PREMIER MINISTRE
Secrétariat général de la défense nationale
Direction centrale de la sécurité des systèmes d'information
Sous-direction des opérations
Bureau conseil

Maturité SSI

Approche méthodologique

Version du 2 novembre 2007

51 boulevard de La Tour-Maubourg - 75700 PARIS 07 SP - Tél 01 71 75 84 15 - Fax 01 71 75 84 00

Ce document a été réalisé par le bureau conseil de la DCSSI
(SGDN / DCSSI / SDO / BCS)

en collaboration avec le Club EBIOS

Les commentaires et suggestions sont encouragés et peuvent être adressés à l'adresse suivante :

Secrétariat général de la défense nationale
Direction centrale de la sécurité des systèmes d'information
Sous-direction des opérations
Bureau Conseil
51 boulevard de La Tour-Maubourg
75700 PARIS 07 SP

conseil.dcssi@sgdn.pm.gouv.fr

Historique des modifications

Date	Objet de la modification	Auteur(s)	Statut
26/10/2005	Création du document	SGDN	Validé
14/09/2007	Révision du document sur la base des retours d'expérience et du marché public N°2006 00683 00 2 12 075 01 – Réalisation d'études relatives à la gouvernance de la sécurité des systèmes d'information (SSI)	SGDN	Document de travail
02/11/2007	Prise en compte des commentaires des membres du Club EBIOS	SGDN	Validé

Table des matières

Introduction

La sécurité des systèmes d'information (SSI) d'un organisme[1] doit être gérée en adéquation par rapport à ses véritables enjeux SSI. En effet, des enjeux faibles ne requièrent pas de gérer la SSI de manière aussi rigoureuse que lorsqu'ils sont élevés. Cet énoncé, simple en apparence, est une gageure si l'on souhaite y répondre simplement et sans investissements importants.

À l'aide de questionnements pragmatiques, le présent guide a pour objectifs de déterminer rapidement les enjeux liés au système d'information de l'organisme, de mesurer l'écart entre ce qui devrait être fait et ce qui est fait, et d'expliquer les actions à mettre en œuvre pour gérer la SSI de manière adéquate.

L'approche s'inspire de l'[ISO 21827][2]. Cette norme définit des niveaux de maturité, dits "cumulatifs", de la gestion de la SSI. La description détaillée de ces niveaux figure en annexe. Chacun représente la manière dont un organisme exécute, contrôle, maintient et assure le suivi d'un processus. L'atteinte d'un niveau suppose d'avoir déjà atteint le précédent.

Niveau 0. Pratique inexistante ou incomplète : pratiques de base éventuellement mises en œuvre et le besoin n'est pas reconnu.

Niveau 1. Pratique informelle : pratiques de base mises en œuvre de manière informelle et réactive à l'initiative de ceux qui estiment en avoir besoin.

Niveau 2. Pratique répétable et suivie : pratiques de base mises en œuvre de façon planifiée et suivie, avec un support relatif de l'organisme.

Niveau 3. Processus défini : mise en œuvre d'un processus décrit, adapté à l'organisme, généralisé et bien compris par le management et par les exécutants.

Niveau 4. Processus contrôlé : le processus est coordonné et contrôlé à l'aide d'indicateurs permettant de corriger les défauts constatés.

Niveau 5. Processus continuellement optimisé : l'amélioration des processus est dynamique, institutionnalisée et tient compte de l'évolution du contexte.

Ces niveaux s'appliquent aux processus SSI qui, d'une manière générique, sont les suivants :

- les processus de pilotage de la SSI, qui permettent de diriger et contrôler la SSI :
  - définir la stratégie SSI,
  - gérer les risques SSI,
  - gérer les règles SSI,
  - superviser la SSI ;
- les processus SSI opérationnels, qui constituent les "processus métiers" de la SSI :
  - concevoir les mesures SSI,
  - réaliser les mesures SSI,
  - exploiter les mesures SSI.

Note : les processus de support ne sont pas spécifiques à la SSI ; il s'agit des processus de support courants d'un organisme (communiquer, gérer les ressources humaines, gérer les contrats…), dont le niveau de maturité ne sera pas étudié.

Connaître le niveau adéquat de maturité SSI constitue la première étape de la réflexion (chapitre 1), qui devrait être menée par l'autorité responsable du(des) périmètre(s) choisi(s). L'analyse des niveaux effectifs par les responsables des processus SSI permet ensuite d'obtenir une "photographie" des niveaux réellement atteints (chapitre 2). Le plan d'action consistera alors à définir les actions à mener et les ressources à allouer afin d'atteindre le niveau adéquat de maturité SSI (chapitre 3).

[1] Terme générique employé pour évoquer une entreprise, un ministère, un organisme sous-tutelle…

[2] Ces travaux sont l'héritage direct des méthodes du domaine du développement logiciel autour du *Capacity Maturity Model*, développé par l'Université de Carnegie Mellon et repris en Europe par l'ESI.

1 Démarche pour déterminer le niveau adéquat

1.1 Choix du(des) périmètre(s)

Le niveau adéquat de maturité SSI peut être appliqué à différents périmètres.

Bien qu'il soit possible de considérer un organisme dans son intégralité, il est souvent plus pertinent de limiter la réflexion à une sous-partie de celui-ci : une direction, un service, un système d'information, un système de management de la SSI, un projet…

En effet, si le périmètre considéré est très vaste, le niveau adéquat de maturité SSI correspondra à la partie du périmètre qui demande le plus de rigueur. Il sera donc probablement trop élevé pour le reste du périmètre.

Par conséquent, il convient de choisir un(des) périmètre(s) relativement homogène(s) en termes de responsabilité.

Le questionnaire qui suit devrait être utilisé par l'autorité responsable du périmètre choisi (le Directeur, le responsable du service, le chef de projet… selon le cas).

