté importantes pour la sécurité ;
— Conception de l'architecture du réseau ;
— Dispositifs frontière entre les domaines du réseau, y compris les politiques concernant la circulation des données pour ces dispositifs ;
— Documentation technique sur les systèmes ;
— Rapports d'évaluation existants (établis par l'installation elle-même ou par un tiers) ;
— Procédures et dossiers concernant les interventions à la suite d'incidents de sécurité informatique ;
— Rapports et mesures correctives pour les incidents de sécurité informatique ;
— Documents sur la gestion de la configuration, y compris les analyses de sécurité associées aux modifications de la configuration.

3.4. CONSTITUTION DE L'ÉQUIPE

3.4.1. Composition de l'équipe

L'équipe peut comprendre un coordonnateur, un chef (s'il y a lieu), trois experts ou plus et, éventuellement, un rédacteur technique pour aider l'équipe à établir les notes techniques et le rapport d'évaluation final. La composition de l'équipe pourra être adaptée en fonction du champ de l'évaluation.

Le coordonnateur ou le chef de l'équipe choisit des experts pour l'équipe, avec l'accord de l'hôte. Ces experts doivent posséder indiscutablement de vastes connaissances et une expérience étendue en matière de sécurité informatique, ainsi qu'une spécialisation dans un ou plusieurs domaines de l'exploitation des centrales, de la sûreté, de la sécurité physique, de la technologie de l'information des installations et de l'ingénierie pour concourir à l'évaluation des domaines fonctionnels. Les membres de l'équipe doivent pouvoir consacrer un certain temps à la préparation, à l'évaluation elle-même et à l'établissement du rapport final. Si un membre au moins de l'équipe connaît bien la conception des installations exploitées par l'hôte, cela facilite l'évaluation.

Il est recommandé en outre que les membres de l'équipe soient choisis de manière à représenter différentes approches de la réglementation et de la mise en œuvre, par exemple de la législation pertinente, de la réglementation des activités nucléaires, de l'exploitation des installations et de l'analyse des systèmes de sécurité informatique. En plus de ses compétences dans son domaine particulier, chaque expert connaîtra sans doute d'autres approches nationales et d'autres domaines pertinents. L'équipe sera ainsi en mesure de fournir la meilleure évaluation et les meilleurs conseils possibles concernant la sécurité informatique.

Un observateur de l'hôte pourra être invité à participer à l'évaluation avec l'équipe. Cela pourra se révéler avantageux en facilitant l'échange d'informations.

3.4.2. Coordonnateur de l'équipe

Le coordonnateur de l'équipe accompagnera celle-ci pendant toute l'évaluation pour assurer la coordination avec les contreparties de l'organisme hôte et fournir le soutien logistique ou autre qui pourra être nécessaire. Dans le cas d'une mission de service consultatif de l'AIEA, le coordonnateur de l'équipe distribuera l'édition la plus récente des documents d'évaluation pertinents et toute autre documentation qui pourra être applicable, en plus des documents fournis à l'avance par le pays hôte, à tous les membres de l'équipe afin qu'ils puissent se familiariser avec les documents qu'ils utiliseront pendant toute la mission.

Le coordonnateur de l'équipe assume la responsabilité générale de la coordination de l'évaluation et de la présentation du rapport d'évaluation final.

Ses responsabilités sont notamment les suivantes :

— Coordonner les travaux préparatoires et prendre les dispositions nécessaires pour l'évaluation ;

— Assurer la liaison en nouant des contacts avec les contreparties appropriées de l'organisme hôte qui constitueront les principaux interlocuteurs de l'équipe d'évaluation durant la mission ;

— Désigner, de concert avec l'organisme hôte s'il y a lieu, un expert en sécurité informatique comme chef d'équipe pour l'évaluation ;

— Prendre des dispositions, de concert avec le chef d'équipe, pour une réunion préparatoire avec l'hôte ;

— Choisir les membres de l'équipe, avec l'approbation de l'organisme hôte ;

— Coordonner les dispositions logistiques à l'appui de l'équipe d'évaluation, y compris la fourniture des documents d'information pertinents ;

— Connaître les règles pertinentes de l'installation concernant la sûreté, la sécurité, la sûreté du personnel et toutes autres prescriptions applicables et communiquer ces informations à l'équipe d'évaluation.

3.4.3. Chef d'équipe

Le chef d'équipe est particulièrement important pour le succès de l'évaluation. Les personnes choisies comme chefs d'équipe doivent posséder des qualités avérées d'encadrement et une très vaste expérience de tout l'éventail des activités d'examen dont devra probablement s'acquitter l'équipe d'évaluation. L'idéal serait que le chef d'équipe ait l'expérience de la conduite des évaluations de la sécurité informatique dans les installations nucléaires.

Le chef d'équipe assume normalement la responsabilité générale de ce qui suit :

— Représenter l'équipe dans ses rapports avec sa contrepartie de l'organisme hôte ;

— Diriger la réunion préparatoire, la réunion d'information initiale et la réunion de clôture ;

— Déterminer les règles d'engagement pour tous les membres de l'équipe ;

— Informer les membres de l'équipe sur l'évaluation, et notamment ses objectifs et ses processus ;

— Veiller à ce que les membres de l'équipe disposent des informations nécessaires pour

être bien préparés à l'évaluation ;

- Diriger la mise au point des détails des activités et des calendriers d'évaluation ;
- Coordonner et superviser les activités d'examen de l'équipe, y compris la tenue des réunions quotidiennes de l'équipe, en veillant à ce que les calendriers soient respectés, en tenant sa contrepartie informée, en réglant les problèmes requérant des décisions et en préparant la réunion de clôture ;
- Coordonner l'examen de toutes les notes techniques ;
- Coordonner l'établissement du projet de rapport ;
- Présenter les résultats de l'évaluation lors de la réunion de clôture ;
- Produire le rapport final ;
- Veiller à ce que les membres de l'équipe soient au fait des problèmes de confidentialité et traitent les informations en conséquence ;
- Veiller à ce que les membres de l'équipe soient sensibilisés et formés aux règles pertinentes éventuelles pour l'installation en ce qui concerne la sûreté, la sécurité et la sûreté du personnel, ainsi qu'aux autres prescriptions applicables.

3.4.4. Membres de l'équipe

Les membres de l'équipe procéderont à l'évaluation en rassemblant des informations, en évaluant et en contribuant au rapport final. Ils devront être experts en sécurité informatique et bien connaître en outre le fonctionnement de l'organisme ou de l'installation.

Les responsabilités et les tâches des membres de l'équipe sont notamment les suivantes :

- Procéder à l'examen des documents et des dossiers ;
- Participer aux réunions et aux discussions avec leurs contreparties dans l'organisme hôte selon qu'il convient ;
- Assister aux réunions de l'équipe et participer à la mise au point des activités d'évaluation ;
- Comparer les conclusions/constatations avec les autres membres de l'équipe ;
- Établir des notes techniques sur la mise en œuvre des mesures de sécurité informatique dans les installations hôtes sur la base d'exposés, de documents, d'entretiens et d'observations directes de l'organisme et de ses pratiques ;
- Évaluer les systèmes dans les domaines fonctionnels par rapport aux contrôles dans les domaines de sécurité ;
- Garder présent à l'esprit l'accord de confidentialité avec l'organisme et traiter toutes les informations en conséquence ;
- Connaître et respecter les règles pertinentes de l'installation concernant la sûreté, la sécurité et la sûreté du personnel, ainsi que les autres prescriptions applicables.

3.4.5. Rédacteur technique

Un rédacteur technique peut être utile à l'équipe pour faciliter l'établissement du rapport d'évaluation en temps voulu et pour aider ses différents membres à établir des notes techniques. Le rédacteur technique assiste à l'ensemble des réunions, des séances d'information et des entretiens pour prendre des notes afin de compléter les informations rassemblées par l'équipe. Tout au long de l'évaluation, le rédacteur technique rassemble les

contributions écrites de l'équipe et les met en forme et les édite selon qu'il convient. Ses responsabilités et ses tâches sont notamment les suivantes :

— Participer aux activités de l'équipe ;
— Prendre beaucoup de notes et/ou aider les membres de l'équipe à préparer les activités d'observation et les entretiens ;
— De concert avec l'équipe et son chef, établir le rapport d'évaluation ;
— Garder présent à l'esprit l'accord de confidentialité avec l'organisme hôte et traiter toutes les informations en conséquence ;
— Connaître et respecter les règles pertinentes de l'installation concernant la sûreté, la sécurité et la sûreté du personnel, ainsi que les autres prescriptions applicables.

3.5. RÉUNION DE L'ÉQUIPE PRÉALABLEMENT À L'ÉVALUATION

Il est recommandé de tenir une réunion de l'équipe avant le commencement de l'évaluation afin d'assurer la coordination entre ses membres. Cela est particulièrement important si les membres de l'équipe n'ont pas travaillé ensemble auparavant, comme ce serait le cas pour les missions internationales avec des experts de différents pays. Même s'ils ont travaillé ensemble régulièrement, il pourra néanmoins être utile de tenir une réunion préalablement à l'évaluation pour examiner et clarifier les détails particuliers de l'évaluation considérée.

Suivant la nature de la mission ou de l'évaluation, cette réunion pourrait être organisée plusieurs mois à l'avance ou immédiatement avant le commencement de l'évaluation.

La réunion est dirigée par le coordonnateur de l'équipe ou le chef de celle-ci. Son ordre du jour pourrait comprendre les points suivants :

i. Présentation des membres de l'équipe ;
ii. Contexte de l'évaluation ;
    a) Champ de l'évaluation ;
    b) Calendrier et délais pour les activités d'évaluation ;
iii. Profils des membres de l'équipe :
    a) Compétences et connaissances des membres de l'équipe ;
    b) Attentes des membres de l'équipe ;
iv. Examen des facteurs propres à l'évaluation et aux installations nucléaires à visiter ;
v. Examen du processus détaillé d'évaluation ;
vi. Définition des détails des rôles, des responsabilités et des domaines d'intervention de chacun des membres de l'équipe.

3.6. CALENDRIER DE L'ÉVALUATION

Le calendrier de l'évaluation variera beaucoup selon que l'évaluation se déroule sur un seul ou de nombreux sites ou qu'il s'agit ou non d'une évaluation spéciale ou d'un module d'une autre évaluation, d'une mission ou d'un service consultatif. Le tableau 1 suggère un calendrier indicatif pour une évaluation spéciale de la sécurité informatique au cours de laquelle la plupart des journées seront passées sur le site et où un rédacteur technique met quotidiennement à jour un projet de rapport.

TABLEAU 1. CALENDRIER INDICATIF DE L'ÉVALUATION

Premier jour
L'équipe d'évaluation tient une réunion préalable à l'évaluation et une session d'orientation
Deuxième jour
L'équipe reçoit la formation nécessaire pour entrer dans l'installation hôte
Réunion initiale d'information avec l'installation hôte
Début de l'évaluation
Réunion de compte rendu et préparatifs pour le lendemain
Le rédacteur technique établit le rapport quotidien sur la base de la réunion de compte rendu
Le chef d'équipe informe un responsable représentant l'organisme hôte selon les besoins
Du troisième à l'avant-avant-dernier jour
Début de l'évaluation
Réunion de compte rendu et préparatifs pour le lendemain
Le rédacteur technique établit le rapport quotidien sur la base de la réunion de compte rendu et compile les notes et les rapports quotidiens rassemblés
Avant-dernier jour
Les membres de l'équipe examinent et résument l'évaluation
Le rédacteur technique rédige un rapport de clôture pour examen par les membres de l'équipe
Le chef d'équipe établit un exposé pour la réunion de clôture
Le chef d'équipe informe un responsable représentant l'organisme hôte selon les besoins
Dernier jour
Réunion de clôture — présentation du résultat de l'évaluation à l'organisme hôte

3.6.1. Réunions de l'équipe

Les réunions quotidiennes de l'équipe, tenues généralement en fin de journée, sont utiles pour passer en revue les activités menées dans la journée, évaluer les progrès, débattre des constatations/conclusions des membres de l'équipe et veiller à ce que le rédacteur technique dispose des informations requises résultant de ces activités.

Ces réunions peuvent également être mises à profit pour préparer les activités à mener le lendemain, par exemple en :

— examinant les parties appropriées des lignes directrices pour l'évaluation et/ou des documents préparatoires ;
— établissant une liste de questions sur chaque sujet ;
— planifiant les activités d'observation sur le terrain ;
— déterminant les principales questions à privilégier le lendemain.

4. MÉTHODOLOGIE D'ÉVALUATION

4.1. APERÇU GÉNÉRAL DE LA MÉTHODOLOGIE

L'évaluation commence le plus souvent par une analyse des pratiques de l'installation en matière de sécurité informatique dans une perspective globale. Une analyse plus détaillée de certains processus et systèmes peut ensuite être effectuée conformément à l'approche décrite dans la section 4.3.1. Celle-ci se fonde sur une répartition des pratiques de sécurité informatique entre les domaines fonctionnels et les domaines de sécurité. Ce processus aidera à affiner l'évaluation de l'efficacité et de la qualité du programme de sécurité informatique dans son ensemble.

4.2. ÉVALUATION DU PROGRAMME GÉNÉRAL DE SÉCURITÉ INFORMATIQUE

Au stade de la collecte d'informations, l'évaluation du programme général de sécurité comporte un examen des politiques, des plans, des procédures, de la mise en œuvre et des organigrammes pertinents. Les entretiens et les observations sur le terrain aideront à évaluer les pratiques de sécurité informatique de manière plus poussée. Les quatre aspects du tableau général à examiner sont l'approche de la direction, les processus de sécurité informatique, la gestion de la menace et des conséquences, et la gestion du risque.

Les sections qui suivent fournissent, pour chacun de ces aspects, des critères indicatifs sur lesquels l'évaluation pourrait se fonder.

4.2.1. Approche de la direction

Une des clés du succès d'un programme de sécurité informatique réside dans l'acceptation de la politique de sécurité informatique à tous les niveaux de la direction et des opérations et dans sa mise en pratique. Le programme de sécurité informatique ne donnera pas de bons résultats sans un ferme engagement de la direction en faveur de ce processus. Les critères indicatifs sont notamment les suivants :

i. L'engagement de la direction est démontré à tous les niveaux.

ii. Les objectifs en matière de sécurité informatique sont clairement définis.

iii. Les rôles et les responsabilités ont été établis clairement de façon que les processus de sécurité informatique, y compris les rôles et les responsabilités spécifiques :

   a) Couvrent tous les domaines fonctionnels ;
   b) Soient établis conformément à une approche coordonnée entre les domaines fonctionnels ;
   c) Assurent une organisation adéquate (avec notamment un responsable de la sécurité informatique ou l'équivalent).

iv. L'accès à des ressources adéquates (humaines, financières, allocation du temps, compétences, etc.) est assuré par la direction.

v. Les processus de gestion prévoient des évaluations internes et des mesures d'assurance de la qualité.

vi. Le respect du cadre réglementaire est assuré.

4.2.2. Processus de sécurité informatique

Ces processus concernent l'utilisation et l'application de mesures de sécurité informatique dans la mise en œuvre de la politique de sécurité informatique. Les mesures en question comprennent l'application de contrôles techniques, de contrôles administratifs et de contrôles physiques pour prévenir les incidents de sécurité informatique, les détecter et intervenir s'il s'en produit. Les critères indicatifs sont notamment les suivants :

— Il existe une politique de sécurité informatique et un programme de sécurité informatique ;

— Il existe un ensemble structuré, officiel et documenté de processus concernant la sécurité informatique ;

— Les processus en place permettent une revue et une amélioration continues grâce par exemple à des examens périodiques, à des audits, à des procédures de maintenance claires, à des autoévaluations, etc. ;

— Les processus sont aussi actifs que possible et non pas réactifs.

