Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

PREMIER MINISTRE

Secrétariat général de la défense nationale

Direction centrale
de la sécurité des systèmes d'information

Maturité SSI

Positionner son organisme en 12 questions

5 niveaux de maturité

La norme ISO/IEC 21827 définit 5 niveaux de maturité SSI. Ils représentent la manière dont une organisation exécute, contrôle, maintient et assure un suivi d'un processus :

1. Pratique informelle : pratiques de base mises en œuvre de manière informelle et réactive sur l'initiative de ceux qui estiment en avoir besoin
2. Pratique répétable et suivie : pratiques de base mises en œuvre de façon planifiée et suivie, avec un support relatif de l'organisme
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
4. Processus contrôlé : le processus est coordonné et contrôlé à l'aide d'indicateurs permettant de corriger les défauts constatés
5. Processus continuellement optimisé : l'amélioration des processus est dynamique, institutionnalisée et tient compte de l'évolution du contexte

Pourquoi se situer ?

Maîtriser ses coûts SSI

Le niveau de maturité SSI fixe les actions et outils correspondant aux réels enjeux de sécurité. Les dépenses SSI induites correspondront ainsi aux mesures nécessaires et suffisantes.

Adapter ses actions SSI

L'analyse des enjeux de sécurité justifie le niveau des mesures et définit les orientations par domaine SSI. Elle contribue à l'élaboration du plan d'action pour atteindre le niveau adéquat.

Se comparer aux concurrents

Le positionnement d'un organisme en maturité SSI lui permet de se comparer aux organismes du même secteur. Le positionnement par direction, par système d'information ou par processus relativise les priorités en terme de SSI.

Autodiagnostic éclair

Afin de situer le niveau de maturité à atteindre, les mêmes questions peuvent être posées pour un organisme, un service, un système, un projet…

Les conséquences potentielles

Adhérence au système d'information (SI) : comment jugez-vous l'importance de votre SI dans l'accomplissement de vos missions ?

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

Niveau des impacts internes : quelles sont les conséquences internes (impacts financiers, juridiques, sur l'activité…) d'un sinistre SSI ?

0. Elles ne peuvent qu'être négligeables
1. Elles peuvent être significatives
2. Elles peuvent être graves
3. Elles peuvent être fatales

Niveau des impacts externes : quelles sont les conséquences externes (image, contrats, sécurité des personnes…) d'un sinistre SSI ?

0. Elles ne peuvent qu'être négligeables
1. Elles peuvent être significatives
2. Elles peuvent être graves
3. Elles peuvent être catastrophiques

Le niveau des conséquences potentielles est égal à la valeur maximale des trois réponses

La sensibilité du patrimoine

Besoins de disponibilité : quelle est l'importance de la disponibilité des SI ?

0. L'inaccessibilité des SI ne gêne pas l'activité
1. Elle perturbe l'activité de manière significative
2. Elle est jugée comme grave pour l'activité
3. Elle peut être fatale pour l'activité

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

Besoins d'intégrité : quelle est l'importance de l'intégrité des données dans le cadre de l'activité ?

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

Besoins de confidentialité : quelle est l'importance de la confidentialité dans le cadre de l'activité ?

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

La sensibilité du patrimoine informationnel est égale à la valeur maximale des trois réponses

Le degré d'exposition aux menaces

Fréquence des sinistres SSI : quelle est la fréquence estimée des sinistres SSI ?

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

Degré de motivation des attaquants : quel est le degré de motivation des attaquants potentiels ?

0. Une attaque SSI ciblée sur le périmètre est relativement inimaginable
1. Elle est jugée faible
2. Elle peut être forte
3. Elle peut être très importante

Moyens des attaquants : quels sont les moyens des attaquants potentiels ?

0. Les attaquants potentiels ne disposent que de faibles moyens
1. Ils peuvent disposer de moyens significatifs
2. Ils peuvent disposer de moyens importants
3. Leurs moyens sont potentiellement illimités

Le degré d'exposition aux menaces est égal à la valeur maximale des trois réponses

L'importance des vulnérabilités

Hétérogénéité du SI : quel est le niveau de variété du SI ?

0. Le SI est jugé comme homogène
1. Il est jugé comme faiblement hétérogène
2. Il est jugé comme fortement hétérogène
3. Il est jugé comme extrêmement hétérogène

Ouverture du SI : Quel est le degré d'ouverture du système d'information ?

0. Le SI n'est pas ouvert
1. Il n'est ouvert qu'à des systèmes internes
2. Il est ouvert à des systèmes externes mais sous contrôle
3. Il est ouvert à des systèmes externes hors de contrôle

Variabilité du SI : 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…) ?

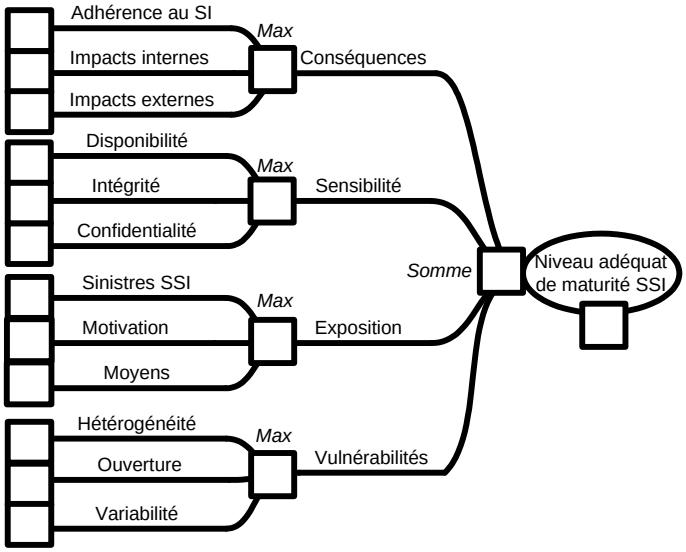
0. Le SI et son contexte sont jugés stables
1. Ils changent peu
2. Ils changent relativement souvent
3. Ils changent très souvent

L'importance des vulnérabilités est égale à la valeur maximale des trois réponses

Détermination du niveau adéquat

Le niveau adéquat de maturité SSI du périmètre choisi dépend de la somme des quatre valeurs que vous venez de calculer :

Somme	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 optimisé



Informations et contacts

conseil.dcssi@sgdn.pm.gouv.fr
http://www.ssi.gouv.fr/fr/confiance/methodes