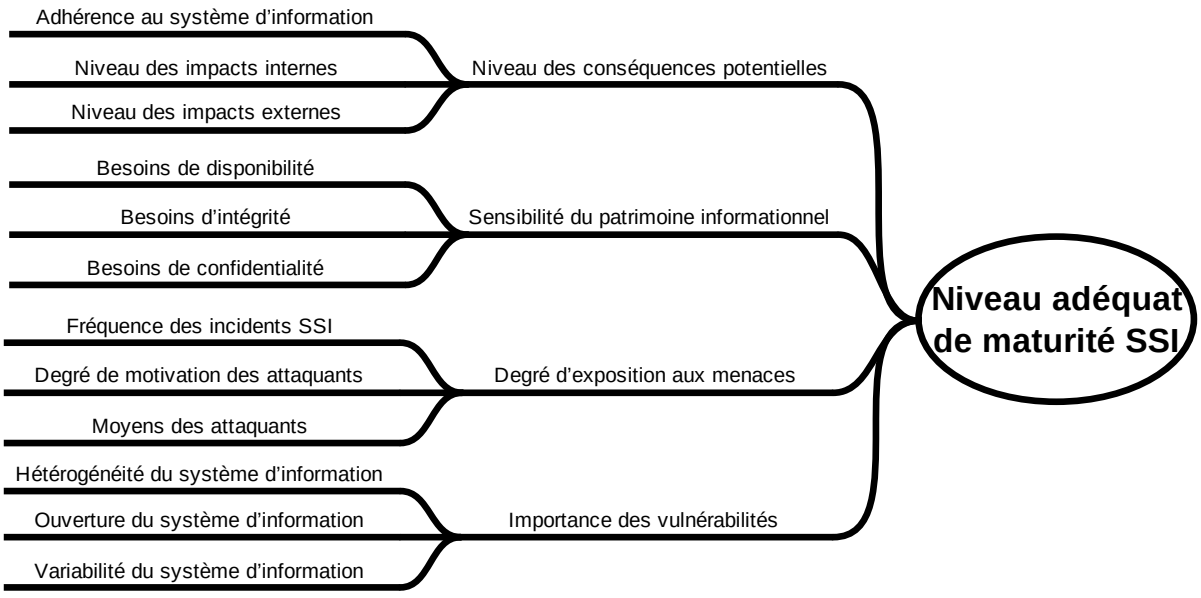
1.2 Autodiagnostic en 12 questions par l'autorité responsable du périmètre

1.2.1 Une estimation basée sur les enjeux SSI

Le "bon" niveau de maturité SSI n'est pas le plus élevé, mais le niveau adéquat au regard des besoins opérationnels et des menaces qui pèsent sur le système d'information.

Le questionnaire aborde donc les principaux enjeux liés au périmètre choisi :
- le niveau des conséquences potentielles (en cas de sinistre SSI),
- la sensibilité du patrimoine informationnel,
- le degré d'exposition aux menaces,
- l'importance des vulnérabilités.

Les enjeux sont chacun abordés à l'aide de trois questions, pour au final déterminer le niveau adéquat de maturité SSI :



Les réponses du responsable du périmètre traduiront sa vision des enjeux relatifs à la SSI. Elles permettront de définir son objectif général et la cible à atteindre : le niveau adéquat de maturité SSI.

1.2.2 Trois questions pour estimer le niveau des conséquences potentielles

Question 1 – Adhérence au système d'information : Comment jugez-vous l'importance de votre système d'information dans l'accomplissement de vos missions ?

Cette question a pour objectif d'évaluer le degré de dépendance au système d'information.

Réponses	Valeur
Le système d'information est accessoire à l'accomplissement des missions	0
Le système d'information est utile à l'accomplissement des missions	1
Le système d'information est nécessaire à l'accomplissement des missions	2
Le système d'information est vital à l'accomplissement des missions	3

Question 2 – Niveau des impacts internes : Quelles sont les conséquences internes (perturbations du fonctionnement, impacts financiers, impacts juridiques…) d'un sinistre touchant la sécurité de votre système d'information (ex : déni de service, perte d'informations, attaque virale…) ?

Cette question permet d'évaluer la portée des impacts internes suite à un sinistre.

Réponses	Valeur
Les conséquences internes d'un sinistre SSI ne peuvent qu'être négligeables	0
Les conséquences internes d'un sinistre SSI peuvent être significatives	1
Les conséquences internes d'un sinistre SSI peuvent être graves	2
Les conséquences internes d'un sinistre SSI peuvent être fatales	3

Question 3 – Niveau des impacts externes : Quelles sont les conséquences externes (image, sécurité de l'environnement, relations contractuelles, sécurité des personnes…) d'un sinistre touchant la sécurité de votre système d'information ?

Cette question permet d'évaluer la portée des impacts externe suite à un sinistre. L'implication des tiers dans les impacts entraine l'élévation du niveau de maturité.

Réponses	Valeur
Les conséquences externes d'un sinistre SSI ne peuvent qu'être négligeables	0
Les conséquences externes d'un sinistre SSI peuvent être significatives	1
Les conséquences externes d'un sinistre SSI peuvent être graves	2
Les conséquences externes d'un sinistre SSI peuvent être catastrophiques	3

Le **niveau des conséquences potentielles**
est égal à la valeur maximale des réponses aux questions 1 à 3.

1.2.3 Trois questions pour estimer la sensibilité du patrimoine informationnel

Question 4 – Besoins de disponibilité (propriété d'accessibilité au moment voulu par des personnes autorisées) : Dans quelle mesure la disponibilité du(des) système(s) informatique(s) est-elle importante ?

Cette question permet d'évaluer le besoin en disponibilité du patrimoine informationnel à partir du niveau d'impact que pourrait engendrer une indisponibilité.

Réponses	Valeur
L'inaccessibilité du(des) système(s) informatique(s) ne gêne quasiment pas l'activité	0
L'inaccessibilité du(des) système(s) informatique(s) perturbe l'activité de manière significative	1
L'inaccessibilité du(des) système(s) informatique(s) est jugée comme grave pour l'activité	2
L'inaccessibilité du(des) système(s) informatique(s) peut être fatale pour l'activité	3

Question 5 – Besoins d'intégrité (propriété d'exactitude et de complétude) : Dans quelle mesure l'intégrité des données manipulées ou manipulables dans le cadre de l'activité est-elle importante ?

Cette question permet d'évaluer le besoin en intégrité du patrimoine informationnel à partir du niveau d'impact que pourrait engendrer une modification non avenue des informations.

Réponses	Valeur
L'altération des données ne gêne quasiment pas l'activité	0
L'altération des données perturbe l'activité de manière significative	1
L'altération des données est jugée comme grave pour l'activité	2
L'altération des données peut être fatale pour l'activité	3

Question 6 – Besoins de confidentialité (propriété de n'être accessible qu'aux personnes autorisées) : Dans quelle mesure la confidentialité des informations exploitées ou exploitables dans le cadre de l'activité est-elle importante ?

Cette question permet d'évaluer le besoin en confidentialité du patrimoine informationnel à partir du niveau d'impact que pourrait engendrer une perte ou divulgation des informations.

Réponses	Valeur
La compromission d'informations ne gêne quasiment pas l'activité	0
La compromission d'informations perturbe l'activité de manière significative	1
La compromission d'informations est jugée comme grave pour l'activité	2
La compromission d'informations peut être fatale pour l'activité	3

La **sensibilité du patrimoine informationnel**
est égale à la valeur maximale des réponses aux questions 4 à 6.