4.2.3. Gestion de la menace et des conséquences

Les autorités nationales compétentes — et les installations selon qu'il convient — devraient définir, à partir de sources d'information crédibles, la menace et les moyens associés sous la forme d'une évaluation de la menace et, s'il y a lieu, d'une menace de référence. Les examens de la menace comprennent des analyses des adversaires dotés de cybercapacités crédibles. Il est conseillé de réexaminer et d'évaluer continuellement la menace en recherchant les indices des changements éventuels susceptibles de nuire à la sécurité informatique de l'organisme ou de l'installation. Les questions et les critères indicatifs sont notamment les suivants :

— L'organisme a en place un processus de gestion éprouvé pour faire face aux menaces, aux vulnérabilités et aux conséquences potentielles.

— Quelles sont les références et la méthodologie qui sont utilisées ?

— Quel est le champ couvert par l'analyse de la menace (par exemple l'organisme, une partie de celui-ci, un système, etc.) ?

— Façon dont l'analyse a été effectuée, documentée et utilisée en liaison avec les contrôles de sécurité de référence.

— Des cibles potentielles ont été identifiées et évaluées en vue de déterminer si elles doivent être protégées contre les menaces pour la sécurité nucléaire.

— Les évaluations comprennent une analyse des conséquences potentielles associées à des cyberattaques contre les cibles.

— En ce qui concerne la façon dont les évaluations de la menace sont effectuées, quelle est la fréquence des réexamens réguliers et des actualisations ?

— Les processus d'atténuation, de continuité et de reprise définis pour la compromission des ordinateurs sont-ils appuyés dans le cadre du programme d'intervention en cas d'incident ?

4.2.4. Gestion du risque et respect des principes fondamentaux de sécurité

L'État et l'installation doivent veiller à ce que le programme de sécurité informatique soit capable d'établir et de maintenir le risque de compromission des ordinateurs à un niveau acceptable grâce à la gestion du risque. Il faut en outre que le programme de sécurité

informatique donne des précisions sur l'application des principes fondamentaux de sécurité, y compris le recours à une approche graduée et à la défense en profondeur, pour protéger les actifs contre les événements de sécurité nucléaire conformément au niveau de conséquences ou d'impact que ces événements pourraient avoir. Les questions et les critères indicatifs sont notamment les suivants :

— Les mesures de sécurité informatique reposent sur une approche graduée. En particulier, des niveaux de sécurité ont été assignés conformément à des règles ou processus clairs (basés par exemple sur la sûreté, la menace de référence, une analyse des conséquences potentielles, etc.). Les règles ou processus
sont-ils effectivement appliqués ?

— Comment la défense en profondeur est-elle mise en œuvre pour les composants et systèmes informatiques ?

— Comment les évaluations du risque influent-elles sur l'approche graduée ?

— L'approche graduée prend-elle en compte tous les éléments recensés dans l'évaluation du risque ?

4.3. MATRICE D'ÉVALUATION

4.3.1. Introduction

Un élément essentiel de cette méthodologie d'évaluation est constitué par une évaluation des domaines fonctionnels et des domaines de sécurité (présentés dans la section 2.4). Le tableau 2 fournit une matrice pour la détermination des deux types de domaines à évaluer en assurant que l'évaluation couvre de manière suffisamment approfondie tous les domaines directement intéressants. La matrice d'évaluation contient :

— Les cinq domaines fonctionnels affichés en tant que colonnes ;

— Les domaines de sécurité (adaptés de ceux qui figurent dans la suite ISO 27000) affichés en tant que rangées.

Cette matrice a pour objet d'aider à :

— Déterminer le champ de l'évaluation ;

— Structurer les résultats des analyses et des observations, tant au stade de la collecte d'informations que sur le terrain ;

— Fournir à l'équipe d'évaluation une analyse suffisamment large pour évaluer en connaissance de cause ;

— Visualiser les résultats de l'évaluation.

4.3.2. Domaines fonctionnels

Une évaluation globale porte sur les cinq domaines fonctionnels : opérations, activité commerciale, sûreté, protection physique et interventions d'urgence. Dans certains cas, le champ peut être limité à un sous-ensemble de ces domaines (lors d'une mission IPPAS typique par exemple, seule la protection physique serait évaluée).

On trouvera ci-après une liste de familles de systèmes ou de fonctions à évaluer pour chacun des cinq domaines fonctionnels. Cette liste variera et pourra être adaptée à l'installation particulière à évaluer. Elle pourra également être adaptée en fonction du champ de l'évaluation et du type d'installation. Ce choix pourra être modifié au besoin durant l'évaluation afin

d'englober des éléments supplémentaires rencontrés au cours des activités sur site. Exemples de systèmes ou de fonctions pour chaque domaine :

Domaine des opérations

- Systèmes de contrôle des processus : systèmes de contrôle-commande pour la commande de la centrale ;
- Contrôle-commande de la salle de commande, y compris les systèmes d'alarme ;
- Systèmes informatiques de processus recueillant et préparant les informations pour la salle de commande ;
- Systèmes de contrôle-commande pour la manutention et l'entreposage du combustible ;
- Gestion/maintenance de la configuration ;
- Accès à distance et réseaux privés virtuels (RPV) pour l'environnement opérationnel ;
- Infrastructure de communication vocale et de communication de données ;
- Infrastructure des systèmes d'exploitation et de contrôle ;
- Environnements pour les essais et le développement des systèmes.

Domaine de l'activité commerciale

- Infrastructure de communication vocale et de communication de données ;
- Systèmes de gestion des ressources humaines et dépôts de données ;
- Systèmes techniques/d'ingénierie ;
- Systèmes de commande et d'autorisation de tâches ;
- Systèmes d'achat ;
- Systèmes de bureau.

Domaine de la sûreté

- Systèmes de protection : Systèmes de contrôle-commande utilisés pour déclencher automatiquement des actions de protection du réacteur et de la centrale ;
- Systèmes actionneurs de sûreté : Systèmes de contrôle-commande accomplissant des actions de sûreté et déclenchés par les systèmes de protection et par des commandes manuelles ;
- Dispositifs auxiliaires des systèmes de sûreté : Contrôle-commande pour les systèmes d'alimentation électrique de secours.

Domaine de la protection physique

- Surveillance du périmètre/détection d'intrusions ;
- Systèmes de contrôle des accès ;
- Systèmes de comptabilité et de contrôle des stocks (autres que pour les matières nucléaires) ;
- Systèmes de comptabilité et de contrôle des matières nucléaires ;
- Infrastructure de communication vocale et de communication de données ;
- Systèmes d'alarme ;
- Base de données sur les habilitations de sécurité utilisée pour s'assurer que le personnel possède l'habilitation appropriée.

Domaine des interventions d'urgence

- Contrôle environnemental ;
- Contrôle radiologique ;
- Systèmes de protection contre l'incendie ;
- Infrastructure de communication vocale et de communication de données.

Le rapport final indiquera les systèmes et les fonctions qui ont été évalués et ceux qui ont été considérés comme sortant du champ de l'évaluation.

4.3.3. Domaines de sécurité

À la différence des domaines fonctionnels, les 11 domaines de sécurité pourront tous être inclus dans l'évaluation afin que celle-ci couvre un champ suffisamment large. Comme indiqué précédemment, les 11 domaines de sécurité ont été adaptés d'après la suite ISO/CEI 27000 [4-8] en vue de leur utilisation pour les évaluations de la sécurité informatique dans les installations nucléaires. La section 5 fournit des orientations particulières pour l'évaluation de chacun de ces domaines en ce qui concerne la sécurité nucléaire. Il s'agit d'une liste indicative et non pas prescriptive.

Le tableau 2 fournit une matrice croisée des domaines de sécurité et des domaines fonctionnels qui peut être utilisée pour contrôler le champ couvert par l'évaluation et assurer un examen approfondi des domaines souhaités. L'utilisation d'une telle matrice est à la discrétion de l'équipe d'évaluation. La matrice peut aider non seulement à vérifier le champ couvert par l'évaluation mais aussi à visualiser les observations dans différents domaines, ce qui pourra faciliter la détermination des tendances ou des lacunes dans la couverture de sécurité.

TABLEAU 2. DOMAINES COUVERTS PAR LA MATRICE

Domaines Domaines de sécurité	Opérations	Activité commerciale	Sûreté	Protection physique	Interventions d'urgence
Politique de sécurité					
Gestion de la sécurité informatique					
Gestion des actifs					
Sécurité des ressources					
Protection physique					
Gestion des communications et des opérations					
Contrôle des accès					
Acquisition, développement et maintenance					
Gestion des incidents de sécurité informatique					
Gestion de la continuité					
Conformité					

5. ORIENTATIONS POUR L'ÉVALUATION PAR DOMAINE DE SÉCURITÉ

5.1. APERÇU GÉNÉRAL

Cette section présente, pour chacun des 11 domaines de sécurité, des orientations et la bonne pratique susceptibles d'être utilisés comme critères lors de l'évaluation. Les orientations ne sont pas destinées à être utilisées directement comme liste de contrôle mais peuvent servir à établir un plan d'évaluation. Au cours de l'évaluation, les membres de l'équipe doivent s'intéresser non seulement aux différents domaines, mais aussi à leur intégration et à leur impact sur le programme général de sécurité informatique.

5.2. POLITIQUE DE SÉCURITÉ

5.2.1. Description de ce domaine de sécurité

Ce domaine fournit à la direction une orientation et un soutien en matière de sécurité informatique conformément aux prescriptions de sûreté et de sécurité ainsi qu'aux prescriptions législatives, réglementaires et commerciales pertinentes.

La direction doit fixer clairement une orientation générale compatible avec la sûreté et la sécurité nucléaires et démontrer son soutien et son attachement à la sécurité informatique en instaurant et en maintenant une politique de sécurité informatique dans tout l'organisme.

La politique de sécurité informatique doit être définie, diffusée, documentée et périodiquement réexaminée. Il est recommandé qu'elle tienne compte des cinq domaines fonctionnels nucléaires : exploitation, activité commerciale, sûreté, protection physique et interventions d'urgence.

Documents et dossiers présentant un intérêt

- Politique/plan de sécurité informatique ;
- Politique/plan de sécurité physique de l'installation ;
- Communication de la politique de sécurité informatique aux salariés ;
- Dossier sur les audits de sécurité informatique ;
- Dossier sur les réexamens et les actualisations de la politique de sécurité ;
- Dossiers sur les exercices de sécurité informatique.

Indications pour l'analyse des documents et des dossiers

- La politique de sécurité a-t-elle été définie ?
- Cette politique est-elle conforme aux autres politiques de l'installation ?
- Comment la politique de sécurité est-elle portée à la connaissance des salariés ?
- Comment l'engagement de la direction est-il démontré ?
- Avec quelle fréquence cette politique est-elle réexaminée en vue de sa modification ? Existe-t-il un dossier sur son réexamen ?
- Comment la direction évalue-t-elle l'efficacité de cette politique ?
- La politique de sécurité couvre-t-elle les cinq domaines fonctionnels nucléaires ?
- S'il existe des exceptions à la politique de sécurité, sont-elles documentées ?

— La politique de sécurité est-elle portée à la connaissance de tiers (sous-traitants, etc.) ?
— Cette politique tient-elle compte des orientations en vigueur concernant la bonne pratique ?
— Cette politique énonce-t-elle clairement les objectifs de sécurité ?
— Les responsabilités sont-elles clairement définies et les pouvoirs correspondants sont-ils attribués ?

Exemples de questions pour les entretiens

— Sont-ils au courant de la politique de sécurité ?
— Comprennent-ils les rôles et les responsabilités (y compris les leurs) ?
— Ont-ils accès à la politique de sécurité ?
— Comment la politique de sécurité est-elle mise en œuvre dans des lignes directrices ou des instructions concernant leur travail ?

Éléments à observer

— Processus spécifiques en rapport avec la mise en œuvre de la politique ;
— S'il y a lieu, vérification de la cohérence entre les politiques.

Indications pour les analyses sur le terrain

— Poser les mêmes questions à des personnes de différents départements et à différents échelons de l'organisme.

5.3. GESTION DE LA SÉCURITÉ INFORMATIQUE

Description de ce domaine de sécurité

Un cadre de gestion de la sécurité informatique doit être établi au sein de l'organisme.

La direction doit approuver la politique de sécurité informatique, assigner les rôles et les responsabilités et examiner la mise en œuvre de la sécurité informatique dans tout l'organisme. Il peut s'agir là d'un élément d'une politique de sécurité plus large. Une approche multidisciplinaire est encouragée dans tous les départements de l'organisme (par exemple TI et contrôle-commande/ingénierie).

Documents et dossiers présentant un intérêt

— Politique/plan de sécurité informatique ;
— Organigrammes et définitions d'emplois ;
— Politique et procédures détaillant la structure de l'organisme ;
— Liste des responsables de la sécurité informatique et des membres de l'équipe qui s'occupe de celle-ci ;
— Description du processus d'autorisation pour les modifications de la politique/des procédures de sécurité informatique ;
— Procédure et processus d'autorisation pour l'acquisition de nouveaux équipements de traitement de l'information ;

— Programme, politique et dossiers concernant la formation.

Indications pour l'analyse des documents et des dossiers

— Quels sont les objectifs en matière de sécurité informatique ?

— Où les responsabilités en matière de sécurité informatique se situent-elles dans la hiérarchie de l'organisme ?

— Quelle est la structure de l'équipe de sécurité informatique ?

— Tous les domaines fonctionnels sont-ils couverts par un responsable de la sécurité informatique ? S'il y a plusieurs responsables de la sécurité informatique, les responsabilités et les lignes de communication doivent être clairement définies. Il est nécessaire de définir clairement les interfaces avec les rôles et les responsabilités.

— Les procédures de modification incluent-elles la sécurité informatique ?

— Une formation spécialisée est-elle dispensée à ceux qui exercent des fonctions en matière de sécurité ?

— Qui sont ceux qui ont besoin d'une formation, avec quelle fréquence reçoivent-ils une formation et quel est le pourcentage du personnel qui a reçu la formation requise ?

Exemples de questions pour les entretiens

— Savez-vous qui est votre responsable de la sécurité informatique et comment le contacter ?

— Quelles sont les procédures fondamentales de sécurité informatique ?

— L'équipe de sécurité informatique se réunit-elle régulièrement ? Établit-on des minutes de leurs réunions ? Quel est le processus pour notifier à l'équipe de sécurité informatique les événements et les incidents ou les changements qui pourraient compromettre la sécurité ?

— Quel est le processus (par exemple outils ou procédures) pour la protection des informations sensibles ?

— Quelle formation à la sécurité informatique le personnel a-t-il reçue ? Est-elle continue ?

— L'organisation interne existante a-t-elle fait l'objet d'une analyse des compétences en vue de déterminer les lacunes éventuelles dans celles-ci ? Les lacunes ont-elles été comblées ?

Éléments à observer

— Les spécialistes de la sécurité informatique ont-ils une formation externe pertinente dans ce domaine ?

— Comment les tâches relatives à la sécurité informatique sont-elles contrôlées et suivies (par exemple au moyen des points d'action tirés des minutes des réunions) ?

