Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

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

Guide d'intégration de la sécurité des systèmes d'information dans les projets

GISSIP

Version du 11 décembre 2006

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)

Les commentaires et suggestions sont encouragés et peuvent être adressés à l'adresse suivante
(voir formulaire de recueil de commentaires en fin de guide) :

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
27/09/2005	Création du document	SGDN	Version de travail
31/10/2005	Finalisation du document pour présentation en Commission interministérielle SSI du 10 novembre 2005	SGDN	Version de travail
11/12/2006	Corrections mineures Vérification de la compatibilité avec la réglementation relative à l'homologation en France et à l'OTAN et ajout d'une annexe présentant les analogies	SGDN	Validé

Table des matières

Avant-propos

Note : les références [entre crochets] sont présentées dans la bibliographie en annexe du document. On trouvera également un glossaire des termes et acronymes utilisés.

Un référentiel d'outils méthodologiques développés par la DCSSI

Ce document fait partie d'une série de guides méthodologiques publiés par la DCSSI. Ces guides sont destinés à contribuer à l'amélioration de la sécurisation des systèmes d'information des organismes publics ou privés. Ils peuvent être obtenus par simple demande à la DCSSI.

Vers une administration électronique sécurisée

Le recours très large aux technologies de télécommunication, de réseaux, informatiques et applicatives rend les organismes dépendants de leurs systèmes d'information et donc vulnérables aux multiples menaces qui pèsent sur eux. Cet état de choses contribue considérablement à augmenter les risques qui résultent du traitement, du stockage et du transport des informations, au cœur de tout organisme.

Les nouvelles lignes directrices de l'Organisation de Coopération et de Développement Économiques [OCDE] font l'objet d'une recommandation de portée internationale. Elles ont pour objectif principal de promouvoir une "culture de la sécurité" en tant que moyen de protection des systèmes et réseaux d'information. Cela signifie qu'il est nécessaire de porter une très grande attention à la sécurité et d'adopter de nouveaux modes de pensée et de comportement lors du développement et de l'utilisation des systèmes d'information et des réseaux. Elles se présentent sous la forme de neuf principes qui se complètent et doivent être considérés comme un tout.

Le gouvernement français s'est engagé dans le domaine de l'administration électronique. Il s'agit de mettre les technologies de l'information au service de la modernisation des services publics, d'améliorer l'efficacité de l'action des administrations de l'État comme des collectivités locales et la qualité des relations entre celles-ci et leurs usagers. Cette dématérialisation "des services publics" ne peut s'effectuer sans une attention minimum portée sur la sécurité. C'est le rôle de la Direction centrale de la sécurité des systèmes d'information (DCSSI) du Secrétariat général de la défense nationale (SGDN) que de contribuer à la définition interministérielle et à l'expression de la politique gouvernementale en matière de sécurité des systèmes d'information.

L'action de l'État peut être mise en cause par les risques issus de l'utilisation des systèmes d'information. C'est pourquoi la protection de l'information et la sécurisation des systèmes d'information de l'État est un devoir national.

Les systèmes d'information doivent être sécurisés conformément à une politique de sécurité définie en fonction du niveau de protection requis, en particulier du niveau de sensibilité, voire de classification, des informations traitées et sur la base d'une analyse des risques. Ils doivent être mis en œuvre au moyen d'une gestion globale de la sécurité.

1 Introduction

À l'heure actuelle, les systèmes d'information (SI), ensembles d'entités organisés pour accomplir des fonctions de traitement d'information, prennent bel et bien en compte non seulement les matériels, logiciels et réseaux, mais aussi les organisations, les locaux et les personnels.

Étant donnée leur nature complexe, changeante, fortement interconnectée et exposée à une menace qui revêt des formes multiples et variables dans le temps, il est aujourd'hui indéniable que la sécurité des systèmes d'information (SSI) doit être intégrée tout au long de leur cycle de vie.

Il apparaît en outre un important besoin de pouvoir moduler les actions SSI selon les enjeux réels du SI vis-à-vis de l'organisme. En effet, une trop faible prise en compte des aspects SSI implique généralement des risques résiduels qui peuvent s'avérer inacceptables pour l'organisme ; inversement, une trop forte prise en compte de la SSI peut rapidement générer des coûts injustifiés ou provoquer un refus de la part des utilisateurs.