1.2.4 Trois questions pour estimer le degré d'exposition aux menaces

Question 7 – Fréquence des sinistres SSI : Quelle est la fréquence estimée des sinistres SSI dans l'organisme ?

Cette question vise à évaluer la fréquence des sinistres SSI, qu'ils soient accidentels ou délibérés. Plus cette valeur est importante, plus l'organisme aura besoin d'être vigilant.

Réponses	Valeur
Les sinistres SSI (vécus ou imaginables) sont rarissimes (moins d'une fois par an)	0
Plusieurs sinistres SSI dans l'année	1
Plusieurs sinistres SSI par trimestre	2
Plusieurs sinistres SSI par mois	3

Question 8 – Degré de motivation des attaquants : Quel est le degré de motivation des attaquants potentiels ?

Cette question vise à évaluer le degré de motivation supposé des attaquants auxquels on estime pouvoir être confronté. La motivation peut être de caractère stratégique, idéologique, politique, terroriste, cupide, ludique, vengeur… et son niveau peut donc fortement varier.

Réponses	Valeur
Une attaque SSI ciblée sur le périmètre est relativement inimaginable	0
La motivation des attaquants potentiels est jugée faible	1
La motivation des attaquants potentiels peut être forte	2
La motivation des attaquants potentiels peut être très importante	3

Question 9 – Moyens des attaquants : Quels sont les compétences et les ressources des attaquants potentiels ?

Cette question vise à évaluer, dans l'absolu, les compétences et les ressources supposées des attaquants auxquels on estime pouvoir être confronté. Plus l'attaquant est compétent et dispose de moyens importants, plus il sera difficile de le contrer.

Réponses	Valeur
Les attaquants potentiels ne disposent que de faibles moyens	0
Les attaquants peuvent disposer de moyens significatifs	1
Les attaquants peuvent disposer de moyens importants	2
Les attaquants peuvent disposer de moyens potentiellement illimités	3

Le **degré d'exposition aux menaces**
est égal à la valeur maximale des réponses aux questions 7 à 9.

1.2.5 Trois questions pour estimer l'importance des vulnérabilités

Question 10 – Hétérogénéité du système d'information : Quel est le niveau d'hétérogénéité du système d'information ?

Cette question vise à évaluer le niveau d'hétérogénéité (variété des composants et complexité de l'architecture fonctionnelle, physique et réseau) du système d'information. Plus celui-ci est élevé, plus le niveau de vulnérabilité aura tendance à l'être également.

Réponses	Valeur
Le système d'information est jugé comme homogène	0
Le système d'information est jugé comme faiblement hétérogène	1
Le système d'information est jugé comme fortement hétérogène	2
Le système d'information est jugé comme extrêmement hétérogène	3

Question 11 – Ouverture du système d'information : Quel est le degré d'ouverture du système d'information ?

Cette question vise à évaluer le degré d'ouverture du système d'information. Cela prend en compte l'interconnexion avec d'autres systèmes d'information internes ou externes avec plus ou moins de maîtrise et de contrôle de l'organisme.

Réponses	Valeur
Le système d'information n'est pas ouvert	0
Le système d'information n'est ouvert qu'à des systèmes internes	1
Le système d'information est ouvert à des systèmes externes mais sous contrôle	2
Le système d'information est ouvert à des systèmes externes hors de contrôle	3

Question 12 – Variabilité du système d'information : Quel est le niveau de variabilité des composants du système d'information (matériels, logiciels, réseaux, organisations, locaux, personnel…) et du contexte dans lequel il opère (contraintes, exigences réglementaires, menaces…) ?

Cette question vise à évaluer la stabilité du système d'information. Le changement augmente le niveau de risque, et donc la rigueur avec laquelle la SSI devrait être gérée.

Réponses	Valeur
Le système d'information et son contexte sont jugés stables	0
Le système d'information et son contexte changent peu	1
Le système d'information et son contexte changent relativement souvent	2
Le système d'information et son contexte change très souvent	3

L'**importance des vulnérabilités**
est égale à la valeur maximale des réponses aux questions 10 à 12.

1.2.6 Détermination du niveau adéquat de maturité SSI

Après avoir répondu aux douze questions de l'autodiagnostic et gardé les valeurs maximales des quatre thèmes, on dispose de quatre valeurs :

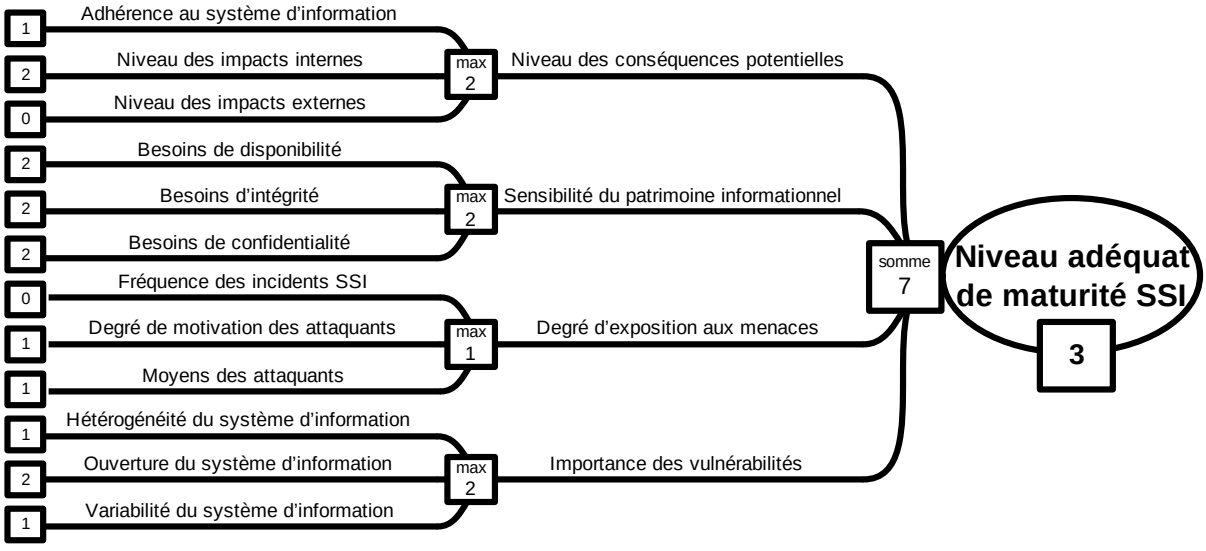
- le niveau des conséquences potentielles (en cas de sinistre SSI),
- la sensibilité du patrimoine informationnel,
- le degré d'exposition aux menaces,
- l'importance des vulnérabilités.