— Une personne est-elle chargée des audits/évaluations de la sécurité informatique ? Les audits/évaluations sont-ils incorporés dans la planification annuelle ?

Indications pour les analyses sur le terrain

— Il est conseillé que les membres de l'équipe de sécurité informatique participent à l'évaluation.

— La sécurité informatique est-elle mise en relief à tous les échelons de la direction et du personnel ?

5.4. GESTION DES ACTIFS

Description de ce domaine de sécurité

Ce domaine a pour objectif de protéger les actifs de l'organisme. Il englobe la responsabilité de la gestion des actifs, un inventaire du matériel et des logiciels autorisés, une liste du matériel et des logiciels non autorisés ainsi qu'une classification des ordinateurs (des systèmes importants pour la sûreté et/ou la sécurité).

Il faut que tous les actifs aient un propriétaire particulier qui est responsable de l'assignation des contrôles appropriés.

Documents et dossiers présentant un intérêt

— Politique et procédures détaillant le système de gestion des actifs ;
— Inventaire des actifs (systèmes informatiques, matériel de réseau, logiciels, versions) ;
— Procédures et critères pour la détermination des ordinateurs relevant du programme de sécurité informatique, s'il y a lieu ;
— Liste/schéma indiquant l'emplacement physique des actifs inventoriés ;
— Procédure d'établissement de l'inventaire, y compris la périodicité des mises à jour de ce dernier et les dossiers à ce sujet ;
— Schéma fonctionnel des systèmes et des actifs informatiques associés ;
— Schéma du modèle des zones (s'il y a lieu) ;
— Politique et procédure de classification des informations sensibles.

Indications pour l'analyse des documents et des dossiers

— La gestion des actifs couvre l'ensemble du cycle de vie de ceux-ci ;
— Quelle partie de l'organisme a établi l'inventaire ?
— Qui tient l'inventaire ?
— Qui y a accès ?
— Traçabilité des changements ;
— Protection de l'inventaire (y compris les sauvegardes) ;
— Comment la classification des actifs est-elle effectuée ? Est-elle documentée ? Quelle en est la qualité ?
— Les actifs sont-ils assignés à une zone et gérés conformément à un « modèle des zones » ?
— Des « niveaux de sécurité » sont-ils définis ? Quelles sont les mesures de sécurité qui ont été prises pour chaque niveau ?
— Des niveaux de sécurité sont-ils assignés à des zones particulières ? Sur quelle base sont-ils assignés ?
— L'emplacement physique correspond-il à ce qui figure dans l'inventaire ?
— Comment le modèle des zones se compare-t-il à l'emplacement physique d'un système ?

— Comment les actifs sont-ils étiquetés conformément à la classification par domaine fonctionnel ?
— Comment la classification se traduit-elle en zones logiques (voir l'approche graduée) ?
— Contrôler si des équipements sont connectés à plusieurs zones ;
— Les mesures de protection physique ont-elles été évaluées du point de vue de la sécurité informatique ?
— Quel est le degré de dépendance des mesures de protection physique à l'égard des systèmes informatiques et/ou de réseaux ?

Exemples de questions pour les entretiens

— Quelles sont les mesures de sécurité pour le niveau observé ?
— Avez-vous ou pouvez-vous avoir accès à l'inventaire des actifs ?
— Les dispositifs externes ou privés sont-ils autorisés et dans quelles circonstances ? (demander quels sont les contrôles de sécurité en place)
— Comment les questions de durée de vie sont-elles réglées (comment les nouveaux équipements sont-ils choisis et quel est le processus de retrait) ?
— Comment le matériel appartenant à des tiers est-il traité ?

Éléments à observer

— Vérifier des dispositifs particuliers par rapport au schéma du réseau.
— Cet ordinateur est-il connecté au réseau approprié ?
— Le dispositif est-il convenablement étiqueté conformément à la politique ?
— Des mesures de sécurité sont-elles appliquées pour cet actif ?
— Contrôler la cohérence entre l'inventaire et les équipements sur le terrain (par exemple au moyen d'une vérification aléatoire).
— Contrôler la gestion des versions ainsi que la gestion de la configuration des paramètres.
— Comment la confidentialité des actifs et de l'inventaire est-elle gérée ?
— D'où et comment l'administration et la maintenance des actifs en réseau sont-elles assurées ?

Indications pour les analyses sur le terrain

— L'emplacement physique correspond-il à ce qui figure dans l'inventaire ?
— Le modèle des zones correspond-il à l'emplacement physique d'un système (ou d'une partie de ce dernier) ?
— Comment les actifs sont-ils étiquetés conformément à la classification par domaine fonctionnel ?
— Comment la classification se traduit-elle en zones logiques ou niveaux de sécurité (voir l'approche graduée) ?
— Contrôler si des équipements sont connectés à plusieurs zones.

5.5. SÉCURITÉ DES RESSOURCES HUMAINES

Description de ce domaine de sécurité

Son objectif est de faire en sorte que les salariés, les entrepreneurs et les tiers utilisateurs — c'est-à-dire tout le personnel exerçant des responsabilités au sein de l'organisme — comprennent leurs rôles et leurs responsabilités en ce qui concerne l'utilisation des ordinateurs et la sécurité informatique. Il faut considérer les responsabilités en matière de sécurité comme une condition d'emploi préalablement au recrutement et pendant toute la durée de l'emploi ou du contrat de l'intéressé.

Une évaluation de l'habilitation (aussi appelée « contrôle de sécurité du personnel ») est conseillée pour l'ensemble des candidats à un emploi, des entrepreneurs et des tiers utilisateurs en fonction de leur niveau d'accès à des données et systèmes sensibles. Les salariés, les entrepreneurs et les tiers utilisateurs des installations de traitement de l'information sont en outre encouragés à signer un accord concernant leurs rôles et responsabilités en matière de sécurité et à participer à des programmes de formation correspondant à leurs responsabilités. Cela peut faire l'objet de lois nationales pertinentes, qui doivent être prises en considération.

Le programme de sensibilisation à la sécurité informatique est un processus continu promu par la direction.

Documents et dossiers présentant un intérêt

- Politique et procédures concernant l'utilisation et la sécurité des ordinateurs pour les salariés, les entrepreneurs et les sous-traitants ;
- Dossiers de gestion du personnel pour ce qui est de l'utilisation des ordinateurs et de la sécurité informatique ;
- Quelles sont les mesures prises pour contrôler la compatibilité entre les privilèges et le statut des salariés (gestion des droits d'accès en fonction du rôle) ?
- Politique et procédure de formation du personnel (orientation, par fonction, remise à niveau) ;
- Dossiers de certification/qualification et conditions d'affectation des membres de l'équipe de sécurité informatique.

Indications pour l'analyse des documents et des dossiers

- Quelle est la fréquence des formations de sensibilisation à la sécurité informatique dispensées au personnel ?
- Quelle est la procédure pour obtenir accès aux ordinateurs, aux applications et aux données ?
- Quel est le processus pour obtenir accès aux données et applications sensibles ?
- Comment l'efficacité de la culture de sécurité informatique est-elle évaluée ?
- Publiez-vous un annuaire du personnel en ligne ? Sous quelle forme et avec quelles informations ?
- Quelle est la politique de l'organisme en ce qui concerne l'utilisation des médias sociaux ?

— Quels sont les membres du personnel pour lesquels des contrôles d'habilitation sont nécessaires ?

— Quelle est la conséquence d'une violation des procédures de sécurité par quelqu'un ?

— Les sanctions sont-elles adéquates et correctement appliquées ? Un bon comportement est-il récompensé comme il convient ?

— A-t-on défini un « accord d'utilisation » ou une « politique d'utilisation acceptable de la technologie » ? Il est possible de les mettre en œuvre sous la forme d'une fenêtre d'attente lors de la connexion à un compte informatique.

— Les ordinateurs sont-ils dotés, s'il y a lieu, d'un écran de veille protégé par un mot de passe ? Quel est son délai d'activation ?

Exemples de questions pour les entretiens

— Quelle est la fréquence des formations de sensibilisation à la sécurité informatique dispensées au personnel ?

— Quelle est la procédure pour obtenir accès aux ordinateurs, aux applications et aux données ?

— Quel est le processus pour obtenir accès aux données et applications sensibles ?

— Quel est le processus pour notifier un incident de sécurité informatique potentiel ?

— Comment l'autonotification par le personnel des incidents de sécurité informatique potentiels est-elle encouragée ?

— Quelle est la conséquence d'une violation des procédures de sécurité par quelqu'un ?

Éléments à observer

— Contrôler l'accord d'accès/la politique d'utilisation concernant les ordinateurs ;

— Vérifier la certification/les dossiers concernant la formation à la sécurité informatique ;

— Contrôler l'état des comptes en fonction de l'emploi de salariés/d'entrepreneurs choisis au hasard (par exemple contrôler l'autorisation formelle des salariés intervenant dans un système de sûreté) ;

— Contrôler l'état des comptes des salariés qui ont quitté récemment l'organisme.

— Les sanctions sont-elles adéquates et correctement appliquées ? Un bon comportement est-il récompensé comme il convient ?

— Les ordinateurs affichent-ils tous un « accord d'utilisation » ou une « politique d'utilisation acceptable de la technologie » lors de l'ouverture d'une session ?

— Les ordinateurs sont-ils dotés, s'il y a lieu, d'un écran de veille protégé par un mot de passe ? Quel est son délai d'activation ?

Indications pour les analyses sur le terrain

— Une ou quelques personnes risquent-elles de représenter un point de défaillance unique dans le processus ?

— Comment les droits d'accès des personnes transférées ou licenciées sont-ils gérés ?

— Comment l'organisme promeut-il une culture de sécurité informatique active en son sein ? Est-ce que cela s'étend au comportement hors du milieu de travail, par exemple à l'utilisation des médias sociaux ?

5.6. PROTECTION PHYSIQUE

Description de ce domaine de sécurité

Ce domaine a pour objectif d'assurer la protection physique des actifs informatiques. Il cherche à prévenir l'accès physique non autorisé à des systèmes dont le sabotage pourrait provoquer un dysfonctionnement ou un déni de services ou de communication d'informations. La prévention et les contrôles de sécurité doivent se fonder sur une évaluation du risque et être mis en œuvre selon une approche graduée. Il faut prendre bien soin d'atténuer la menace interne.

Dans le cas des systèmes de contrôle-commande, la mise en œuvre de contrôles physiques constitue souvent le seul moyen d'assurer un contrôle des accès ; il n'existe peut-être pas de contrôles techniques ou ceux-ci peuvent ne pas convenir pour ces systèmes.

Documents et dossiers présentant un intérêt

— Politique/plan de sécurité (ou de protection) physique de l'installation ;
— Politique/plan de sécurité informatique ;
— Schéma fonctionnel des systèmes et des actifs informatiques associés ;
— Schéma de l'aménagement physique des installations ;
— Liste/schéma indiquant l'emplacement physique des actifs inventoriés ;
— Schéma/liste des contrôles physiques ;
— Schémas de câblage des réseaux physiques ;
— Procédures pour les processus pertinents d'accès physique et la gestion des listes d'accès ;
— Journaux des contrôles des accès physiques à des locaux ou à des équipements ;
— Organigrammes et définitions d'emplois.

Indications pour l'analyse des documents et des dossiers

— Cohérence entre les contrôles techniques, les contrôles administratifs et les contrôles physiques ;
— Cohérence entre la sensibilité d'une fonction et la protection physique des systèmes/composants concernés ;
— Sécurité informatique appropriée des systèmes assurant la protection physique ;
— Sécurité informatique appropriée des systèmes assurant le contrôle environnemental ;
— Vérification de la séparation physique appropriée des réseaux/composants/équipements aux différents niveaux de sécurité ;
— La menace a-t-elle été caractérisée, et les contrôles mis en œuvre sont-ils adéquats ?
— Déterminer les restrictions d'accès fondées uniquement sur des procédures (c'est-à-dire des contrôles administratifs).

Exemples de questions pour les entretiens

- Quelles sont les zones contrôlées/sensibles désignées ?
- Décrire les mécanismes techniques et procéduraux de contrôle des accès qui sont en place pour chaque zone contrôlée/sensible ;
- Les mesures de protection physique sont-elles adéquates pour les systèmes informatiques en question ?
- Quelles sont les menaces physiques perçues par l'organisme (notamment en termes de ressources et de motivations, y compris la menace interne) ?
- Quelle est la politique en matière d'accès ou d'accompagnement pour les tiers travaillant dans des zones contrôlées ?
- Quelle est la politique concernant les médias portatifs et les dispositifs électroniques de poche dans les zones contrôlées ?
- Quel est le processus de mise au rebut des équipements informatiques brisés ou remplacés ?
- Quel est le processus de mise au rebut des médias électroniques ?
- Quelle est la procédure applicable quand on emporte des équipements et des médias informatiques hors du site (par exemple un ordinateur portable chez soi pour travailler) ?
- Quelle est la procédure applicable quand on apporte des équipements externes (c'est-à-dire n'appartenant pas à l'installation) tels qu'un ordinateur portable, une clé USB, etc., en vue de les utiliser au travail ?
- Quels sont les contrôles physiques et administratifs associés à la protection de l'environnement informatique ?

Éléments à observer

- Observer les moyens et les procédures d'application des contrôles des accès en cours d'exploitation.
- Contrôler que le nombre des personnes titulaires d'une autorisation d'accès physique est maintenu au minimum. Il faut tenir une liste de contrôle des accès des personnes autorisées et la mettre à la disposition du personnel de sécurité.
- Observer la protection des câbles et des fils, les armoires, les supports, les panneaux et la façon dont les câbles sont reliés entre eux. Garder à l'esprit le fait que les équipements de réseaux peuvent être situés dans des zones polyvalentes et pas seulement dans des salles de serveurs. Les équipements se trouvent-ils dans une zone sécurisée ? Qui y a accès ?
- Quels sont les dispositifs, tels que systèmes antifraude, dispositifs de verrouillage physique, alarmes, vidéosurveillance, etc., qui sont en place pour sécuriser les équipements ?
- Observer l'application des mesures de protection procédurales (badges, accompagnateurs, lignes peintes à ne pas franchir, application des règles des deux personnes, etc.).
- Observer l'utilisation des dispositifs personnels de TI tels que smartphones, ordinateurs portables, tablettes, médias portatifs, etc.

— Observer l'emplacement des terminaux d'ordinateurs : sont-ils placés de manière à empêcher de voir les écrans et les claviers sans autorisation ?

— Des médias informatiques sont-ils laissés sans surveillance sur les bureaux ?

— Quelles sont les mesures de sécurité en place autour de l'infrastructure de soutien de l'infrastructure informatique (contrôles de sécurité pour la ventilation et le refroidissement, l'alimentation électrique primaire et de secours, etc.) ?

— Comment les différents équipements sont-ils étiquetés, inventoriés et tracés ?

Indications pour les analyses sur le terrain

— Analyser parallèlement les contrôles physiques et les contrôles administratifs ;

— Examiner la menace interne et ce qu'un accès physique aux ressources informatiques peut permettre d'accomplir ;

— Observer les personnes apportant des dispositifs informatiques personnels tels que smartphones, ordinateurs portables, tablettes, médias portatifs, etc.

— Contrôler la cohérence entre le contrôle des accès logiques et le contrôle des accès physiques.

— Contrôler si les systèmes de contrôle-commande (ou certains d'entre eux) sont dotés d'une alarme d'accès physique. Où l'alarme est-elle donnée ? Quelles sont les actions normales pour une alarme ?