Ce document, le guide d'intégration de la SSI dans les projets (GISSIP), présente une méthode modulaire qui décrit l'ensemble des actions SSI à mener depuis l'étude d'opportunité d'un projet[1] jusqu'à la fin de vie des SI. L'approche se décline différemment en termes d'actions SSI selon les enjeux de sécurité qui auront été identifiés au tout début du projet.

La réflexion repose sur la **proposition d'un cycle de vie et de rôles et responsabilités génériques** (chapitre 2) qu'il convient de transposer à son propre contexte.

Elle repose également sur des **grands principes fondateurs de la démarche** (chapitre 3) qui mettent en évidence le rapprochement avec la gestion des risques SSI, la validation des enjeux de sécurité en début de projet, les différents niveaux de maturité SSI possibles selon ces enjeux, la notion d'homologation de sécurité des SI et la description du dossier de sécurité qui sert de base à l'homologation.

L'**approche méthodologique** (chapitre 4) résultant de cette réflexion décrit les actions SSI à mener selon chaque étape du cycle de vie des SI et selon leur niveau de maturité SSI adéquat.

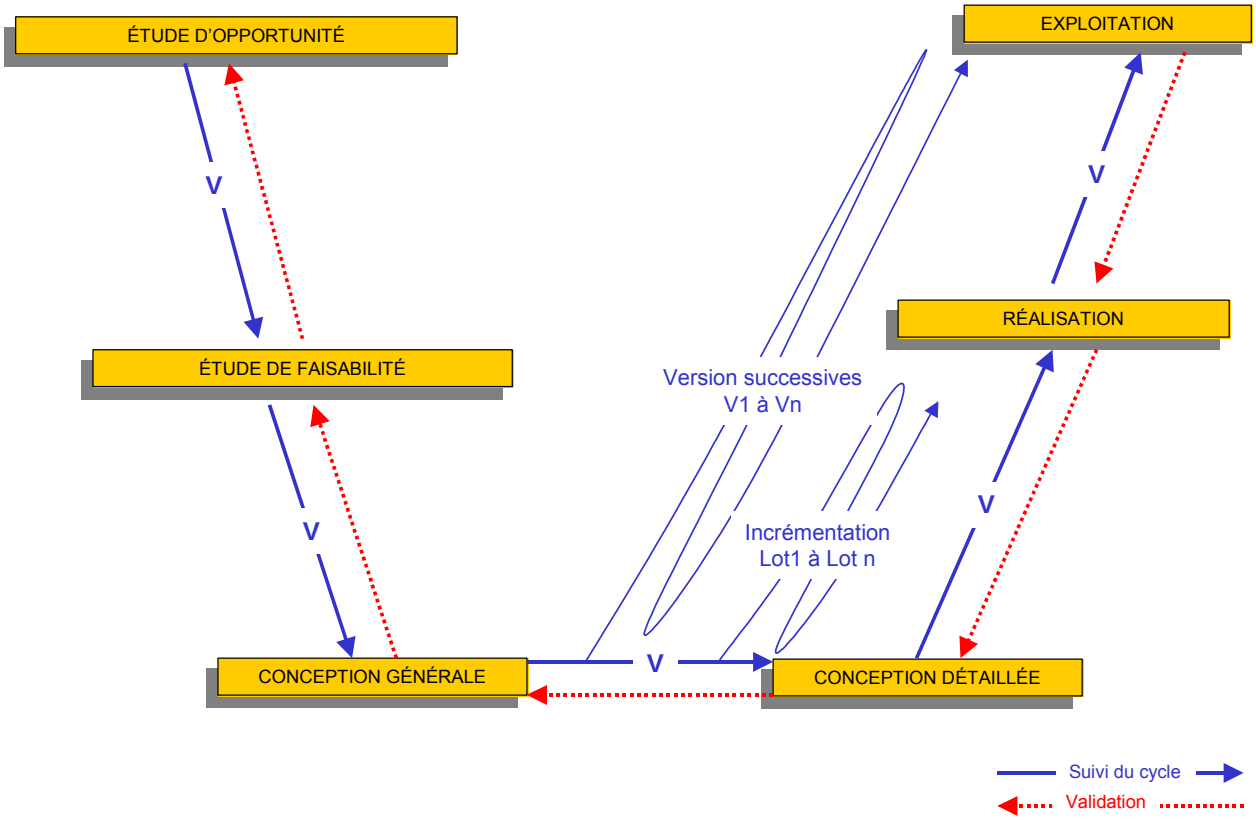
Des exemples de **plans des livrables** issus de la démarche, les **références bibliographiques** utiles, le **glossaire** et les **acronymes** figurent en annexes du document.