Il suffit alors d'additionner ces quatre valeurs et de comparer le résultat au tableau suivant pour obtenir le niveau adéquat de maturité SSI :

Somme des quatre valeurs	Niveau adéquat de maturité SSI
De 0 à 2	1 - Pratique informelle
De 3 à 5	2 - Pratique répétable et suivie
De 6 à 8	3 - Processus définis
De 9 à 10	4 - Processus contrôlés
De 11 à 12	5 - Processus continuellement optimisés

Un arbre de détermination du niveau adéquat de maturité SSI est proposé en annexe.

Par exemple, des réponses menant à un résultat de 7 amènent la maturité adéquate au niveau 3 :



1.2.7 Ajustement du niveau global (optionnel)

L'autorité responsable du périmètre considéré peut ajuster le niveau adéquat de maturité SSI obtenu à l'aide de l'autodiagnostic. Il s'agit en effet d'une aide à l'expression de ses propres objectifs. La taille et la capacité du périmètre peuvent notamment influencer ce choix. Cette décision doit néanmoins être justifiée et ne pas varier de plus d'un niveau. Réduire le niveau adéquat peut exposer l'organisme à des risques liés à une gestion de la SSI inadaptée au regard des enjeux. L'augmenter peut engendrer des dépenses non nécessaires.

1.2.8 Ajustement du niveau par processus (optionnel)

Il est également possible d'ajuster le niveau adéquat de maturité SSI selon chaque processus SSI (définir la stratégie SSI, gérer les risques SSI…). Il est néanmoins souhaitable de ne pas varier de plus d'un niveau et de justifier cette décision.

1.3 Agrégation des résultats de plusieurs périmètres (optionnel)

Dans le cas où plusieurs niveaux adéquats de maturité SSI ont été déterminés au sein d'un même organisme (par exemple un niveau par Direction d'un organisme), il est possible et utile d'agréger les différents résultats.

Pour ce faire, il est généralement utile de calculer **la moyenne** et **l'écart type** des niveaux adéquats de maturité SSI des différents périmètres. On peut ainsi disposer d'une vision synthétique et suivre aisément son évolution.

Cette agrégation sera uniquement informative. Elle ne reflète pas le niveau adéquat de maturité SSI de l'organisme. Néanmoins, elle servira à suivre l'évolution dans le temps en réitérant l'opération régulièrement (par exemple une fois par an).

2 Démarche pour déterminer les niveaux effectifs

2.1 Identification des processus SSI dans le(s) périmètre(s) choisi(s)

Le positionnement des processus SSI en terme de maturité requiert de reconnaître ces processus au sein de l'organisation existante.

En effet, les sept principaux processus SSI, définis de manière générique, ne se concrétisent pas sous la même forme dans tous les organismes. Il se peut même que certains n'existent pas, notamment :

- si les processus sont mis en œuvre en dehors du périmètre (dans un autre service, dans un autre organisme…),
- si les processus n'existent tout simplement pas (les processus peuvent avoir été jugés comme non opportuns au vu du périmètre présent, ou bien ils n'ont pas été pensés jusque là et devraient être créés).

Il convient donc de commencer par vérifier l'existence des activités liées aux processus suivants, dans le(s) même(s) périmètre(s) que celui(ceux) dont le niveau adéquat a été déterminé précédemment :

Catégorie	Processus génériques	Objectif
Processus de pilotage de la SSI	Définir la stratégie SSI	Disposer d'objectifs SSI mesurables, d'orientations SSI et d'un plan d'action adaptés au niveau adéquat de maturité SSI et alignés avec la stratégie de l'organisme.
	Gérer les risques SSI	Identifier les risques SSI et les maintenir à un niveau acceptable pour l'organisme compte tenu de son contexte.
	Gérer les règles SSI	Disposer de règles SSI pertinentes et basées sur la gestion des risques SSI, prévoir les actions à entreprendre pour se conformer aux règles SSI et disposer d'éléments pour vérifier la conformité aux règles SSI.
	Superviser la SSI	Définir un cadre de contrôle adapté, puis s'assurer que le contrôle est effectué conformément au cadre défini et disposer de résultats pertinents et directement exploitables.
Processus SSI opérationnels	Concevoir les mesures SSI	Assurer l'intégration de la mesure dans son contexte opérationnel et rédiger les caractéristiques générales puis détaillées de la mesure afin d'obtenir un cahier des charges.
	Réaliser les mesures SSI	Concevoir ou d'acquérir la mesure, l'intégrer et en valider le prototype en vue de le déployer.
	Exploiter les mesures SSI	Déployer et mettre en état opérationnel la mesure, assurer la conformité et le suivi opérationnel de la mesure et identifier les incidents et remettre le Système d'Information en état opérationnel selon les exigences SSI.

L'outil de positionnement qui suit devrait être utilisé par la personne en charge des activités concernées (le responsable du processus).

2.2 Un constat basé sur les pratiques existantes

Pour chaque processus SSI générique, son responsable doit identifier le niveau dont la description correspond à la manière dont il est effectivement réalisé.

Si tous les points d'une description ne sont pas réalisés, alors le niveau n'est pas atteint. Il convient idéalement de s'assurer que des éléments de preuve peuvent être fournis.

Les réponses des responsables des processus SSI traduiront leur perception de la manière dont ceux-ci sont actuellement gérés.

2.3 Positionnement de chaque processus SSI par son responsable

Les différents niveaux de maturité SSI sont synthétisés par la manière dont un organisme exécute, contrôle, maintient et assure le suivi des processus. D'une manière générique, ils peuvent être décrits sous la forme d'exigences d'atteinte du niveau.

2.3.1 Niveau 1 – Pratique informelle : quelques actions isolées

- Des actions sont réalisées en employant des pratiques de base.

2.3.2 Niveau 2 – Pratique répétable et suivie : des actions reproductibles

- Les actions sont planifiées.
- Les actions sont réalisées par une personne qui possède des compétences en SSI.
- Certaines pratiques sont formalisées, ce qui permet la duplication et la réutilisation (éventuellement par une autre personne).
- Des mesures qualitatives sont réalisées (indicateurs simples sur les résultats).
- Les autorités compétentes sont tenues informées des mesures effectuées.

2.3.3 Niveau 3 – Processus défini : la standardisation de pratiques

- Les actions sont réalisées conformément à un processus défini (ex : adaptation au contexte, emploi d'une méthode), standardisé (commun à tout l'organisme) et formalisé (existence d'une documentation).
- Les personnes réalisant les actions possèdent les compétences appropriées au processus.
- L'organisme soutien le processus et accorde les ressources, les moyens et la formation nécessaires à son fonctionnement. Le processus est bien compris autant par le management que par les exécutants.