5.7. GESTION DES COMMUNICATIONS ET DES OPÉRATIONS INFORMATIQUES

Description de ce domaine de sécurité

Ce domaine de sécurité a principalement pour objectif de contrôler l'exfiltration et l'infiltration de données depuis et dans les systèmes informatiques relevant du programme de sécurité informatique afin de protéger contre l'introduction de nouvelles vulnérabilités et de contrôler les procédures opérationnelles de manière à garantir que les systèmes fonctionnent et protègent comme prévu. Il a aussi pour objectif de protéger l'intégrité des ordinateurs et des communications.

Documents et dossiers présentant un intérêt

— Diagrammes de flux de données afin de déterminer les interconnexions entre les réseaux et les flux de données ;

— Politique et procédure de gestion de la configuration ;

— Schéma de l'architecture des réseaux ;

— Politique et procédure de reconfiguration des ordinateurs/réseaux ;

— Politique et procédure de durcissement des systèmes informatiques ;

— Politique et procédure concernant les médias : accès aux médias, étiquetage, stockage, transport et assainissement ;

— Politique et procédure de vérification et de validation des contrôles de sécurité mis en œuvre sur les ordinateurs et les réseaux dans le cadre des programmes de sécurité informatique ;

— Dossiers sur la certification/qualification des personnes procédant aux essais de vérification et de validation ;

— Politique et procédure pour la diffusion d'informations à l'extérieur/auprès du public (par exemple sur un site Web de l'entreprise) ;

— Politique et procédure pour traitement des informations du domaine public ;

— Politique et procédure concernant la gestion de la prestation de services par des tiers pour toutes les classes d'ordinateurs et de réseaux dans le cadre du programme de sécurité informatique ;

— Accords avec des tiers concernant les réseaux de l'installation auxquels les tiers peuvent accéder et les solutions de sécurité des tiers ;

— Politique et procédure pour traiter avec les entrepreneurs tiers ;

— Politique et procédure pour surveiller et évaluer continuellement le programme de sécurité informatique ;

— Politique et procédure pour l'échange électronique d'informations au sein des installations et avec des installations extérieures ;

— Politique et procédure pour les exemptions au programme de sécurité informatique, y compris les dossiers sur ces exemptions ;

— Politique et procédure pour l'utilisation de dispositifs sans fil, de dispositifs mobiles et de médias amovibles ;

— Politique et procédure pour les restrictions d'utilisation et la mise en œuvre des technologies sans fil ;

— Politique et procédure concernant l'exécution de balayages pour rechercher les connexions sans fil non autorisées et les points d'accès sans fil ;

— Politique et procédure concernant la suite à donner à la découverte de connexions ou de points d'accès sans fil non autorisés ;

— Politique et procédure pour l'utilisation des dispositifs informatiques portatifs, y compris les téléphones portables ;

— Politique et procédure pour la surveillance et l'évaluation continues des connexions non sécurisées et frauduleuses ;

— Politique et procédure de détection de l'utilisation de systèmes et/ou de réseaux et de l'accès à ceux-ci sans autorisation et description des méthodes utilisées à cette fin ;

— Il pourrait aussi y avoir intérêt à effectuer une recherche sur les informations provenant de sources librement accessibles en vue d'évaluer celles à la disposition du public sur l'installation ou l'organisme qui pourraient présenter un risque pour la sécurité informatique.

Indications pour l'analyse des documents et des dossiers

— Examiner les procédures approuvées mises en œuvre par le personnel d'exploitation et de maintenance pour assurer une sécurité intrinsèque ainsi que leur cohérence avec la politique et le plan de sécurité.

— Les procédures de sécurité prennent-elles en compte les différents modes de fonctionnement de l'installation afin de parer aux différentes préoccupations de sécurité qui y sont associées ?

— Les procédures rassemblées couvrent-elles les préoccupations de sécurité contre lesquelles elles sont censées protéger ?

— L'installation hôte a-t-elle procédé à une analyse efficace pour s'assurer que les contrôles de sécurité fonctionnent et protègent comme prévu ?

— L'installation hôte a-t-elle évalué l'impact d'une tentative réussie de déjouer les contrôles de sécurité dans le domaine de la gestion des communications et des opérations ?

— L'installation hôte a-t-elle évalué l'impact d'une tentative réussie de déjouer les contrôles de sécurité en ce qui concerne les activités menées à distance ou par des tiers (y compris la maintenance) ?

— L'installation hôte a-t-elle configuré ses ordinateurs de manière à remédier aux vulnérabilités déjà connues ?

— Le concept du « moindre privilège » est-il mis en œuvre ?

— L'installation hôte dispose-t-elle d'une analyse de sécurité et d'un programme d'essais (faisant appel à l'analyse des vulnérabilités, aux essais d'intrusion et à d'autres moyens) pour déterminer les vulnérabilités potentielles connues et inconnues ? Quelle est la portée du programme d'essais ?

— Les entrepreneurs et les sous-traitants sont-ils tenus d'appliquer la politique de sécurité informatique ?

Exemples de questions pour les entretiens

— Quelle est la procédure applicable quand on emporte des équipements et des médias informatiques hors du site (par exemple un ordinateur portable chez soi pour travailler) ?

— Quelle est la procédure applicable quand on apporte des équipements externes (c'est-à-dire n'appartenant pas à l'installation) tels qu'un ordinateur portable, une clé USB, un smartphone, etc., en vue de les utiliser sur le site ?

Éléments à observer

— Vérifier que l'installation hôte a configuré ses ordinateurs conformément au concept du moindre privilège et à un processus d'analyse et d'atténuation des vulnérabilités déjà connues ;

— Observer la performance des procédures ;

— Identifier tout signe concernant des entités ou des connectivités externes (par exemple pour la sauvegarde ou la surveillance) ;

— Procéder à des contrôles ponctuels des blocs-notes électroniques/dispositifs mobiles et se renseigner sur leur utilisation ;

— Contrôler que les systèmes, les applications, l'architecture de réseau, etc., documentés correspondent à ce qui est effectivement en place.

Indications pour les analyses sur le terrain

— Examiner si l'analyse des risques recense intégralement les risques associés aux communications en réseau et aux dispositifs mobiles.

— Examiner la question de savoir quel est le principal problème qui subsiste.

5.8. CONTRÔLES DES ACCÈS AUX ORDINATEURS

Description de ce domaine de sécurité

L'objectif est de contrôler l'accès logique (au moyen de contrôles techniques et administratifs) aux systèmes informatiques ou aux informations électroniques.

Ce domaine a trait aux prescriptions concernant le contrôle des accès, la gestion des accès des utilisateurs, les responsabilités des utilisateurs, le contrôle des accès aux réseaux, le contrôle des accès aux systèmes d'exploitation, le contrôle des accès aux applications et aux informations, ainsi que l'informatique mobile et le télétravail.

L'accès aux systèmes informatiques (systèmes de contrôle-commande, systèmes de supervision, systèmes techniques, systèmes de sécurité et systèmes administratifs) est contrôlé sur la base du plan de sécurité informatique.

Les règles de contrôle des accès logiques aux ordinateurs et aux réseaux sont spécifiées dans le cadre d'un processus formel d'autorisation.

Documents et dossiers présentant un intérêt

— Plan de sécurité informatique ;

— Politique et procédure de contrôle des accès aux ordinateurs (gestion des droits, gestion des comptes) ;

— Dossier sur les résultats de tout audit des contrôles des accès ;

— Politique et procédure de réexamen des autorisations d'accès aux systèmes, y compris les privilèges ;

— Organigramme pour la gestion des droits administratifs sur les ordinateurs ;

— Politique et procédure en matière de mots de passe (complexité, durée de validité et politique de verrouillage des comptes) ;

— Politique et procédure pour l'octroi et la documentation des privilèges ;

— Description des mécanismes d'authentification employés ;

— Documentation sur la journalisation et la surveillance des contrôles des accès ;

— Politique et procédure pour l'autorisation et la comptabilisation des comptes ;

— Politique d'accès aux réseaux — commutateurs de réseaux, sockets non connectés, etc. ;

— Politique d'accès aux réseaux — utilisation de réseaux locaux virtuels ;

— Topologies des réseaux et du trafic ;

— Politique de sécurité des passerelles — liste des contrôles des accès aux routeurs, règles des pare-feu ;

— Schéma/liste des points d'accès sans fil ;

— Politique et procédure pour l'accès à distance (qui, quand, pourquoi, quels services) ;

— Politique et procédure pour l'utilisation et la sécurité des modems ;

— Politique et procédure pour les comptes administratifs/à hauts privilèges.

Indications pour l'analyse des documents et des dossiers

— Dans les cas où des mesures techniques de contrôle des accès (par exemple mots de passe) ne peuvent pas être mises en œuvre dans certains composants de contrôle-commande, que ce soit pour des raisons techniques ou de performance opérationnelle, vérifier que des mesures correctives
(par exemple accroissement de la sécurité physique, de la sécurité du personnel, de la détection des intrusions et des mesures d'audit) sont appliquées conformément au niveau de sécurité du système de contrôle-commande ;

— Contrôler la cohérence entre les contrôles techniques, les contrôles administratifs et les contrôles physiques ;

— Dans le cas des systèmes de contrôle-commande, accorder une attention particulière aux méthodes et aux exemples d'accès à distance lorsque des technologies sans fil et mobiles sont mises en œuvre.

— Dans celui des technologies sans fil, existe-t-il une politique d'utilisation pour les accès et un programme d'évaluation destiné à assurer le respect de cette politique ?

— Contrôler l'application des politiques, techniques ou administratives, de « séparation des tâches » et de « moindre privilège ». Dans le cas plus particulièrement des systèmes de contrôle-commande et des systèmes anciens essentiels, contrôler l'existence de mesures correctives si ces politiques ne sont pas appliquées.

Exemples de questions pour les entretiens

— Quels sont les systèmes auxquels a accès le personnel exerçant certaines fonctions ?

— Quels sont les systèmes auxquels il est accédé à distance ? Avec quelle fréquence ? Pourquoi est-il accédé à distance à ces systèmes ?

— Contrôler si des droits d'accès sont délégués ou accordés en dehors de la procédure.

— Comment la politique de contrôle des accès est-elle perçue : est-elle trop stricte, trop faible, etc. ? Est-elle adaptée aux besoins opérationnels ?

— Déterminer les questions/problèmes qui se posent régulièrement en ce qui concerne la gestion incorrecte du contrôle des accès (c'est-à-dire les contournements).

— Quel est le processus applicable pour accorder/obtenir accès aux ordinateurs ? Quels sont les processus de révocation et de renouvellement ?

— Déterminer si les contrôles des accès sont contournés dans certains cas pour des raisons d'efficacité opérationnelle (ou de commodité).

— Quels sont les incidents survenus précédemment — ou même les anecdotes — en ce qui concerne le contrôle des accès ?

— L'administrateur a-t-il deux comptes (administrateur/utilisateur) ?

— Comment l'organisme gère-t-il les changements dans la situation du personnel (par exemple changement de département, changement de tâches, etc.) ?

Éléments à observer

- Demander des démonstrations concernant les moyens et les procédures d'application du contrôle des accès ;
- Contrôler si des droits d'accès sont délégués ou accordés en dehors des procédures ;
- Contrôler les listes de contrôle des accès logiques pour s'assurer que le nombre des titulaires de droits d'accès est maintenu au minimum ;
- Contrôler les points d'accès aux modems et sans fil ;
- Surveiller l'activité sans fil ;
- Contrôler les ports de connexion accessibles ;
- Déterminer les points de connexion possibles pour une surveillance passive ;
- Rechercher les systèmes et les postes de travail déverrouillés ;
- Rechercher les systèmes sans mot de passe, avec des comptes par défaut ou des mots de passe évidents ;
- Contrôler les bannières informant les utilisateurs des types d'utilisation autorisés ;
- Contrôler comment la ségrégation des réseaux est assurée (logique, physique, isolement) ;
- Contrôler l'architecture des réseaux et en particulier les interfaces entre les domaines de sécurité ;
- Déterminer les voies possibles de compromission des systèmes critiques (sûreté, commande) à partir de réseaux commerciaux ou d'entreprise ou d'autres façons ;
- Déterminer les questions/problèmes qui se posent régulièrement en ce qui concerne la gestion incorrecte du contrôle des accès (contournements) ;
- Rechercher les mécanismes d'authentification non documentés ;
- Examiner les procédures de connexion ; un mécanisme d'authentification en texte clair est-il en place ?
- Les comptes et les mots de passe sont-ils échangés entre le personnel ? Des comptes de groupe sont-ils utilisés ?
- Demander les calendriers des activités au moment de l'évaluation et sélectionner certaines activités à observer, telles que l'installation de correctifs, le paramétrage, l'installation de logiciels, etc.

Indications pour les analyses sur le terrain

- Combien de mots de passe différents une personne doit-elle utiliser dans les opérations quotidiennes ? Durant les opérations spéciales ? (De trop nombreux mots de passe peuvent conduire à utiliser des notes autocollantes, etc.)
- Les membres du personnel ferment-ils la session/verrouillent-ils leur compte, s'il y a lieu, lorsqu'ils s'éloignent de leur ordinateur ?
- Comment la traçabilité est-elle gérée lorsque des comptes de groupe/partagés sont utilisés ?
- Comment la complexité des mots de passe est-elle assurée ?
- Le contrôle des accès logiques et le contrôle des accès physiques sont-ils cohérents ?

5.9. ACQUISITION, DÉVELOPPEMENT ET MAINTENANCE DES SYSTÈMES INFORMATIQUES

Description de ce domaine de sécurité

Ce domaine de sécurité a pour objectif d'assurer la sécurité et l'intégrité des systèmes informatiques acquis ainsi que des activités de maintenance effectuées par le vendeur après la mise en service des systèmes. Les contrôles de sécurité couverts par ce domaine comprennent la protection de la chaîne d'approvisionnement, la conformité des logiciels, l'intégration de capacités de sécurité, les essais en usine et les essais de réception.

Il faut prendre note tout particulièrement des activités de maintenance sur les systèmes informatiques. Il convient d'évaluer ces activités afin de s'assurer que des contrôles suffisants sont en place pour se prémunir contre l'introduction de vulnérabilités ou de logiciels malveillants. En outre, il est conseillé d'évaluer si les activités de maintenance de la sécurité informatique, telles que la gestion des correctifs, sont effectuées en temps opportun et de manière efficace.

Documents et dossiers présentant un intérêt

- Politique et procédure d'acquisition des systèmes et des services, y compris l'élaboration de prescriptions de sécurité pour les systèmes acquis ou développés ;
- Description des prescriptions concernant les mesures de sécurité à prévoir pour protéger contre l'introduction de vulnérabilités et de menaces par le biais de la chaîne d'approvisionnement ;
- Description des prescriptions exigeant que les vendeurs emploient des méthodes de contrôle de la qualité et de validation des logiciels afin de réduire au minimum les logiciels défectueux ou mal conçus ;
- Description ou démonstration de la façon dont l'installation veille à ce que les systèmes nouvellement acquis comportent suffisamment de renseignements descriptifs ou de capacités en matière de sécurité, ou les deux à la fois, pour la mise en œuvre et le maintien des contrôles de sécurité requis ;
- Description ou démonstration des prescriptions de sécurité exigeant que des essais de sécurité et des plans d'évaluation soient élaborés, mis en œuvre et documentés pour veiller à ce que les produits acquis satisfassent à toutes les prescriptions de sécurité spécifiées ;
- Description et démonstration de la prescription de sécurité exigeant que l'intégrité du système acquis soit préservée jusqu'à la livraison du produit à l'installation. Description de la façon dont l'installation vérifie et contrôle que le programme de sécurité mis en œuvre avant la livraison présente au moins le même niveau de sécurité que celui qui est appliqué au système informatique lorsqu'il est en service.
- Plan et résultats d'essais pour la vérification et la validation du code au regard des prescriptions concernant la conception et la configuration de la sécurité ;
- Procédures pour les essais de réception des ordinateurs/équipements électroniques ;
- Document sur les prescriptions concernant la mise en œuvre et le maintien des mesures de sécurité informatique ;
- Plan et résultats d'essais de validation pour évaluer l'efficacité des mesures de sécurité informatique mises en œuvre ;

— Conception et méthodologie pour la sécurité informatique décrivant les caractéristiques de conception sécurisée mises au point pour répondre aux exigences de sécurité définies pour les ordinateurs ;
— Dossiers de maintenance pour les systèmes informatiques ;
— Calendriers de maintenance tenant compte des tâches prioritaires en matière de sécurité informatique.