[1] Le terme "projet" désigne ici tout type de projet, qu'il soit relatif à un SI ou même spécifique à la SSI.

2 Présentation du cycle de vie et des acteurs

2.1 Un cycle de vie générique transposable à tous les projets

Afin de pouvoir transposer la réflexion de l'intégration de la sécurité dans le cycle de vie des SI à tous les modèles courants (en cascade, en cascade avec retour, en V, incrémental, par versions successives, etc., qui sont présentés en annexe du document), un cycle de vie générique a été défini :



La plupart des organismes peuvent, moyennant une interprétation qui leur est propre, se positionner par rapport à ce modèle générique et le traduire dans leur propre structure.

2.1.1 Étape 1 – Étude d'opportunité

L'étude d'opportunité vise à définir le cadre potentiel du projet, son intérêt pour l'organisme :

- analyse et hiérarchisation des enjeux,
- analyse des freins et des leviers (organisation, technologie, culture et motivation),
- identification et évaluation des ressources internes et externes à mettre en œuvre,
- estimation du retour sur investissement.

Dans le domaine de la SSI, cette étape est fondamentale, elle conditionne toute la suite du projet car c'est à ce moment que sont évalués les grands enjeux SSI du projet et donc l'investissement consenti pour gérer les risques.

2.1.2 Étape 2 – Étude de faisabilité

L'étude de faisabilité vise à analyser la faisabilité économique, organisationnelle et technique de projet.
On s'interrogera notamment sur la faisabilité du projet en termes de produits éprouvés, rendement, ressources, compétences, capacité, financement et risques induits.

D'un point de vue SSI, il peut avoir été conclu lors de la phase précédente que cette phase ne devra pas comporter d'action SSI ; dans les autres cas, on affinera les éléments stratégiques, les contraintes juridiques, calendaires, financières.

2.1.3 Étape 3 – Conception générale

Lors de la conception générale, on s'attachera à affiner l'expression de besoins fonctionnels sans rechercher les solutions techniques. On précisera également l'ensemble des contraintes et les différentes phase du projet.

Soit on s'attache à rechercher les meilleurs pratiques SSI que devra mettre en œuvre le SI considéré, soit on formalise le premier cahier des charges de sécurité sous la forme d'une fiche d'expression rationnelle des objectifs de sécurité (FEROS). Les objectifs de sécurité sont alors ajoutés au cahier des charges global du projet.

2.1.4 Étape 4 – Conception détaillée

À cette étape, la maîtrise d'œuvre est choisie, le travail est donc réalisé conjointement maîtrise d'ouvrage et maîtrise d'œuvre dans l'objectif de décrire finement l'engagement des deux parties en terme de réalisation. Cette étape permet d'aboutir au livrable appelé cahier des clauses techniques particulières (CCTP).

Dans le domaine de la SSI, seuls sont concernés les projets dont la prise en compte de la sécurité s'appuie sur une approche méthodologique. Pour ces projets, il s'agira de décrire des solutions techniques et organisationnelles qui sont retenues pour satisfaire les objectifs de sécurité formulés au sein du cahier des charges. Un tableau de bord SSI élaboré à partir des objectifs de sécurité pourra également être constitué.

2.1.5 Étape 5 – Réalisation

La phase de réalisation comprend la réalisation des composantes du système d'information, c'est à dire le développement, l'intégration, la qualification et la recette.
Les phases de développement, intégration et qualification sont de la responsabilité du maître d'œuvre, sous contrôle du maître d'ouvrage. En revanche, la recette qui est la vérification de la conformité du projet par rapport à la demande formulée dans le dossier validé de conception générale, est du ressort de la maîtrise d'ouvrage.