2.3.4 Niveau 4 – Processus contrôlé : la mesure quantitative

- Le processus est coordonné dans tout le périmètre choisi et pour chaque exécution.
- Des mesures quantitatives sont régulièrement effectuées (en termes de performance).
- Les mesures effectuées (indicateurs qualitatifs et quantitatifs) sont analysées.
- Des améliorations sont apportées au processus à partir de l'analyse des mesures effectuées.

2.3.5 Niveau 5 – Processus optimisé : l'amélioration continue

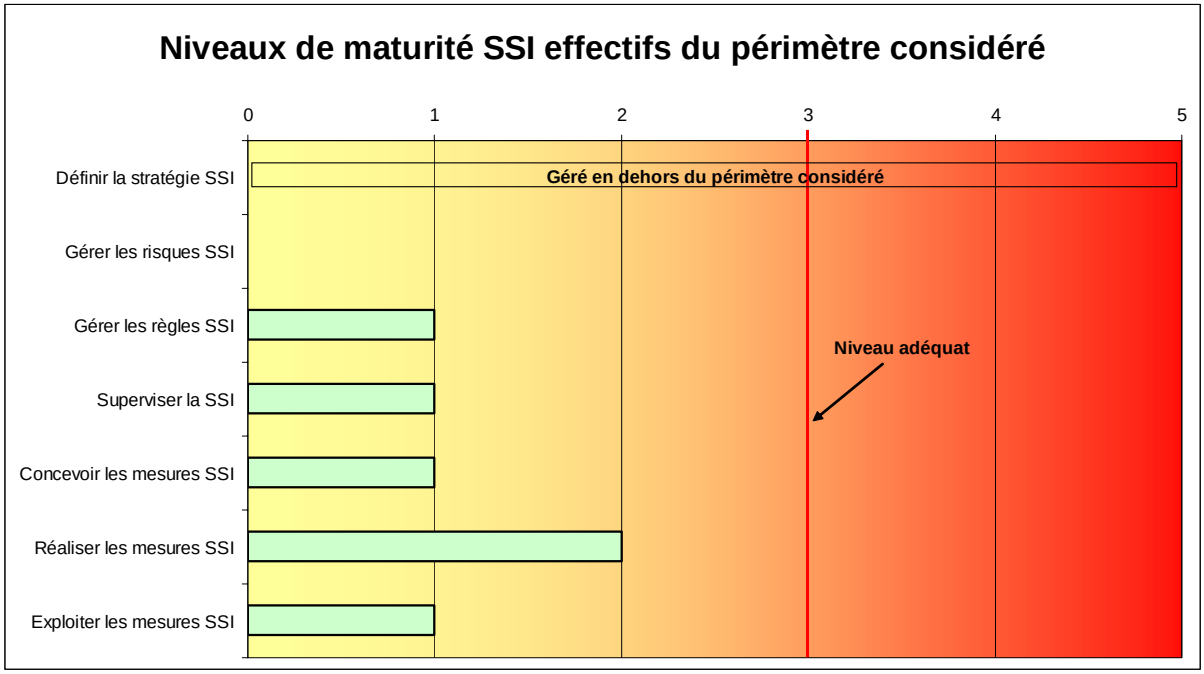
- Le processus est adapté de façon dynamique à la situation.
- L'analyse des mesures effectuées est définie, standardisée et formalisée.
- L'amélioration du processus est définie, standardisée et formalisée.
- Les évolutions du processus sont journalisées.

Un tableau permettant de déterminer les niveaux effectifs est proposé en annexe. Il pourra ensuite être tenu à jour quand les niveaux effectifs évolueront.

Exemple :

Exigences d'atteinte du niveau de maturité SSI	***Définir la stratégie SSI***	***Gérer les risques SSI***	***Gérer les règles SSI***	***Superviser la SSI***	***Concevoir les mesures SSI***	***Réaliser les mesures SSI***	***Exploiter les mesures SSI***
Des actions sont réalisées en employant des pratiques de base			X	X	X	X	X
Niveau 1			***Complet***	***Complet***	***Complet***	***Complet***	***Complet***
Les actions sont planifiées				X	X	X	
Les acteurs sont compétents en SSI		X	X	X	X	X	X
Certaines pratiques sont formalisées						X	X
Des mesures qualitatives sont réalisées			X			X	
Les autorités compétentes sont informées des mesures effectuées			X			X	
Niveau 2						***Complet***	
Le processus est défini, standardisé et formalisé							
Les acteurs ont des compétences appropriées au processus				X		X	X
L'organisme soutien le processus			X	X	X	X	X
Niveau 3							
Le processus est coordonné dans tout le périmètre choisi			X	X			
Des mesures quantitatives sont régulièrement effectuées							
Les mesures effectuées sont analysées							
Le processus est amélioré en fonction des mesures effectuées							
Niveau 4							
Le processus est adapté de façon dynamique à la situation							
L'analyse des mesures est définie, standardisée et formalisée							
L'amélioration du processus est définie, standardisée et formalisée							
Les évolutions du processus sont journalisées							
Niveau 5							
Niveau effectif de maturité SSI des processus	***-***	***0***	***1***	***1***	***1***	***2***	***1***

On peut synthétiser les résultats de la manière suivante :



Note : Le processus "Définir la stratégie SSI" est géré en dehors du périmètre considéré. Il n'a pas été jugé opportun de le créer car la volonté de l'organisme est de piloter la stratégie au sein d'un périmètre dédié.

2.4 Agrégation des résultats de plusieurs périmètres (optionnel)

Dans le cas où plusieurs périmètres ont été déterminés au sein d'un même organisme, il est possible et utile d'agréger les différents résultats.

Pour ce faire, il est généralement intéressant de calculer **la moyenne** et **l'écart type** des niveaux effectifs de maturité SSI des différents périmètres par processus SSI générique. On peut ainsi disposer d'une vision synthétique et suivre aisément son évolution.

Cette agrégation sera uniquement informative. Elle ne reflète pas le niveau effectif de maturité SSI des différents processus SSI. Néanmoins, elle servira à suivre l'évolution dans le temps en réitérant l'opération régulièrement (par exemple une fois par an).

3 Démarche pour atteindre le niveau adéquat

3.1 Principe général : commencer par les processus dont le niveau est le plus faible

Pour passer du niveau de maturité SSI effectif au niveau de maturité SSI adéquat, l'organisme devra progressivement faire évoluer ses pratiques. L'échelle de maturité étant cumulative, l'atteinte d'un niveau suppose l'atteinte préalable du niveau précédent.