Indications pour l'analyse des documents et des dossiers

— Contrôler que les tiers se préoccupent comme il convient de la sécurité informatique ;
— Contrôler la sécurité le long de la chaîne d'acquisition et de développement, en tenant compte du fait que les entrepreneurs, sous-traitants, etc., peuvent être nombreux ;

Exemples de questions pour les entretiens

— Quels sont les contrôles appliqués sur les équipements sur le site avant et pendant l'installation ?
— Quels sont les essais effectués pour évaluer les fonctions de sécurité — chez le vendeur et après l'installation ?
— Quels sont les contrôles en place pour veiller à ce que des vulnérabilités informatiques ou des exploits tels que des logiciels malveillants ne soient pas insérés dans le système durant les activités de maintenance ?
— Comment les activités de maintenance effectuées par des tiers sont-elles surveillées sur le site ?
— Preuves d'inspections de sécurité chez le vendeur et dossier sur le respect des prescriptions de sécurité.

Éléments à observer

— Quels sont les contrôles appliqués sur les équipements sur le site avant et pendant l'installation ?
— Comment les informations sensibles circulent-elles entre le vendeur et l'installation ?

Note : Ce domaine est difficile à observer sur le site, car il concerne essentiellement des tiers avant la livraison des systèmes.

Indications pour les analyses sur le terrain

— Observer une activité de maintenance de la sécurité informatique effectuée par du personnel interne ou des entrepreneurs extérieurs.

5.10. GESTION DES INCIDENTS DE SÉCURITÉ INFORMATIQUE

Description de ce domaine de sécurité

Un incident de sécurité informatique peut se produire malgré tous les efforts déployés par un organisme. Ce domaine de sécurité a pour objectif d'assurer que des processus sont en place pour atténuer efficacement l'impact potentiel des incidents de sécurité informatique et communiquer efficacement au sujet de ces incidents.

D'après le n° 17 de la collection Sécurité nucléaire de l'AIEA [3], un incident de sécurité informatique est un événement qui nuit effectivement ou peut nuire à la confidentialité, à l'intégrité ou à la disponibilité d'un système informatique, de réseau ou d'information numérique ou aux informations traitées, conservées ou transmises par le système, ou qui constitue une violation ou présente un risque imminent de violation des politiques de sécurité, des procédures de sécurité ou des politiques d'utilisation acceptable.

Documents et dossiers présentant un intérêt

- Politique et procédure de gestion des incidents ;
- Plan de communication en cas d'incident ;
- Demandes adressées au service d'assistance informatique (tickets) ;
- Démonstration de l'évaluation de la sécurité concernant les événements d'arrêt non prévu de l'installation ou des systèmes (évaluation des causes profondes) ;
- Exemple ou modèle de rapport d'incident (un rapport réel serait préférable) ;
- Procédure/considérations concernant les effets interdomaines d'une intervention en cas d'incident (par exemple les mesures prises sur un système de TI d'entreprise peuvent ne pas être acceptables dans un environnement de contrôle-commande) ;
- Plan et procédures d'intervention en cas d'incident ;
- Dossiers sur l'exécution d'exercices pour évaluer l'efficacité du plan d'intervention en cas d'incident et mesures prises à la suite de ces exercices.

Indications pour l'analyse des documents et des dossiers

- Dans la gestion des incidents de sécurité informatique, est-il tenu compte comme il convient des menaces externes et internes (agresseur d'origine interne) ?
- Existe-t-il un système de classification clair pour caractériser un incident ?
- La procédure d'escalade est-elle clairement définie (critères, points de contact) ?
- Le processus de communication concerne les communications internes (y compris pour la gestion générale des incidents dans l'installation) et les communications externes [liaisons avec les équipes d'intervention informatique d'urgence (CERT), autorités nationales et internationales].
- Les procédures de criminalistique, de préservation des traces, etc., ont-elles été élaborées et adaptées de manière à faciliter le processus d'investigation ?
- Évaluer le processus de remédiation ainsi que la définition et l'application des mesures correctives ;
- Vérifier la cohérence entre la gestion des incidents et la gestion de la continuité ;
- Contrôler le lien entre la gestion des incidents de sécurité informatique et la gestion générale des incidents dans l'installation.
- L'installation a-t-elle appliqué les plans et procédures d'intervention en cas d'incident dans le cadre d'un exercice d'autoévaluation (c'est-à-dire d'un exercice sur table ou d'un exercice de simulation) ?
- L'installation a-t-elle participé à d'éventuels exercices coordonnés relatifs aux incidents informatiques auxquels ont participé des organismes externes ?

— Les prescriptions relatives à la préservation des preuves et à la chaîne de responsabilité ont-elles été incorporées dans le plan et les procédures d'intervention en cas d'incident de sécurité informatique ?

Exemples de questions pour les entretiens

— Contrôler si les salariés et les entrepreneurs connaissent la procédure à suivre, et notamment le point de contact, en cas d'incident de sécurité.

— Décrire ce qui constitue un incident de sécurité. Comment un incident de sécurité est-il catégorisé ?

— Quand et dans quelles circonstances un incident serait-il notifié ? À qui l'incident est-il notifié à l'extérieur ?

— Quelle est la procédure à suivre si un écart dans la mise en œuvre des contrôles de sécurité est décelé par un salarié ou un entrepreneur ?

— L'installation a-t-elle connu éventuellement des incidents de sécurité (informatique) ?

— Pouvez-vous décrire ce qui a été fait ou modifié à la suite d'un incident récent de sécurité informatique ?

— Les processus existants sont-ils jugés efficaces ? Y a-t-il encore des problèmes éventuels ?

— Comment et avec quelle fréquence les plans d'intervention en cas d'incident font-ils l'objet d'exercices ?

— L'installation a-t-elle participé à d'éventuels exercices coordonnés relatifs aux incidents informatiques au niveau d'une installation ou de l'État ou au niveau international ?

Éléments à observer

— Demander une démonstration du système particulier de gestion assurant le suivi des incidents (application papier ou logicielle).

Indications pour les analyses sur le terrain

— Évaluer si le personnel a reçu une formation suffisante à la procédure.

5.11. GESTION DE LA CONTINUITÉ

Description de ce domaine de sécurité

Ce domaine de la sécurité a pour objectif général d'assurer la continuité et le rétablissement des fonctions critiques de l'installation à la suite de perturbations majeures des systèmes et processus informatiques normaux. Ces perturbations comprennent celles provoquées par des aléas naturels, une erreur humaine et une intention délictueuse.

Il est à noter que la section relative à la gestion des incidents de sécurité informatique traite de l'intervention initiale et de l'atténuation en cas d'incident, alors que ce domaine est axé sur la continuité et le processus de reprise.

Documents et dossiers présentant un intérêt

— Politique et procédures de gestion de la continuité ;

— Liste des applications et des systèmes soumis à une gestion de la continuité et liste de leurs propriétaires/responsables ;

— Dossiers sur la formation à la continuité des opérations (y compris les rapports sur les exercices) ;

— Plan de continuité des opérations.

Indications pour l'analyse des documents et des dossiers

— Examiner comment la gestion de la continuité en matière de sécurité informatique est intégrée aux programmes existants de continuité de l'exploitation de l'installation (par exemple via un plan de continuité des activités du site) ;

— Il est à noter que la gestion de la continuité est prise en compte dans la conception de base et les spécifications techniques des systèmes de sûreté et d'exploitation du contrôle-commande. Il est recommandé de prendre ces spécifications en considération lors de l'évaluation de la gestion de la continuité pour les systèmes de sûreté et d'exploitation du contrôle-commande. Il n'en ira peut-être pas ainsi pour d'autres domaines fonctionnels. Dans le cas des systèmes de contrôle-commande remplissant des fonctions de sûreté ou de sécurité importantes, la moyenne des temps de bon fonctionnement et le temps moyen de réparation sont deux caractéristiques de conception essentielles à prendre en considération pour la détermination des mesures de gestion de la continuité ;

— Les sous-systèmes et les interdépendances importants sont-ils déterminés ? Les accords contractuels sont-ils suffisants pour appuyer les objectifs en matière de continuité ?

— Les fonctions et les systèmes importants comportent-ils un degré suffisant de diversification et de redondance ?

— La dimension malveillante (attaque intentionnelle par opposition à une défaillance fortuite) est-elle prise en compte comme il convient dans la gestion de la continuité ?

— Contrôler la cohérence entre la gestion des incidents et la gestion de la continuité.

Exemples de questions pour les entretiens

— Contrôler si les plans d'essais concernant la continuité et la reprise des systèmes informatiques ainsi que les procédures de reprise (par exemple pour la restauration et la mise à jour des données entre un arrêt et un redémarrage) sont connus, testés et examinés.

— Le personnel a-t-il été formé à la reprise des systèmes et à la gestion de la continuité ? Qui a été formé ? Comment la gestion de la continuité traite-t-elle de la détermination des priorités en matière d'accès et de ressources en cas de dégradation opérationnelle ?

— L'installation a-t-elle effectué des exercices axés sur la reprise des systèmes et la gestion de la continuité dans le cas d'un cyberévénement ?

— Existe-t-il des systèmes de secours pour gérer les fonctions informatiques importantes en cas d'incident/accident ?

— Quels sont les contrôles de sécurité appliqués pour les systèmes de secours ?

— Quel est le lien architectural avec les systèmes de secours ?

— Existe-t-il des procédures pour assurer l'exploitation à la suite d'une perte des fonctions informatiques ?

Éléments à observer

— Contrôler que les salariés ont accès aux procédures pertinentes de continuité ;

— L'évaluation pourrait sélectionner, en vue de leur examen, un sous-ensemble de contrôles de la gestion de la continuité, tels que les procédures de secours et de restauration, les moyens de communication de rechange (en particulier pour les interventions d'urgence) et les accords de priorité des entrepreneurs ;

— Demander le rapport sur le dernier exercice ;

— Observer les installations de rechange et de secours s'il en existe.

Indications pour les analyses sur le terrain

— Observer l'application d'une procédure de reprise, sur le système ou dans un laboratoire de développement, ou au moyen d'un processus « papier ».

— Les informations sur la configuration de l'installation sont-elles à jour ? Quel est le mécanisme/processus appliqué ?

— Évaluer la pertinence des priorités en matière d'accès et de ressources en cas de dégradation opérationnelle par rapport aux objectifs généraux de l'installation.

5.12. CONFORMITÉ

Description de ce domaine de sécurité

Si l'évaluation est effectuée par l'autorité compétente ou s'il s'agit d'une autoévaluation, le respect des obligations juridiques, statutaires, réglementaires ou contractuelles pertinentes concernant la sécurité informatique peut s'inscrire dans le champ de l'évaluation.

Ce domaine de sécurité a pour objectif de contrôler que le programme de sécurité informatique est conforme à ces obligations juridiques, statutaires, réglementaires ou contractuelles.

Il est à noter que ce domaine peut ne pas être applicable dans certains contextes ; il faudra examiner cela lors de la planification du champ de l'évaluation.

Documents et dossiers présentant un intérêt

— Documents énonçant les obligations juridiques, statutaires, réglementaires ou contractuelles qui concernent des aspects de la sécurité informatique ;

— Rapport(s) interne(s) ou externe(s) sur le respect des règlements ;

— Procédures/processus de certification s'ils sont pertinents pour la sécurité informatique ;

— Composante sécurité informatique de la menace de référence ;

— Documents d'orientation sur la conception et la modification des systèmes (sections mentionnant les contraintes de conformité).

Indications pour l'analyse des documents et des dossiers

— Chaque domaine fonctionnel peut avoir des contraintes et des critères de conformité différents ;

— En outre, suivant les pays et le type d'installations, il peut être nécessaire de prendre en considération plusieurs cadres réglementaires émanant d'organismes relevant de différents niveaux de l'État (par exemple à la fois de l'organisme de réglementation de la sûreté et d'un organisme s'occupant de la sécurité) ;

— Les aspects de la sécurité informatique peuvent être traités dans des documents de portée plus large ; par exemple les normes de sûreté applicables peuvent comporter des sections consacrées à la sécurité informatique.

— Comment les prescriptions juridiques et réglementaires sont-elles incorporées dans la politique, l'organisation et les procédures en matière de sécurité ?

— Les documents correspondants sont-ils clairement référencés ou énumérés dans la politique de sécurité ?

— Les systèmes de contrôle-commande font habituellement l'objet de documents d'orientation spécifiques concernant leur conception et leur modification, mais l'équipe d'évaluation peut analyser ces aspects pour d'autres domaines (par exemple la comptabilité des matières nucléaires, les systèmes liés aux interventions d'urgence).

Exemples de questions pour les entretiens

— Comment les prescriptions réglementaires sont-elles déterminées, suivies et mises en œuvre ?

— Qui est responsable de ces tâches (détermination, suivi et mise en œuvre) ?

— Expliquez comment les modifications sur le terrain sont validées en fonction de leur impact sur le respect des obligations juridiques, statutaires, réglementaires et contractuelles.

Éléments à observer

— L'évaluation pourrait sélectionner un sous-ensemble de prescriptions découlant des obligations juridiques, statutaires, réglementaires et contractuelles et valider leur mise en œuvre sur le terrain.

Indications pour les analyses sur le terrain

— Commencer avec un petit échantillon représentatif ; si plusieurs écarts sont constatés, l'échantillon pourra être réexaminé et des éléments supplémentaires pourront être étudiés.

6. RAPPORT FINAL ET ACTIVITÉS POST-ÉVALUATION

6.1. ÉLABORATION DU RAPPORT FINAL

Un des aspects les plus importants de l'évaluation réside dans l'examen des observations, dans la détermination des constatations et dans les recommandations et les suggestions formulées à l'intention de l'organisme hôte. Ces informations sont consignées dans le rapport final et présentées à l'installation ou à l'organisme hôte lors d'une réunion de clôture.

Le rapport final pourra varier dans sa forme et son contenu suivant l'objet de l'évaluation, mais il comportera toujours des éléments tels qu'une synthèse, une introduction et des sections consacrées aux résultats et aux conclusions. L'annexe III fournit un exemple de rapport d'évaluation. La figure 3 illustre le processus de préparation et d'élaboration du rapport.