Pour la SSI, dans les projets qui le requièrent, cette étape permet au maître d'œuvre de constituer la cible de sécurité, c'est à dire d'affiner les exigences de sécurité et d'expliciter la façon dont ces exigences doivent être mises en œuvre.

2.1.6 Étape 6 – Exploitation

Cette étape comprend l'homologation du système d'information, son déploiement, sa mise en œuvre en situation opérationnelle, sa maintenance jusqu'à sa fin de vie.

Dans le domaine de la SSI, cette étape permet d'homologuer le système suite à un audit de sécurité vérifiant le niveau de risque résiduel et à la vue du dossier de sécurité du système. Ce dossier sera constitué de plus ou moins d'éléments en fonction des enjeux de sécurité.
Par ailleurs, durant la phase d'exploitation, pour des systèmes requérant un haut niveau de maturité SSI, les différents intervenants alimenteront des tableaux de bord SSI dont les indicateurs sont issus des objectifs de sécurité du système.

2.2 Des rôles et responsabilités génériques

Bien que chaque structure soit spécifique, il est possible de proposer un ensemble de rôles et responsabilités que l'on retrouve généralement dans le cadre des projets et de la vie des SI.

2.2.1 Utilisateurs

Les utilisateurs sont généralement à l'origine du besoin d'un système d'information (SI). Ils définissent le calendrier de mise en œuvre du SI et sont responsables de la mise en œuvre du SI.

2.2.2 Maîtrise d'ouvrage

La maîtrise d'ouvrage est responsable de la définition des besoins. Elle fixe l'organisation du projet, ses objectifs, ses enjeux et ses contraintes. D'une manière générale, elle est responsable de l'identification des objectifs de sécurité et du pilotage du projet. Dans la conduite du projet, la maîtrise d'ouvrage assure le choix du maître d'œuvre, le suivi des différentes phases du projet, sa validation et sa réception définitive. Elle est responsable de la maîtrise du budget, du calendrier et des performances, y compris des performances en matière de SSI. La maîtrise d'ouvrage est représentée par un directeur de projet. Par ailleurs, la maîtrise d'ouvrage peut être déléguée.

2.2.3 Maîtrise d'œuvre

La maîtrise d'œuvre est responsable des propositions techniques et de l'évaluation des charges de réalisation. D'une manière générale, elle est responsable de la détermination des exigences de sécurité devant satisfaire les objectifs de sécurité et de leur mise en œuvre. Lorsque des sous-traitants sont appelés à intervenir sur le projet, la maîtrise d'œuvre assure la préparation des appels d'offre, le traitement et le choix des sous-traitants, le suivi technique et administratif de leur intervention, ainsi que la recette. La maîtrise d'œuvre se doit de faire l'analyse des risques techniques du projet et d'y apporter les mesures appropriées.

2.2.4 Autorité d'homologation

L'autorité d'homologation est l'autorité qui doit valider le compromis entre la sécurité et les contraintes opérationnelles, financières, humaines du projet. Cette autorité doit donc s'appuyer sur une commission d'homologation qui lui fournira les éléments d'informations nécessaires à sa décision. Si l'autorité sur le système d'information n'est pas incarnée par une seule entité, l'autorité d'homologation peut être collégiale.

2.2.5 Responsable de la sécurité des systèmes d'information (RSSI)

En fonction des organismes, le RSSI peut avoir différents rattachements. Rattaché à la direction générale, il est chargé de la définition et de l'application de la PSSI. Dans le cadre d'un projet, il conseille l'autorité d'homologation. Rattaché à la direction informatique, il intervient en tant qu'expert auprès de la direction de projet et valide les livrables SSI au regard de la PSSI. Dans le cadre de la commission d'homologation, il a la charge de présenter l'analyse de risques.