L'objectif de la démarche est de planifier une série d'actions permettant de faire évoluer progressivement la maturité effective jusqu'à la faire converger avec le niveau adéquat du périmètre. Il est conseillé de mener cette progression par étapes successives, chacune ayant pour effet d'augmenter la maturité d'un niveau.

Le principe consiste à toujours commencer par les processus dont le niveau effectif est le plus bas pour uniformiser les niveaux effectifs de maturité SSI et de réitérer l'opération pour atteindre le niveau adéquat de maturité : on travaillera d'abord sur les processus dont le niveau est égale à 0, puis sur ceux dont le niveau est égale à 1 et ainsi de suite. Cette approche permettra d'obtenir des résultats visibles et des gains rapides.

Chacune de ces étapes devrait faire l'objet d'un plan d'action, permettant de répondre aux exigences d'atteinte du niveau suivant.

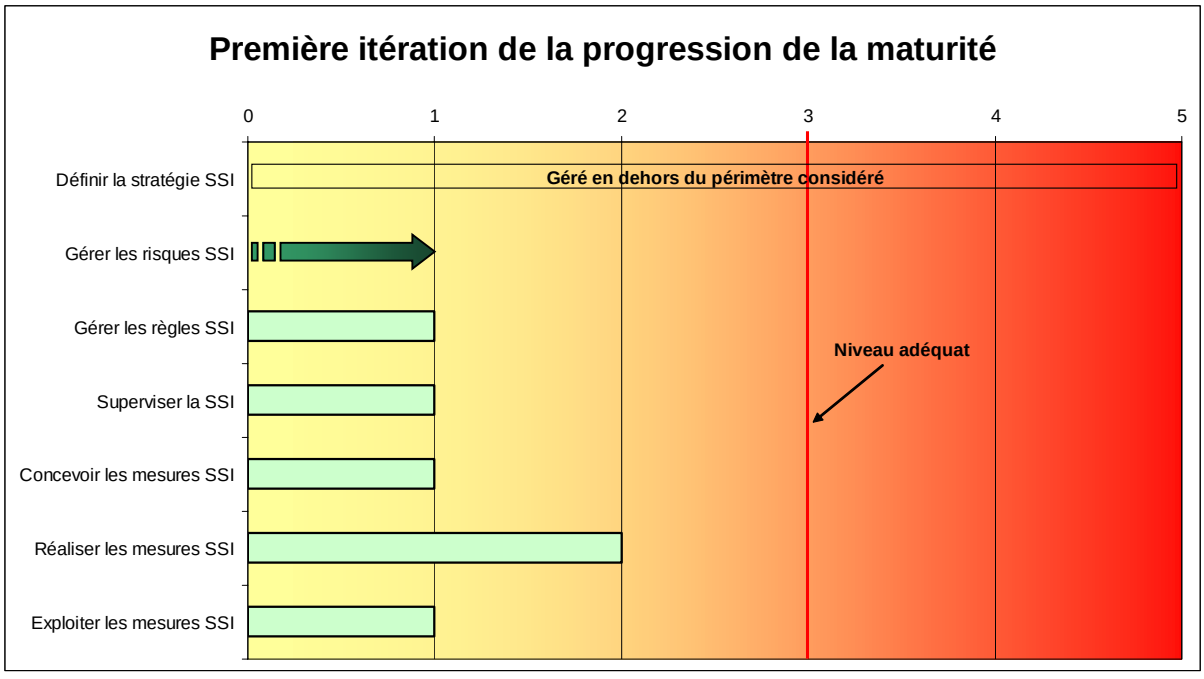
Il est également conseillé de prévoir une phase de stabilisation entre chaque étape afin de laisser au processus le temps de s'adapter au nouveau fonctionnement.

3.2 Conseils pour identifier les étapes de progression

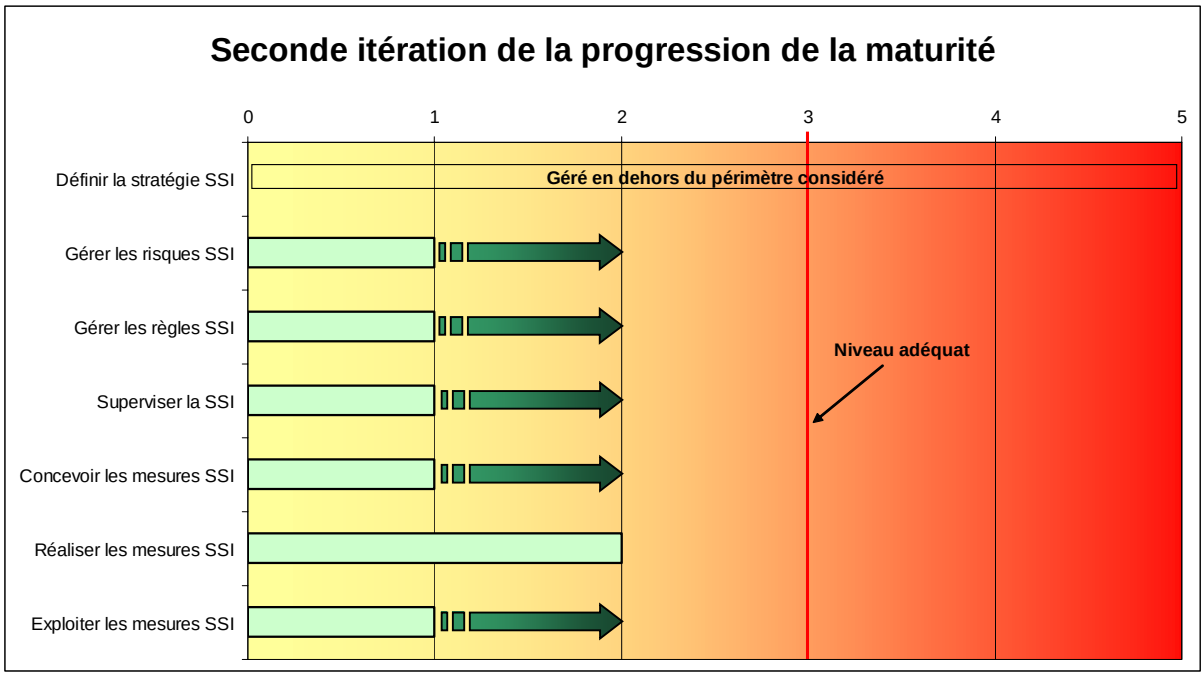
Il convient tout d'abord d'identifier les étapes de progression des niveaux effectifs de maturité SSI. Chaque étape consistera à faire évoluer les processus dont le niveau effectif est minimal.