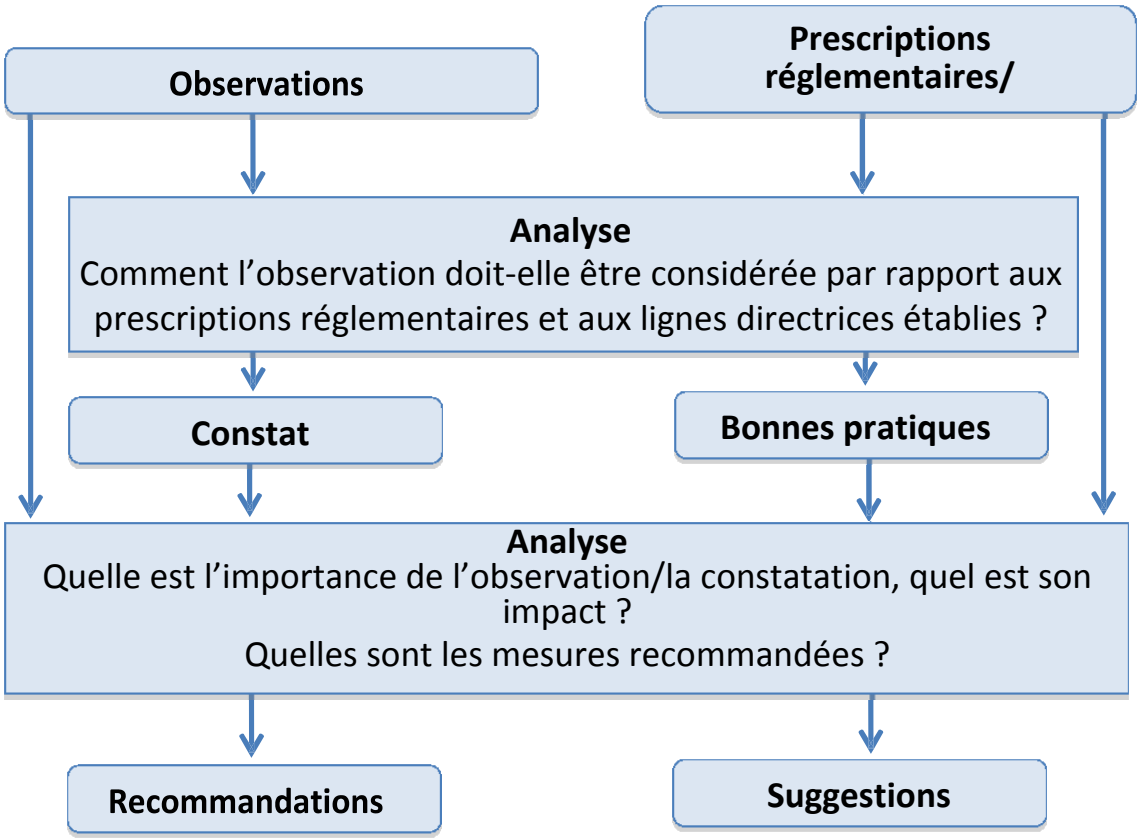

FIG. 3. Processus d'analyse de l'évaluation

La composante collecte des données de l'évaluation consiste à consigner les observations sur les données présentant un intérêt qui ont été recueillies lors de l'examen des documents/dossiers, des entretiens et des observations directes. Les observations sont importantes individuellement, mais peuvent aussi constituer collectivement un indicateur de tendances dans l'installation ou l'organisme dont il faut se préoccuper. Lors de l'examen des notes prises sur le terrain, les observations similaires pourront être regroupées pour donner des indications sur des tendances ou des cas récurrents.

Les observations sont alors analysées par rapport aux prescriptions, telles que les règlements nationaux, les procédures de l'organisme et/ou les normes internationales selon qu'il convient.

Une constatation est formulée en cas de non-respect d'une procédure réglementaire ou interne ou d'écart par rapport à cette procédure. La base utilisée pour la formulation des constatations doit être bien définie et convenue lors des réunions de planification préliminaires.

Il est en outre important de comprendre que la liste des constatations ne donne qu'un aperçu instantané de l'installation sur la base d'un certain nombre d'observations effectuées par l'équipe d'évaluation. Pour l'analyse des observations et l'élaboration des constatations, il faut prendre en compte de multiples facteurs, dont les suivants :

— La profondeur et l'étendue de l'évaluation ;
— Les compétences et l'expérience de l'équipe d'évaluation ;
— Le niveau d'accès accordé à l'équipe d'évaluation ;
— Le niveau des ressources allouées à l'évaluation, par exemple temps imparti et nombre d'évaluateurs.

Les constatations de l'évaluation constitueront donc un échantillon sélectif et non une représentation exhaustive des pratiques de sécurité informatique de l'organisme. Une constatation confirme la présence d'un problème, mais l'absence de constatation ne signifie pas qu'il n'existe pas de problèmes de sécurité informatique.

Les observations ne débouchent par toujours sur des constatations et les constatations ne sont pas toutes négatives. Elles peuvent en outre aboutir à l'identification d'une « bonne pratique », c'est-à-dire d'une procédure ou d'un processus organisationnel qui fournit une méthode originale et efficace d'atteindre les objectifs de sécurité. Ces pratiques doivent être recensées et citées comme exemples possibles pour l'amélioration des programmes de sécurité d'autres organismes.

En plus des constatations et de la bonne pratique, l'équipe d'évaluation peut aussi formuler d'autres orientations, recommandations et suggestions dans le rapport associé aux constatations.

Les recommandations fournissent des lignes directrices de conformité pour les prescriptions juridiques et réglementaires (lois/règlements nationaux) et/ou les normes internationales, s'il y a lieu. Normalement, les recommandations n'indiquent pas comment corriger un problème, mais seulement qu'il faut le corriger.

Les suggestions fournissent un niveau supplémentaire d'information au sujet d'une constatation, y compris les stratégies correctives ou d'atténuation. Ces informations ne découlent pas nécessairement des orientations réglementaires, mais plutôt des normes techniques et de la bonne pratique de l'industrie.

Les actions suggérées peuvent être notamment les suivantes :

— Modifications des équipements et installation de dispositifs et de moyens supplémentaires pour améliorer la sécurité ;
— Amélioration des procédures et des mesures administratives ;
— Mise en place de vérifications et de contrôles supplémentaires ;
— Rectification des déficiences révélées dans les procédures opérationnelles ;
— Rectification des déficiences dans les documents d'orientation ;
— Formation du personnel à des fonctions professionnelles tant générales que spécifiques ;
— Modifications de l'environnement de travail ;

— Modifications de la planification et de la programmation du travail et/ou de l'assignation de membres du personnel à des tâches particulières.

6.1.1. Analyse de la signification

Souvent, dans une évaluation, il ne suffit pas de formuler une constatation ; il faut en définitive étudier l'impact ou la conséquence potentielle de la constatation. L'organisme hôte doit examiner l'impact ou la signification de la constatation en ce qui concerne la sécurité et la sûreté. L'analyse d'impact peut être effectuée à de multiples niveaux. Au premier niveau, on examine l'impact de la constatation considérée, en étudiant plus particulièrement son impact ou sa signification en ce qui concerne les caractéristiques de confidentialité, d'intégrité et de disponibilité. Au deuxième niveau d'analyse, on examine systématiquement l'ensemble des constatations et leur effet général sur une installation ou un organisme. Une telle analyse n'est pas sans intérêt et exigera qu'une équipe multidisciplinaire se penche sur toutes les ramifications pour la sûreté, la sécurité, les opérations, etc.

En général, l'équipe d'évaluation ne procède pas à une telle analyse à ce niveau dans le cas d'un examen réglementaire et en laisse le soin à l'organisme hôte. Cette analyse peut cependant être effectuée conjointement avec l'équipe d'évaluation dans le cas des autoévaluations ou des missions consultatives techniques de tiers. De telles évaluations exigent d'importantes ressources et prennent du temps.

6.2. ÉLÉMENTS POUR L'ÉTABLISSEMENT DU RAPPORT

Suivant les dispositions prises pour l'évaluation, on peut établir le rapport au cours de l'évaluation, par exemple mettre un projet de rapport à disposition pour la réunion de clôture, ou le présenter ultérieurement.

Il convient de tenir compte des considérations ci-après en ce qui concerne le contenu du rapport :

— Les membres de l'équipe doivent être objectifs en fondant leurs conclusions sur leur examen des documents pertinents, les entretiens avec le personnel clé et l'observation directe ;

— Les membres de l'équipe doivent consulter leurs contreparties de l'hôte pour clarifier tout élément qui fait question afin de s'assurer qu'il est compris convenablement ;

— Les membres de l'équipe doivent se consulter mutuellement, et en particulier consulter le chef d'équipe, et échanger les résultats de leurs constatations afin d'éviter les doubles emplois, un manque de cohérence et les éléments qui peuvent empiéter sur d'autres constatations ;

— Les conclusions des membres de l'équipe — en particulier celles qui débouchent sur des recommandations, des suggestions et la reconnaissance d'une bonne pratique — doivent être documentées brièvement et étayées par une « base » sur laquelle se fonde la justification d'une recommandation, d'une suggestion ou d'une bonne pratique particulière ;

— La sensibilité du rapport final doit être prise en considération, compte tenu de la sensibilité de son contenu, des vulnérabilités qu'il peut révéler (et des conséquences potentielles de celles-ci) ainsi que de toute politique nationale ou de l'organisme concernant les informations sensibles. La sensibilité du rapport doit être clairement indiquée sur le document, et le rapport doit être traité en conséquence.

Lorsqu'il rend compte d'une constatation, le rapport doit être clair et indiquer si possible ce qui suit :

— Fonction et domaines de sécurité concernés (l'impact peut se faire sentir sur de multiples domaines) ;

— Orientations et/ou bonne pratique utilisées pour l'évaluation (en citant la référence dans le cas des orientations) ;

— Constatation ;

— Impact potentiel de la constatation (pourrait être considéré comme un degré de gravité, par exemple administratif, mineur, majeur, grave, etc.) ;

— Solution ou action corrective recommandée.

Les constatations peuvent être agrégées plus avant entre les fonctions et domaines de la sécurité aux fins d'une évaluation ou d'un classement général des éléments collectifs.

Le rapport indique le degré de confiance avec lequel l'équipe estime que l'examen est suffisamment exhaustif pour fournir une véritable évaluation de l'installation.

Les éléments qui n'ont pas été évalués doivent être indiqués.

En ce qui concerne la présentation et le style du rapport, les considérations ci-après pourront être utiles :

— Un résumé initial exposant les impressions générales que l'équipe a retirées de l'examen peut être utile pour mettre en perspective l'analyse ultérieure plus détaillée des différents éléments.

— La rédaction doit être simple, claire, concise, objective et impersonnelle.

— Des graphiques et des photos peuvent être insérés dans la section à laquelle ils se rapportent. Des organigrammes du gouvernement ou de l'organisme — ainsi que des schémas ou des photos illustrant une déficience ou une bonne pratique — sont particulièrement utiles.

— Les noms officiels (ou leurs traductions officielles) sont utilisés pour désigner les unités organisationnelles, les postes et les systèmes.

— Les abréviations doivent être explicitées lorsqu'elles sont employées pour la première fois, et il faut les énumérer et les définir dans un tableau pour qu'il soit possible de s'y référer aisément.

6.3. RÉUNION DE CLÔTURE

Les participants à la réunion de clôture peuvent comprendre du personnel de l'entité évaluée et aussi d'autres parties. Au besoin, le chef de l'équipe d'évaluation informera l'entité évaluée de toute situation rencontrée durant l'évaluation qui est susceptible de diminuer le crédit à accorder aux conclusions de l'évaluation. Il s'agit d'une réunion formelle, en sorte qu'il faut tenir des minutes et des relevés de présence.

RÉFÉRENCES

[1] AGENCE INTERNATIONALE DE L'ÉNERGIE ATOMIQUE, Objectif et éléments essentiels du régime de sécurité nucléaire d'un État, collection Sécurité nucléaire de l'AIEA n° 20, AIEA, Vienne (2014).

[2] AGENCE INTERNATIONALE DE L'ÉNERGIE ATOMIQUE, Recommandations de sécurité nucléaire sur la protection physique des matières nucléaires et des installations nucléaires, collection Sécurité nucléaire de l'AIEA n° 13, AIEA, Vienne (2011).

[3] AGENCE INTERNATIONALE DE L'ÉNERGIE ATOMIQUE, La sécurité informatique dans les installations nucléaires, collection Sécurité nucléaire de l'AIEA n° 17, AIEA, Vienne (2013).

[4] COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE, Technologies de l'information — Techniques de sécurité — Systèmes de management de la sécurité de l'information — Vue d'ensemble et vocabulaire, ISO/CEI 27000:2009, ISO, Genève (2009).

[5] COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE, Technologies de l'information — Techniques de sécurité - Systèmes de management de la sécurité de l'information - Exigences, ISO/CEI 27001:2005, ISO, Genève (2005).

[6] COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE, Technologies de l'information — Techniques de sécurité — Code de bonne pratique pour le management de la sécurité de l'information, ISO/CEI 27002:2005, ISO, Genève (2005).

[7] COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE, Technologies de l'information — Techniques de sécurité — Gestion des risques en sécurité de l'information, ISO/CEI 27005:2008, ISO, Genève (2008).

[8] COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE, Technologies de l'information — Techniques de sécurité — Exigences pour les organismes procédant à l'audit et à la certification des systèmes de management de la sécurité de l'information, ISO/CEI 27006:2007, ISO, Genève (2007).

[9] ORGANISATION INTERNATIONALE DE NORMALISATION, Lignes directrices pour l'audit des systèmes de management, ISO 19011:2011, ISO, Genève (2011).

[10] UNITED STATES NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, Technical Guide to Information Security Testing and Assessment, NIST Special Publication 800–115, Gaithersburg, Maryland, USA (2008).

GLOSSAIRE

Les termes employés dans la présente publication sont définis ci-après. Lorsqu'elles sont disponibles, les définitions sont tirées de publications existantes de l'AIEA ou de normes internationales. En pareil cas, la définition renvoie à la publication dont elle est tirée (indiquée dans la section Références à la fin du document principal).

Bonne pratique. La bonne pratique est un programme, une activité, une façon d'utiliser les équipements, etc., qui s'est révélé excellent et qui contribue directement ou indirectement à la sûreté ou à la sécurité ainsi qu'à une bonne performance soutenue. La bonne pratique est nettement supérieure au comportement attendu et ne consiste pas simplement à satisfaire aux prescriptions du moment.

Constatation. Observation d'un écart entre la façon dont quelque chose est effectué et la façon dont il est censé l'être d'après une prescription réglementaire, une norme ou la bonne pratique.

Évaluation. La méthodologie décrite dans le présent document concerne une activité qui, par souci de simplicité et de cohérence, est dénommée partout « évaluation ». Toutefois, ainsi qu'il a été indiqué précédemment, cette méthodologie peut être appliquée dans divers contextes, et d'autres dénominations telles que « service consultatif », « visite d'experts », « audit » ou « autoévaluation » peuvent convenir. L'emploi du terme « évaluation » ne doit pas être interprété comme conférant un pouvoir ou une responsabilité supplémentaire à l'AIEA ou à tout autre organisme procédant à une évaluation.

Observation. Quelque chose qui a été identifié à la suite de l'examen de documents, d'un entretien ou d'une observation directe.

Ordinateurs et systèmes informatiques. Dispositifs de calcul, de communication et de contrôle-commande qui constituent les éléments fonctionnels de l'installation nucléaire. Ils comprennent non seulement les ordinateurs de bureau, les systèmes centraux, les serveurs et les dispositifs de réseaux, mais aussi les composants de niveau inférieur comme les systèmes incorporés et les PLC (automates programmables). En milieu industriel, ces systèmes informatiques peuvent être appelés « systèmes de contrôle industriel » (SCI) et, dans les centrales nucléaires, « systèmes de contrôle-commande nucléaires ».