2.2.6 Experts techniques

Les experts techniques apportent le soutien technique requis dans toutes les phases du projet : conseil, conception, évaluation, validation… en fonction de la phase du cycle de vie du SI, au profit des différents acteurs. Leurs rapports sont souvent utilisés par le comité de pilotage ou la commission d'homologation afin de faciliter les arbitrages. Ce rôle est habituellement rempli par plusieurs acteurs, consultants internes et/ou externes.

2.2.7 Comité de pilotage

Le comité de pilotage prend les décisions stratégiques sur le projet. Il est présidé par l'autorité d'emploi. Cette structure est à même de rendre les arbitrages budgétaires, techniques et fonctionnels tout au long du projet. Elle est garante de l'atteinte des objectifs.

2.2.8 Commission d'homologation

En matière de SSI, la commission d'homologation est le pendant du comité de pilotage. Elle est placée sous la présidence de l'autorité d'homologation, assiste cette dernière afin de lui fournir les éléments d'informations nécessaires à sa décision.

3 Fondements de l'intégration de la sécurité dans le cycle de vie des SI

3.1 Une réflexion au cœur du processus continu de la gestion des risques SSI

L'intégration de la SSI dans le cycle de vie des SI s'appuie sur la gestion des risques SSI.

C'est en effet le niveau de risque SSI qui permettra de faire émerger les enjeux en matière de sécurité et de définir la rigueur adéquate des actions à entreprendre afin de se prémunir des risques. Par ailleurs, chaque projet et SI mis en œuvre contribue à la continuité de la gestion des risques SSI en alimentant les réflexions sur le sujet.

Le **risque SSI** est une combinaison d'une menace et des pertes qu'elle peut engendrer. La menace SSI est définie à partir d'un élément menaçant, exploitant une méthode d'attaque afin d'atteindre un bien.

La **gestion des risques SSI** consiste à coordonner, de manière continue, les activités visant à diriger et piloter un organisme vis-à-vis des risques. Elle inclut l'appréciation, le traitement, l'acceptation et la communication relative aux risques SSI :

1. L'**appréciation des risques SSI** représente l'ensemble du processus d'analyse des risques (mise en évidence des composantes des risques) et d'évaluation des risques (estimation de leur importance).

   Elle consiste tout d'abord à décrire au minimum l'organisme, le système d'information (SI), les biens à protéger, les enjeux liés au SI et les contraintes à prendre en compte.
   Les besoins de sécurité des informations et fonctions doivent ensuite être exprimés au moins en termes de disponibilité, d'intégrité et de confidentialité. Cette expression des besoins doit être faite indépendamment des menaces.
   Les menaces pesant sur le SI doivent être identifiées et évaluées en terme d'opportunité (représentant l'incertitude de ces menaces).
   Les risques doivent enfin être déterminés en confrontant les menaces aux besoins de sécurité.

2. Le **traitement des risques SSI** représente le processus de sélection et de mise en œuvre des mesures visant une réduction des risques, un transfert des risques ou une prise de risque.

   Il consiste tout d'abord à identifier les objectifs de sécurité permettant de couvrir le risques tout en prenant en compte les éléments du contexte. Ces objectifs représentent un cahier des charges ne préjugeant pas des solutions à mettre en œuvre, mais exprimant la volonté et la manière de traiter les risques.
   Le traitement des risques se poursuit par la détermination d'exigences de sécurité, techniques ou non, satisfaisant les objectifs de sécurité identifiés.
   Des mesures techniques ou non techniques répondant aux exigences de sécurité déterminées peuvent enfin être mises en œuvre.
   À l'issue, les risques ont été soit réduits, soit transférés (vers des tiers) et un ensemble de risques résiduels peut subsister.

3. L'**acceptation des risques SSI** représente la décision d'accepter les risques traités.

   Cette activité consiste en une **homologation de sécurité**.

4. La **communication relative aux risques SSI** représente l'échange ou le partage d'informations concernant les risques.

La gestion des risques SSI doit être considérée comme un processus continu et itératif.

3.2 La validation des enjeux de sécurité constitue le point de départ de la réflexion

L'intégration de la sécurité dans le cycle de vie des SI doit être mesurée et être en adéquation avec les enjeux de sécurité du système.