Exemple :

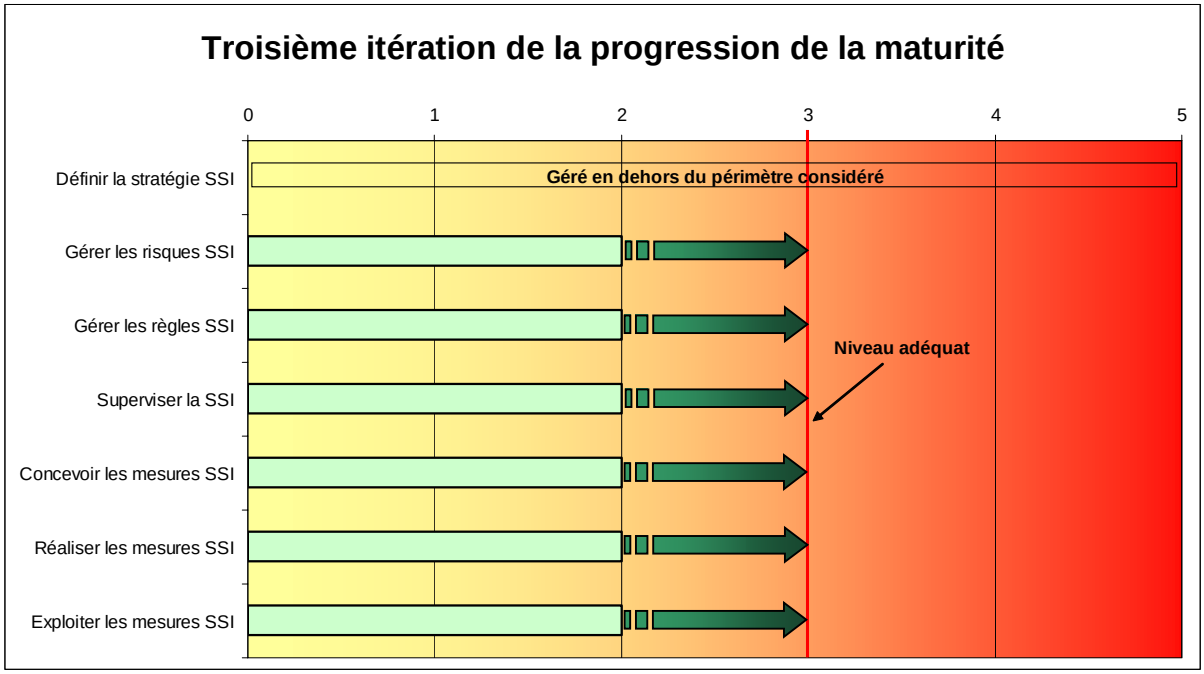
- *Étape 1 – Passer le processus "gérer les risques SSI" au niveau 1 de maturité (le processus "Définir la stratégie SSI" est géré en dehors du périmètre considéré, il n'a pas besoin d'être crée ni augmenter au sein de celui-ci) :*



- *Étape 2 – Passer les processus "gérer les risques SSI", "gérer les règles SSI", "Superviser la SSI" et "Exploiter les mesures SSI" au niveau 2 de maturité :*



- *Étape 3 – Passer tous les processus au niveau 3 de maturité :*



3.3 Conseils pour établir les plans d'action

Un plan d'action devrait être élaboré pour chaque processus devant augmenter sa maturité effective d'un niveau (si trois processus doivent progresser dans une étape, trois plans d'actions seront établis).

Chaque plan d'action devrait planifier les actions nécessaires pour que le processus satisfasse les exigences d'atteinte du niveau ciblé (actions, responsables, livrables, calendrier…). Ceci permettra de compléter le tableau des niveaux effectifs.

Dans notre exemple, la première étape consiste à faire passer le processus "Gérer les risques SSI" du niveau 0 au niveau 1. Il convient donc de satisfaire l'exigence d'atteinte suivante : "Des actions sont réalisées en employant des pratiques de base". Le plan d'action prévoira d'identifier des bonnes pratiques simples et exploitables pour gérer les risques lorsque des individus en ressentent le besoin.

Conclusion

Une démarche de maturité SSI permet de définir simplement et rapidement les pratiques nécessaires et suffisantes en matière de SSI.

En outre, la facilité de positionnement en terme de maturité SSI et son approche "*benchmarking*" fait de cet outil un élément de marketing pour la SSI, parfaitement adapté à la communication envers les plus hauts niveaux de décision.

Enfin, l'utilisation de la démarche, notamment la détermination d'un niveau de maturité SSI adéquat, fournit les éléments fondamentaux à l'élaboration de schémas directeurs SSI ou de politiques SSI, à la mise en place d'un système de management de la SSI, à l'intégration de la SSI dans les projets…

Annexes

Glossaire

Niveau de maturité	Le niveau de maturité mesure le degré d'amélioration d'un processus dans un groupe prédéfini de pratiques qui ont atteint leur but. [SEI 2006]
Processus	Ensemble d'activités organisées dans le temps et en fonction d'un but. [ISO 2382-1]
Disponibilité	Propriété d'accessibilité au moment voulu du patrimoine informationnel par les personnes autorisées.
Intégrité	Propriété d'exactitude et de complétude du patrimoine informationnel.
Confidentialité	Propriété du patrimoine informationnel de n'être accessible qu'aux personnes autorisées.
Système d'information (SI)	Ensemble de matériels, logiciels, réseaux, organisations, sites et personnels, organisé pour traiter des informations.
Sécurité des systèmes d'information (SSI)	Satisfaction des besoins de sécurité (disponibilité, intégrité, confidentialité…) des systèmes d'information.