Prescription. Fondement d'une évaluation particulière, c'est-à-dire règles, règlements et normes à suivre.

Recommandation. Action qui renforce la sécurité d'une installation nucléaire (pour une évaluation de l'hôte) ; action coercitive pour donner suite à une constatation (émanant par exemple de l'organisme de réglementation d'un État).

Une recommandation est un conseil que l'on est vivement encouragé à suivre pour l'activité ou le programme évalué afin d'améliorer la sécurité opérationnelle. Elle se fonde sur les orientations de la collection Sécurité nucléaire de l'AIEA, les règlements nationaux, les normes ou la bonne pratique internationale éprouvée et porte sur les causes profondes d'un problème et non pas simplement sur ses symptômes. Une recommandation intègre souvent une méthode éprouvée de recherche de l'excellence allant au-delà des exigences minimales. Elle doit être précise, réaliste et conçue pour déboucher sur une amélioration tangible.

Le terme « recommandation » tel qu'employé dans la présente publication ne doit pas être confondu avec le sens qu'il a dans les orientations des publications de la collection Sécurité nucléaire.

Sécurité informatique. Aspect particulier de la sécurité de l'information qui a trait aux systèmes informatiques, aux réseaux et aux systèmes numériques [3].

Dans la présente publication, l'expression « sécurité informatique » désigne la sécurité de tous les ordinateurs tels qu'ils sont définis ci-dessus et de tous les systèmes et réseaux interconnectés. (Les termes « sécurité de la TI » et « cybersécurité » sont considérés comme des synonymes, mais ne sont pas employés ici)

Suggestion. Action ou amélioration proposée que l'installation évaluée pourrait mettre en œuvre.

Une suggestion peut venir s'ajouter à une recommandation ou en être indépendante. Elle peut contribuer indirectement à des améliorations de la sécurité opérationnelle, mais elle a principalement pour objet de rendre une bonne performance plus efficace, d'indiquer un élargissement utile pour un programme existant ou d'appeler l'attention sur une possibilité éventuellement supérieure pour un travail en cours. D'une manière générale, une suggestion est destinée à inciter la direction et le personnel de la centrale à continuer d'examiner les moyens d'améliorer la performance.

ANNEXE I

INDICATIONS POUR L'ÉVALUATION DES SYSTÈMES DE CONTRÔLE-COMMANDE

APERÇU GÉNÉRAL DES SYSTÈMES DE CONTRÔLE-COMMANDE

Dans le contexte de la présente publication, on entend par « ordinateurs » et par « systèmes informatiques » les dispositifs de calcul, de communication et de contrôle-commande constituant les éléments fonctionnels de l'installation nucléaire. Ces dispositifs comprennent non seulement les ordinateurs de bureau, les systèmes centraux, les serveurs et les dispositifs de réseaux, mais aussi des composants de niveau inférieur comme les systèmes incorporés et les PLC (automates programmables). Un sous-ensemble de ces systèmes informatiques comprend les systèmes de contrôle numériques et les systèmes de contrôle-commande. Ceux-ci sont particulièrement importants lors de l'évaluation, car leur compromission peut avoir de graves effets à la fois sur la sécurité et la sûreté.

Le système de contrôle-commande sert de socle opérationnel pour les processus de l'installation. Le n° NP–T–3.12 de la collection Énergie nucléaire de l'AIEA (réf. I-1, pages 2 et 3 de la version anglaise) précise les trois fonctions fondamentales du système de contrôle-commande des processus d'une centrale. Sa première est de fournir des capacités sensorielles (par exemple mesure et surveillance) à l'appui de fonctions telles que le suivi ou le contrôle et de permettre au personnel de la centrale d'évaluer son état. Les systèmes de contrôle-commande tels que les capteurs et les détecteurs constituent donc directement les interfaces avec les processus physiques de la centrale nucléaire et leurs signaux sont envoyés par les systèmes de communications à l'opérateur ainsi qu'aux applications décisionnelles (analogiques ou informatiques).

Sa deuxième fonction est d'assurer la commande automatique à la fois de l'installation principale et de nombreux systèmes auxiliaires. La troisième fonction du système de contrôle-commande est de réagir aux défaillances et aux événements anormaux en assurant la sûreté de la centrale et sa protection contre les conséquences de toute défaillance ou déficience ou d'erreurs manuelles.

Ces systèmes informatiques et associés (contrôle-commande) utilisés dans les fonctions opérationnelles d'une centrale nucléaire, d'une installation du cycle du combustible ou d'une installation d'entreposage appuient diverses fonctions et sont dénommés de multiples façons dans l'industrie. L'expression « systèmes de contrôle industriel » (SCI) est employée ici pour désigner ces systèmes, qui comprennent les systèmes de commande de surveillance et d'acquisition de données (SCADA), les systèmes de contrôle distribué (DCS) et d'autres configurations de systèmes de contrôle tels que les automates programmables montés sur châssis [I-2].

Les composants de contrôle des systèmes de contrôle industriel peuvent comprendre (réf. [I-2], pages 2 à 4 de la version anglaise) :

— Les terminaux à distance pour assurer le contrôle et la surveillance de dispositifs ;

— Les automates programmables, qui sont de petits ordinateurs souvent utilisés dans les processus de contrôle industriel ;

— Les dispositifs électroniques intelligents, qui sont de petits capteurs/actionneurs intelligents pour l'acquisition de données, la communication et le contrôle local ;

— L'interface homme-machine/interface homme-système, qui fournit l'interface opérateur pour le suivi et le contrôle des processus de la centrale.

Ces systèmes font partie du réseau des SCI, qui comprennent également des composants standard et spécialisés de réseaux tels que les routeurs, les pare-feu, les modems et les points d'accès à distance.

Le réseau de contrôle est alors relié aux composants de niveau inférieur tels que les capteurs et les actionneurs pour contrôler et/ou surveiller les processus de la centrale, comme indiqué dans la figure I-1.

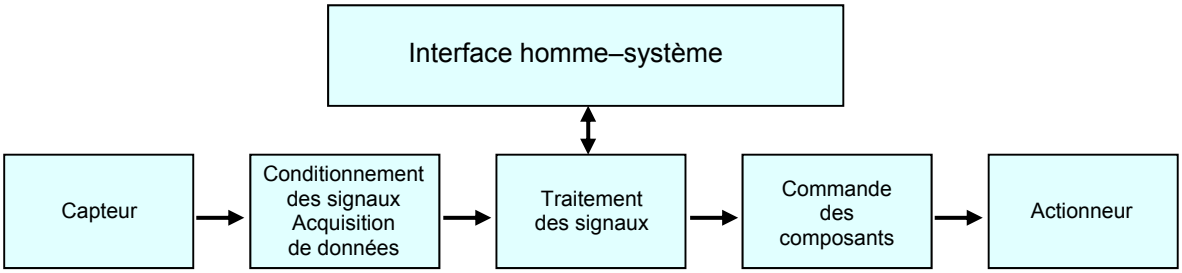

FIG. I-1. Schéma d'une fonction typique de contrôle-commande[I-1].

De multiples processus identiques peuvent être commandés sur un seul réseau. Inversement, les processus peuvent être gérés sur des réseaux entièrement distincts. Dans le réseau de commande, chacun de ces différents composants est un point vulnérable potentiel du système et doit donc être examiné à un certain niveau dans le cadre de l'évaluation. Un problème est que ces composants n'ont pas été nécessairement conçus dans l'optique de la sécurité informatique.

VULNÉRABILITÉS COURANTES DES SYSTÈMES DE COMMANDE

On trouvera ci-après une liste des vulnérabilités courantes recensées par le Département de la sécurité intérieure (DHS) des États-Unis [I-3], dont il peut être tenu compte dans l'élaboration et la conduite de l'évaluation des SCI et des systèmes de contrôle-commande d'une installation. Aucun élément ne peut, en soi, constituer nécessairement un sujet de préoccupation, mais il convient plutôt de considérer les différents éléments dans le contexte général de l'évaluation. Les contrôles compensatoires ou les mécanismes de défense imbriqués peuvent déjà avoir remédié à ces problèmes potentiels.

Contrôle des accès

— L'accès n'est pas restreint aux objets pour lesquels il est nécessaire ;
— Le protocole des SCI a autorisé des hôtes des systèmes à lire ou à écraser des fichiers sur d'autres hôtes sans aucune journalisation ;
— La documentation et les informations sur la configuration sont échangées librement (lecture seule) ;
— Des partages communs sont disponibles sur des systèmes multiples ;
— Il n'y a pas d'authentification en fonction des rôles pour la communication avec les composants des SCI ;

— Un utilisateur distant peut télécharger un fichier en n'importe quel endroit sur l'ordinateur cible ;
— Le téléchargement arbitraire de fichiers vers l'aval est autorisé sur des hôtes de SCI ;
— Le téléchargement arbitraire de fichiers vers l'amont est autorisé sur des hôtes de SCI ;
— Un client distant est autorisé à lancer n'importe quel processus ;
— Le service SCI autorise un accès anonyme ;
— Comptes administratifs « clandestins » pour donner ultérieurement accès au vendeur aux fins de la maintenance, des mises à jour et de la formation ;
— Utilisation excessive des comptes administrateurs ;
— L'exploitation à distance des services d'application des CSI a autorisé un accès au niveau racine sur les hôtes de SCI ;
— Service de base de données fonctionnant comme administrateur ;
— Une authentification n'est pas requise pour lire un fichier de configuration des systèmes qui contient les détails des comptes utilisateurs, y compris les mots de passe ;
— Absence de séparation des tâches par le biais de l'autorisation d'accès assignée ;
— Non-application d'un système de verrouillage pour les tentatives de connexion infructueuses.

Mots de passe

— Certains hôtes de SCI ont des mots de passe administratifs très faibles à trois caractères ;
— Les mots de passe faibles ont été récupérés et ont donné accès à toutes les ressources des systèmes au niveau racine ;
— Plusieurs mots de passe faibles ont été trouvés ;
— Le mot de passe par défaut n'avait pas été changé ;
— Des noms d'utilisateur et des mots de passe par défaut sont utilisés au niveau administrateur ;
— Des informations d'identification par défaut sont assignées à plusieurs comptes d'utilisateurs prédéfinis sur le dispositif, y compris le compte d'utilisateur administratif ;
— Un composant de SCI est directement accessible par Internet à l'aide du nom d'utilisateur et du mot de passe par défaut ;
— La longueur, la force et la complexité des mots de passe ne sont pas imposées ;
— Nombre de comptes, y compris celui de l'administrateur, n'ont pas de date d'expiration du mot de passe ;
— Une politique de verrouillage des comptes n'a pas été définie ;
— Le paramètre complexité des mots de passe a été désactivé ;
— Historique des mots de passe paramétré pour ne mémoriser aucun mot de passe précédent.

Artéfacts de code

La mémoire d'un SCI, par exemple le code source et la configuration du système sur un système de fichiers partagés, offre d'importantes possibilités de recherche d'information par un attaquant. La conception de nombreux SCI prévoit des partages réseaux ouverts sur les hôtes de SCI. Voici des exemples de constatations associées à cette vulnérabilité qui ont été faites lors d'évaluations :

— Partages réseaux accessibles publiquement sur des hôtes de SCI. Deux partages ont été découverts sur les ordinateurs de postes de travail et de serveurs ;

— Partages communs sur des systèmes multiples ;

— Fichiers accessibles à la lecture ;

— Fuite d'informations par le biais de répertoires partagés ;

— Nombreux partages réseaux accessibles publiquement sur des hôtes de SCI ;

— Partage du code source du SCI sur les hôtes de ces systèmes. Le code source pouvait être téléchargé et utilisé pour trouver des vulnérabilités.

Gestion des correctifs

Les constatations ci-après ont été faites à propos des versions non corrigées ou anciennes d'applications tierces incorporées dans le logiciel de SCI :

— Version vulnérable pour bases de données ;

— Version vulnérable pour serveurs Web ;

— La liaison et l'incorporation d'objets pour le contrôle de processus se fondent sur l'appel de procédure à distance (RPC) et l'architecture d'objets distribués (DCOM) ; sans correctif, le contrôle de processus est exposé aux vulnérabilités RPC/DCOM connues ;

— Bibliothèques SSL vulnérables (non corrigées).

Planification/politique/procédures

— Absence de documentation formelle ;

— Maintenance médiocre de la documentation sur la sécurité ;

— Absence d'équipe de sécurité informatique bien établie ;

— Absence de politique de reprise après sinistre ;

— Procédures de reprise mal comprises ;

— Faibles capacités de sauvegarde et de restauration.

Faiblesse de conception des réseaux

En général

— Pas de périmètre de sécurité défini ;

— Les dispositifs des réseaux ne sont pas configurés comme il convient ;

— Les ports des dispositifs des réseaux ne sont pas sécurisés.

Absence de segmentation des réseaux

- Réseaux de contrôle utilisés pour le trafic sans lien avec le contrôle ;
- Services du réseau de contrôle non intégrés à ce réseau ;
- Absence de segmentation interne du réseau production du SCI ; Les serveurs du protocole de communication inter-centres de conduite (ICCP) ne sont pas dans une DMZ ;
- Absence de segmentation interne du réseau production du SCI : l'hôte doté d'une liaison série dédiée pour le transfert de données utilise une application à haut risque qui n'est pas dans une DMZ ;
- Les systèmes liés au contrôle sont accessibles sur le réseau local de l'entreprise ;
- Les évaluations des interventions en cas d'incident et les évaluations faites à l'aide de l'outil d'évaluation de la cybersécurité sur le site ont mis en évidence les problèmes ci-après sur de multiples sites :
- Réseaux de contrôle utilisés pour le trafic sans lien avec le contrôle ;
- Services du réseau de contrôle non intégrés à ce réseau.

Pare-feu/DMZ

- Absence de pare-feu ;
- Absence de DMZ fonctionnelle ;
- Câbles connectés directement au réseau local du SCI en contournant le pare-feu ;
- Le serveur SSH relie les réseaux locaux de l'entreprise et du SCI en contournant le pare-feu ;
- Une troisième carte réseau sur le serveur de l'ICCP est connectée directement au réseau local du SCI ;
- L'accès à des ports particuliers sur l'hôte n'est pas restreint aux adresses IP requises ;
- Listes d'accès définies mais pas appliquées ; Pas de filtrage entrant ;
- Listes d'accès incorrectes pour les ports requis ;
- L'accès aux services d'impression en réseau sur le réseau local de l'entreprise n'est pas protégé par un mot de passe ou une liste de contrôle des accès ;
- Un client de courrier électronique de la DMZ avait accès au réseau local et à l'Internet de l'entreprise ;
- Restrictions d'accès sortant insuffisantes ;
- Règles des pare-feu non adaptées au trafic du SCI.

Audits et responsabilisation

- Absence d'audits/évaluations de la sécurité ;
- Journalisation absente ou médiocre ;
- Architecture de réseau pas bien comprise ;
- Faible application des politiques de connexion à distance ;
- Faible contrôle des médias entrants et sortants ;
- Méthode insuffisante de surveillance des événements sur le réseau de contrôle.

ANNEXE I RÉFÉRENCES

[I-1] INTERNATIONAL ATOMIC ENERGY AGENCY, Core Knowledge on Instrumentation and Control Systems in Nuclear Power Plants, IAEA Nuclear Energy Series No. NP–T–3.12, IAEA, Vienna (2011).