Dans ce contexte, une **note d'orientations SSI** permet de définir la stratégie de sécurité à adopter en précisant les enjeux du projet. Elle doit être validée par l'**autorité d'homologation** pour tout système d'information, et ce, dès l'étude d'opportunité.

En fonction de l'importance des enjeux de sécurité retenus, les actions SSI à mener et le contenu du **dossier de sécurité** seront adaptés.

3.3 Le niveau d'intégration de la SSI varie selon les enjeux de sécurité

Différents niveaux de maturité SSI (issus de l'[ISO 21827]) synthétisent la manière dont une organisation exécute, contrôle, maintient et assure le suivi des processus relatifs à la SSI :

0. il n'y a pas de mise en œuvre,
1. la mise en œuvre est informelle (mise en œuvre de pratiques de base),
2. elle est planifiée et suivie (planification de la performance, performance disciplinée, vérification de la performance, suivi de la performance),
3. elle est définie (formalisée et d'application généralisée, utilisation d'un processus défini, mise en œuvre du processus défini, coordination des pratiques),
4. elle est contrôlée qualitativement (établissement de buts mesurables, gestion objective de la performance),
5. elle permet une amélioration continue (amélioration de la capacité organisationnelle, amélioration de l'efficacité du processus).

Chaque organisme peut déterminer son niveau de maturité SSI adéquat selon l'adhérence au système d'information et le niveau de menace pesant sur celui-ci.

Les actions relevant de la SSI, qui devront être réalisées tout au long du cycle de vie d'un SI, ne sont pas nécessairement identiques selon le niveau de maturité SSI adéquat.

En effet, il n'est pas nécessaire d'investir dans une étude très détaillée de la SSI ni d'élaborer un dossier de sécurité très complet si l'on constate rapidement que les enjeux et les risques pesant sur le système d'information sont très faibles, voire négligeables.

3.4 L'homologation de sécurité comme condition nécessaire à la mise en œuvre des SI

D'une manière générale, il convient d'apprécier si un SI donné est bien apte à protéger les informations qu'il doit traiter conformément aux besoins de sécurité exprimés.

L'homologation de sécurité d'un SI est la déclaration par l'**autorité d'homologation**, conformément à une **note d'orientations SSI** et au vu du **dossier de sécurité**, que le SI considéré est apte à traiter des informations au niveau de besoins de sécurité exprimé conformément aux objectifs de sécurité, et que les risques de sécurité résiduels sont acceptés et maîtrisés.

Cette décision se fait dans le cadre de la commission d'homologation et peut être :

- une homologation provisoire, qui peut devenir définitive après avoir appliqué le plan d'action déterminé lors d'un audit,
- un refus d'homologation au vu des résultats d'audit et des risques résiduels encourus,
- une homologation "définitive", pour une durée maximale (fréquemment entre 3 et 5 ans).

L'homologation de sécurité reste valide tant que le SI opère dans les conditions approuvées par l'autorité d'homologation. Elle traduit donc l'acceptation d'un niveau de risque résiduel qualifié et quantifié en termes de confidentialité, d'intégrité, de disponibilité…

3.5 Un dossier de sécurité selon le niveau de maturité SSI

L'autorité d'homologation s'appuie sur un dossier de sécurité dont le contenu sera fonction des enjeux de sécurité. Selon le niveau de maturité SSI adéquat, ce dossier de sécurité peut comporter les documents suivants :

1. Une **fiche d'expression rationnelle des objectifs de sécurité (FEROS)**

   La FEROS constitue le cahier des charges SSI de la maîtrise d'ouvrage. Elle doit être rédigée à l'aide des données de la gestion des risques SSI.

   Elle doit inclure au minimum la définition des responsabilités, la description du SI, les objectifs de sécurité et les risques résiduels.

2. Une **cible de sécurité** du système d'information

   La cible de sécurité identifie sans ambiguïté le périmètre sur lequel porte l'homologation. La cible de sécurité est la réponse aux objectifs de sécurité identifiés dans la FEROS. Elle doit inclure au minimum la liste des exigences de sécurité et une démonstration de la couverture des objectifs de sécurité par les exigences de sécurité. Elle constitue le lien entre les objectifs de sécurité de la maîtrise d'ouvrage et les exigences de sécurité de la maîtrise d'œuvre. Elle constitue donc un moyen de traçabilité.