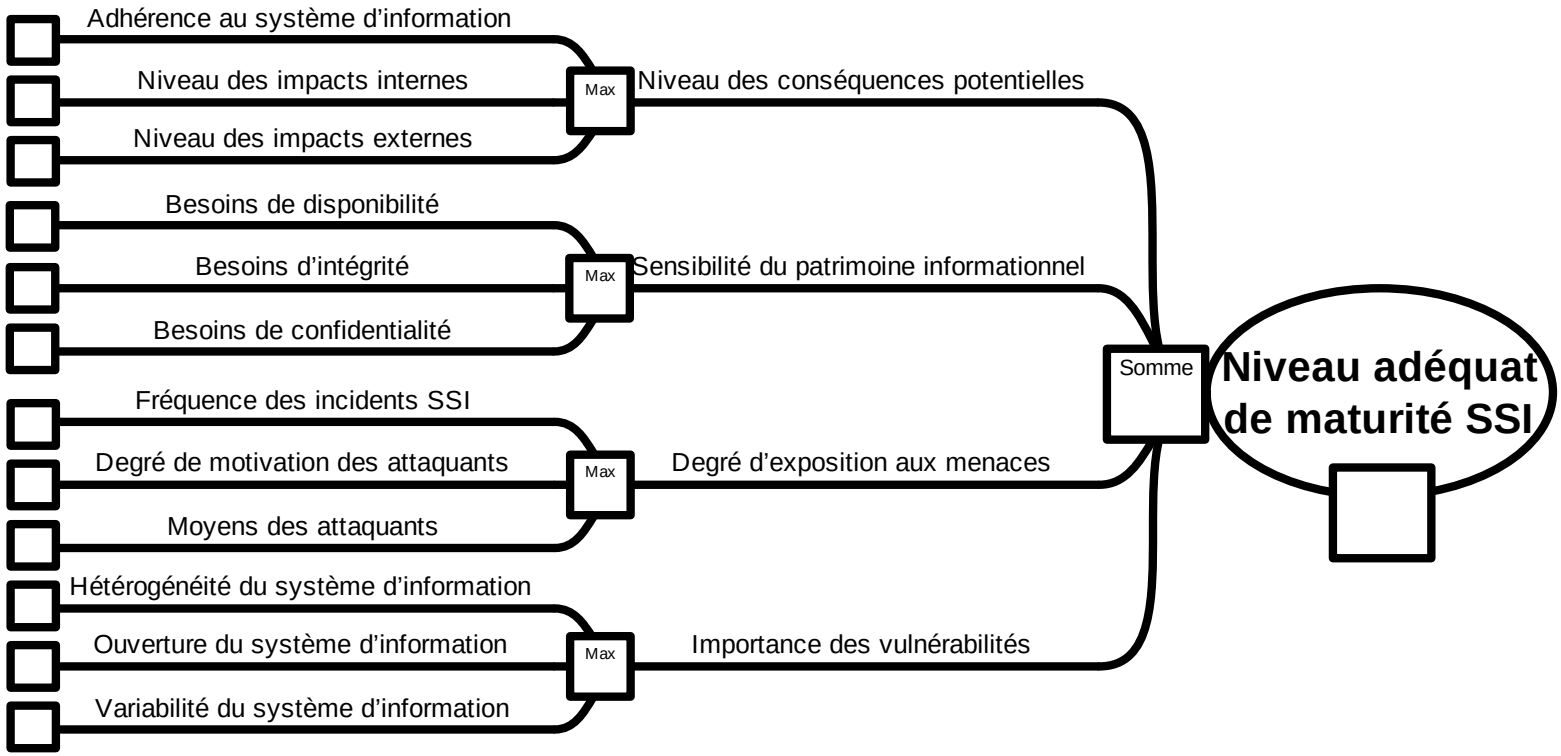
Acronymes

SSI	Sécurité des Systèmes d'Information
SI	Système d'Information

Références bibliographiques

[ISO 21827]	*Systems Security Engineering – Capability Maturity Model*, International Organization for Standardization (ISO), 2001.
[ISO 2382-1]	*Information Technology – Vocabulary – Fundamental vocabulary*, International Organization for Standardization (ISO), 1998.
[SEI 2006]	*Information Security as an Institutional Priority*, Carnegie Mellon University, Software Engineering Institute, 2006.

Outillage : arbre de détermination du niveau adéquat de maturité SSI



Outillage : tableau des niveaux effectifs de maturité SSI

Exigences d'atteinte du niveau de maturité SSI	Définir la stratégie SSI	Gérer les risques SSI	Gérer les règles SSI	Superviser la SSI	Concevoir les mesures SSI	Réaliser les mesures SSI	Exploiter les mesures SSI
Des actions sont réalisées en employant des pratiques de base							
Niveau 1							
Les actions sont planifiées							
Les acteurs sont compétents en SSI							
Certaines pratiques sont formalisées							
Des mesures qualitatives sont réalisées							
Les autorités compétentes sont informées des mesures effectuées							
Niveau 2							
Le processus est défini, standardisé et formalisé							
Les acteurs ont des compétences appropriées au processus							
L'organisme soutien le processus							
Niveau 3							
Le processus est coordonné dans tout le périmètre choisi							
Des mesures quantitatives sont régulièrement effectuées							
Les mesures effectuées sont analysées							
Le processus est amélioré en fonction des mesures effectuées							
Niveau 4							
Le processus est adapté de façon dynamique à la situation							
L'analyse des mesures est définie, standardisée et formalisée							
L'amélioration du processus est définie, standardisée et formalisée							
Les évolutions du processus sont journalisées							
Niveau 5							
Niveau effectif de maturité SSI des processus							

Formulaire de recueil de commentaires

Ce formulaire peut être envoyé à l'adresse suivante :

Secrétariat général de la défense nationale
Direction centrale de la sécurité des systèmes d'information
Sous-direction des opérations
Bureau conseil
51 boulevard de La Tour-Maubourg
75700 PARIS 07 SP
conseil.dcssi@sgdn.pm.gouv.fr

Identification de la contribution
Nom et organisme (facultatif) : .....
Adresse électronique : .....
Date : .....

Remarques générales sur le document
Le document répond-il à vos besoins ? Oui ☐ Non ☐

Si oui :

Pensez-vous qu'il puisse être amélioré dans son fond ? Oui ☐ Non ☐

Si oui :

Qu'auriez-vous souhaité y trouver d'autre ?
.....
.....

Quelles parties du document vous paraissent-elles inutiles ou mal adaptées ?
.....
.....

Pensez-vous qu'il puisse être amélioré dans sa forme ? Oui ☐ Non ☐

Si oui :

Dans quel domaine peut-on l'améliorer ?
- lisibilité, compréhension ☐
- présentation ☐
- autre ☐

Précisez vos souhaits quant à la forme :
.....
.....

Si non :

Précisez le domaine pour lequel il ne vous convient pas et définissez ce qui vous aurait convenu :
.....
.....

Quels autres sujets souhaiteriez-vous voir traiter ?
.....
.....

Remarques particulières sur le document

Des commentaires détaillés peuvent être formulés à l'aide du tableau suivant.

"N°" indique un numéro d'ordre.

"Type" est composé de deux lettres :

La première lettre précise la catégorie de remarque :

- O Faute d'orthographe ou de grammaire
- E Manque d'explications ou de clarification d'un point existant
- I Texte incomplet ou manquant
- R Erreur

La seconde lettre précise son caractère :

- m mineur
- M Majeur

"Référence" indique la localisation précise dans le texte (numéro de paragraphe, ligne…).

"Énoncé de la remarque" permet de formaliser le commentaire.

"Solution proposée" permet de soumettre le moyen de résoudre le problème énoncé.

N°	Type	Référence	Énoncé de la remarque	Solution proposée
1				
2				
3				
4				
5				

Merci de votre contribution