[I-2] UNITED STATES NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, Guide to Industrial Control Systems (ICS) Security, NIST Special Publication 800–82, Gaithersburg, Maryland, USA (2011).

[I-3] UNITED STATES DEPARTMENT OF HOMELAND SECURITY, Common Cybersecurity Vulnerabilities in Industrial Control Systems, US Department of Homeland Security, (2011), disponible en ligne à l'adresse :

https://ics-cert.us-cert.gov/sites/default/files/documents/DHS_Common_Cybersecurity_Vulnerabilities_ICS_2010.pdf

ANNEXE II

MODÈLE POUR LES OBSERVATIONS

On trouvera ci-après des exemples de modèles destinés à aider les évaluateurs à recueillir et à analyser les données pour une évaluation.

Ces modèles et les tableaux de données sont destinés uniquement à servir d'exemples et pourront être adaptés aux besoins de l'équipe d'évaluation.

Les observations seront utilisées pour élaborer le rapport d'évaluation final.

Nom de l'évaluateur		**Numéro**			
Date et heure					
Emplacement	Lieu de l'observation				
Installation	S'il y a lieu				
Système	S'il y a lieu				
Domaine de sécurité	Comme défini				
Domaine fonctionnel	Comme défini				
Niveau de sécurité					
Observation :	Décrire ce qui a été observé ou déterminé				
Mode de détermination	Revue documentaire	Entretien	Observation	Source ouverte	Autre :
Intention	Recommandation	Suggestion	Bonne pratique	Autre :	
Constatation*	Décrire l'écart				
Base*	Renvoi aux orientations de l'AIEA, à la bonne pratique, à une norme, à un règlement, à un vecteur d'attaque connu, etc.				
Cause profonde*	Raison du problème				
Exploitabilité*	Aisée	Modérée	Complexe		
Accessibilité*	Menace externe/menace interne (dont on a conscience ou non)				
Impact potentiel*	Description de l'impact direct et indirect de la constatation.				
Niveau de signification*	Catégorisation de la constatation sur la base de son impact potentiel (les organismes peuvent concevoir leur propre échelle de signification ou d'impact)				
Action*	Mettre en œuvre la bonne pratique, une norme, un règlement, un système de correctifs, etc.				
NOTES :					

*Ces éléments ne seront peut-être pas immédiatement évidents durant l'observation et pourront être ajoutés ultérieurement.

Légende du modèle de terrain

Domaines fonctionnels

OP : Domaine des opérations

AC : Domaine de l'activité commerciale

SÛ : Domaine de la sûreté

PP : Domaine de la protection physique

IU : Domaine des interventions d'urgence

Domaines de sécurité

PS : Politique de sécurité

OI : Organisation de la sécurité de l'information

GA : Gestion des actifs

RH : Sécurité des ressources humaines

PP : Protection physique

CO : Gestion des communications et des opérations

CA : Contrôle des accès aux ordinateurs

AM : Acquisition, développement et maintenance des systèmes informatiques

GI ; Gestion des incidents de sécurité informatique

AM : Gestion de la continuité, conformité, interventions d'urgence

CF : Conformité

Exploitabilité

Aisée	Vulnérabilité généralement connue ; il existe des exploits publics
Modérée	Certains détails sont connus ; une validation de principe existe
Complexe	Pas de détails disponibles

Types d'actions potentiels

Modification des équipements et installation de dispositifs et de moyens supplémentaires pour empêcher que des événements identiques ou similaires se reproduisent.

Amélioration des procédures et des mesures administratives, et vérifications et contrôles supplémentaires.

Rectification des déficiences révélées dans la documentation d'exploitation (manuels d'exploitation).

Rectification des déficiences dans les documents normatifs.

Formation du personnel à la bonne exécution de ses tâches.

Apporter des changements à l'environnement de travail.

Apporter des changements à la planification et à la programmation du travail et/ou aux personnes assignées à des tâches particulières.

ANNEXE III

MODÈLE POUR LE RAPPORT FINAL

SYNTHÈSE

La synthèse décrit de manière brève et concise le contexte, les objectifs, la méthodologie et les prescriptions, les principales recommandations et la bonne pratique.

INTRODUCTION

- Objectifs ;
- Champ ;
- Carte simplifiée de l'architecture du réseau afin de s'assurer que l'équipe d'évaluation et l'organisme hôte comprennent de la même façon les limites de l'évaluation ;
- Méthodologie ;
- Définitions (au besoin).

RÉSULTATS DE L'ÉVALUATION

Constatations

- Les constatations sont obtenues par application des filtres des prescriptions aux observations. Énumération des constatations ;
- Il faut définir les documents prescriptifs tels que règlements, procédures, normes, bonne pratique, etc., et en indiquer les références avec la constatation ;
- Des observations peuvent être incluses ou non, mais on peut y renvoyer pour les constatations (ou les exclure si elles ont déjà été communiquées à l'installation).

Recommandations, suggestions et bonne pratique

- Il faut formuler les recommandations (pour les constatations) et les suggestions en les rattachant aux prescriptions ou à la ligne directrice citées en référence ;
- Si l'évaluation est effectuée par un État ou un organisme de réglementation, les recommandations peuvent être formulées de manière précise sous la forme, par exemple, de directives, d'avis d'action, etc. ;
- Les recommandations peuvent être classées conformément à une approche graduée en fonction du risque ou de l'impact potentiel pour l'installation. Il faut examiner la base de classement et en convenir lors de la réunion préalable à l'évaluation.

Stratégie d'atténuation (facultatif)

- L'adjonction d'une section sur une stratégie d'atténuation est une option qui peut être examinée préalablement à l'évaluation ;
- Si une stratégie d'atténuation doit être incluse dans le rapport final, il faut examiner le contenu de cette section avec le personnel de l'installation.

Analyse d'impact (facultatif)

— Une analyse de l'impact potentiel des constatations sur les domaines fonctionnels de l'installation comme la sûreté, la sécurité physique, la radioprotection, etc., peut être incluse dans le rapport. Cette analyse ne constituera pas une composante de toutes les évaluations, et le niveau d'analyse doit être examiné et convenu lors de la réunion de planification.

CONCLUSION

Cette section donne un aperçu général du résultat de l'évaluation et réitère les principales recommandations et suggestions ainsi que la bonne pratique au regard des prescriptions et de l'analyse des risques pour l'installation nucléaire. Si une stratégie d'atténuation est incluse dans le rapport final, un plan d'actions d'envergure peut être ajouté.

RÉFÉRENCES

Liste des documents/références utilisés pour l'évaluation et l'analyse :

— Prescriptions ;
— Guides réglementaires ;
— Normes ;
— Procédures, tout autre document utilisé, etc. ;
— Entretiens avec les salariés ;
— Emplois fonctionnels des interlocuteurs (responsable, ingénieur, technicien, etc.).

ABRÉVIATIONS

ANNEXE

— Calendrier d'évaluation ;
— Formulaires pour les observations ;
— Formulaires pour les constatations.

ANNEXE IV

CONSIDÉRATIONS RELATIVES À L'EXAMEN DES RÉSULTATS DU RAPPORT

La présente annexe fournit à l'organisme hôte des éléments à prendre en considération lors de l'examen des résultats figurant dans le rapport final d'évaluation. Le rapport contiendra un ensemble de constatations, d'observations, de recommandations et de suggestions. Chaque organisme disposera de ses propres processus pour l'élaboration d'un plan d'action à partir de ces résultats.

De multiples échelons de la hiérarchie, y compris la haute direction, doivent être impliqués dans l'examen du rapport. Cela est important pour faire en sorte que l'attention et les ressources voulues soient consacrées à l'élaboration d'un plan d'action. Certaines mesures correctives ou d'atténuation pourront être évidentes, mais d'autres exigeront peut-être une analyse approfondie. Les considérations ci-après pourront être utiles à l'appui du processus décisionnel concernant l'élaboration de ce plan d'action.

Impact

- Quel est le principal impact du rapport pour l'organisme ?
- Comment le rapport influe-t-il sur le profil de risque général de l'organisme ?

Atténuation

- Quelles sont les informations supplémentaires nécessaires pour prendre une décision ?
- Quelle est l'efficacité de la solution proposée ? (Dans quelle mesure les risques sont-ils réduits ?)
- Une solution unique permet-elle de donner suite à de multiples constatations ?
- Quel est l'impact de la mise en œuvre de la solution proposée (la mise en œuvre de la solution proposée a-t-elle, par exemple, des effets secondaires négatifs tels qu'une invalidation de la certification de systèmes, d'une licence ou de garanties) ?
- La solution proposée impose-t-elle des risques supplémentaires ou différents ?
- Quelles sont les mesures de substitution possibles à la solution recommandée ?
- Comment l'organisme peut-il vérifier que la recommandation proposée est efficace ?

Délai d'atténuation

- Quel est le délai pour la mise en œuvre de la recommandation ? Est-il suffisant pour remédier à la menace ?
- Quelles sont les conditions particulières à remplir pour mettre la solution en œuvre (par exemple, période d'arrêt et d'entretien) ?
- Peut-il être donné suite à la constatation grâce à des mesures intérimaires jusqu'à ce que des mesures plus permanentes soient en place ?
- L'organisme a-t-il, pour les projets futurs, des plans qui remédient aux problèmes ou les modifient ou qui offrent la possibilité d'y remédier ?

Coûts d'atténuation

- L'organisme possède-t-il le savoir-faire ou les compétences requis pour mettre la recommandation en œuvre ?
- Quels sont les coûts qu'entraîne la solution proposée ?
  - Coûts d'acquisition ;
  - Coûts de mise en œuvre ;
  - Coûts de communication pour la nouvelle solution ;
  - Coûts de formation du personnel ;
  - Coûts de formation des utilisateurs ;
  - Coûts en ce qui concerne la productivité et la commodité ;
  - Coûts d'audit et de vérification de l'efficacité ;
  - Coûts d'élimination en fin de vie.

Communications

- Y a-t-il intérêt à communiquer à des organismes extérieurs, par exemple aux vendeurs, aux partenaires industriels ou aux autorités compétentes, certains résultats de l'évaluation ?
- Si l'évaluation s'inscrit dans le cadre du processus réglementaire, l'autorité compétente peut exiger que le plan d'action et les mesures de suivi lui soient communiqués.

Autres considérations

- S'il s'agit d'une constatation récurrente, est-ce peut-être parce que le problème n'a pas été traité comme il convient ou que la mesure prise précédemment n'a pas été efficace ?
- L'ensemble de constatations est-il symptomatique d'un problème plus vaste de l'organisme ?
- Comment l'organisme peut-il éviter la répétition de cette constatation ou de constatations connexes à l'avenir ?
- Comment le suivi des résultats du rapport et du plan d'action sera-t-il assuré au sein de l'organisme ?

IAEA
Agence internationale de l'énergie atomique

N° 25

OÙ COMMANDER ?

Dans les pays suivants, vous pouvez vous procurer les publications de l'AIEA disponibles à la vente chez nos dépositaires ci-dessous ou dans les grandes librairies.

Les publications non destinées à la vente doivent être commandées directement à l'AIEA. Les coordonnées figurent à la fin de la liste ci-dessous.

ALLEMAGNE

Goethe Buchhandlung Teubig GmbH

Schweitzer Fachinformationen
Willstätterstrasse 15, 40549 Düsseldorf, ALLEMAGNE
Téléphone : +49 (0) 211 49 874 015 • Fax : +49 (0) 211 49 874 28
Courriel : kundenbetreuung.goethe@schweitzer-online.de • Site web : www.goethebuch.de

CANADA

Renouf Publishing Co. Ltd

22-1010 Polytek Street, Ottawa, ON K1J 9J1, CANADA
Téléphone : (+1 613) 745 2665 • Fax : +1 643 745 7660
Courriel : order@renoufbooks.com • Site web : www.renoufbooks.com

Bernan / Rowman & Littlefield

15200 NBN Way, Blue Ridge Summit, PA 17214, ÉTATS-UNIS D'AMÉRIQUE
Téléphone : +1 800 462 6420 • Fax : +1 800 338 4550
Courriel : orders@rowman.com • Site web : www.rowman.com/bernan

ÉTATS-UNIS D'AMÉRIQUE

Bernan / Rowman & Littlefield

15200 NBN Way, Blue Ridge Summit, PA 17214, ÉTATS-UNIS D'AMÉRIQUE
Téléphone : +1 800 462 6420 • Fax : +1 800 338 4550
Courriel : orders@rowman.com• Site web : www.rowman.com/bernan

Renouf Publishing Co. Ltd

812 Proctor Avenue, Ogdensburg, NY 13669-2205, ÉTATS-UNIS D'AMÉRIQUE
Téléphone : +1 888 551 7470 • Fax : +1 888 551 7471
Courriel : orders@renoufbooks.com • Site web : www.renoufbooks.com

FÉDÉRATION DE RUSSIE

Scientific and Engineering Centre for Nuclear and Radiation Safety

107140, Moscou, Malaya Krasnoselskaya st. 2/8, bld. 5, FÉDÉRATION DE RUSSIE
Téléphone : +7 499 264 00 03 • Fax : +7 499 264 28 59
Courriel : secnrs@secnrs.ru • Site web : www.secnrs.ru

FRANCE

Form-Edit

5 rue Janssen, B.P. 25, 75921 Paris CEDEX, FRANCE
Téléphone : +33 1 42 01 49 49 • Fax : +33 1 42 01 90 90
Courriel : formedit@formedit.fr • Site web : www.form-edit.com

INDE

Allied Publishers

1st Floor, Dubash House, 15, J.N. Heredi Marg, Ballard Estate, Mumbai 400001, INDE
Téléphone : +91 22 4212 6930/31/69 • Fax : +91 22 2261 7928
Courriel : alliedpl@vsnl.com • Site web : www.alliedpublishers.com

Bookwell

3/79 Nirankari, Delhi 110009, INDE
Téléphone : +91 11 2760 1283/4536
Courriel : bkwell@nde.vsnl.net.in • Site web : www.bookwellindia.com

ITALIE

Libreria Scientifica “AEIOU”

Via Vincenzo Maria Coronelli 6, 20146 Milan, ITALIE
Téléphone : +39 02 48 95 45 52 • Fax : +39 02 48 95 45 48
Courriel : info@libreriaaeiou.eu • Site web : www.libreriaaeiou.eu

JAPON

Maruzen-Yushodo Co., Ltd

10-10 Yotsuyasakamachi, Shinjuku-ku, Tokyo 160-0002, JAPON
Téléphone : +81 3 4335 9312 • Fax : +81 3 4335 9364
Courriel : bookimport@maruzen.co.jp • Site web : www.maruzen.co.jp

RÉPUBLIQUE TCHÈQUE

Suweco CZ, s.r.o.

Sestupná 153/11, 162 00 Prague 6, RÉPUBLIQUE TCHÈQUE
Téléphone : +420 242 459 205 • Fax : +420 284 821 646
Courriel : nakup@suweco.cz • Site web : www.suweco.cz

Les commandes de publications destinées ou non à la vente peuvent être adressées directement à :

Unité de la promotion et de la vente
Agence internationale de l’énergie atomique
Centre international de Vienne, B.P. 100, 1400 Vienne, AUTRICHE
Téléphone : +43 1 2600 22529 ou 22530 • Fax : +43 1 2600 29302 ou +43 1 26007 22529
Courriel : sales.publications@iaea.org • Site web : www.iaea.org/books

17-19762

Agence internationale de l'énergie atomique
Vienne
ISBN 978–92–0–206517–8