3. Une **politique de sécurité du système d'information (PSSI)**

   La PSSI constitue le document de référence en matière de SSI pour l'ensemble des acteurs du SI. Elle doit être conforme à la PSSI de l'organisme et peut ne présenter que les spécificités par rapport à cette dernière.
   Elle doit inclure des éléments stratégiques (le périmètre du SI, les enjeux liés et orientations stratégiques, les aspects légaux et réglementaires, une échelle de besoins, les principaux besoins de sécurité et l'origine des menaces), ainsi que les règles de sécurité présentées par domaine (par exemple organisationnel, mise en œuvre, technique…).

4. Les **documents d'application de la PSSI**

   Les documents d'application comprennent notamment les procédures d'exploitation de sécurité (PES) du système d'information, mais aussi les documents de communication, les procédures de sécurité, les notes d'organisation, la charte des utilisateurs…

5. La **documentation relative aux tests**

   Les documents de tests comprennent notamment les résultats d'audit, mais aussi le cahier de recette, les comptes-rendus de qualification et de recette, la documentation des tests unitaires, les rapports de vérification de conformité…

6. La **documentation relative aux évaluations de sécurité**

   L'ensemble des documents relatifs aux évaluations comprend notamment la documentation nécessaire à l'évaluation et les rapports d'évaluation.

7. Les **tableaux de bord SSI (TDBSSI)**

   Les TDBSSI sont constitués des documents de conception tels que des fiches descriptives et procédures d'alimentation des indicateurs et des TDBSSI, ainsi que des TDBSSI résultant de leur utilisation.

Ces documents font généralement l'objet de synthèses et de validations successives. Une fois le SI homologué, le dossier de sécurité doit rester conforme et cohérent au cycle de vie du SI. Il devra être régulièrement mis à jour, pour refléter les évolutions du contexte du SI.

4 Actions SSI à mener par étape du cycle de vie des SI

La démarche proposée vise à satisfaire les contraintes financières, calendaires et fonctionnelles des projets sans pour autant occulter la SSI.

Ainsi, une première appréciation du niveau de risque SSI auquel est exposé le projet lors de sa phase d'étude d'opportunité permet de définir la démarche d'intégration la plus appropriée aux enjeux de sécurité du SI.

Les éléments d'une réponse adaptée consistent alors à choisir la bonne démarche d'intégration de la sécurité. Plusieurs démarches coexistent et se complètent. D'une manière générale, on peut rencontrer les situations suivantes :

- une approche basée sur **l'utilisation de meilleures pratiques** seules, généralement sous la forme de guides de configuration, de check-lists…
- une approche basée sur **l'analyse des risques SSI, sans méthode** mais résultant du retour d'expérience des acteurs
- une approche basée sur **la gestion structurée des risques SSI**, reposant sur l'emploi d'une démarche méthodologique de gestion des risques.

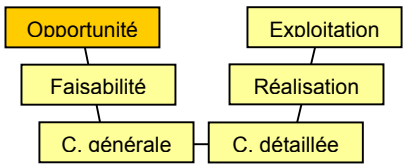
La démarche proposée ici s'appuie sur les caractéristiques des niveaux de maturité SSI :

0. La SSI n'est pas prise en compte dans le cycle de vie des systèmes.
1. Des meilleures pratiques SSI sont occasionnellement et informellement utilisées dans le cycle de vie des systèmes ; la mise en œuvre ne correspond pas forcément à ce qui a été planifié.
2. Les meilleures pratiques SSI sont intégrées dans le cycle de vie des systèmes (planification, vérification, actions correctives), de manière peu régulière, mais homogène ; les actions correspondent à ce qui a été planifié.
3. Le processus d'intégration de la SSI dans le cycle de vie des systèmes est formalisé, éventuellement sur la base d'une démarche méthodologique, depuis les phases amont d'un projet jusqu'à sa fin de vie ; il est régulièrement utilisé ; les systèmes font l'objet d'une homologation de sécurité formelle sur la base d'un dossier de sécurité défini.
4. Des objectifs mesurables d'intégration de la SSI dans les projets sont définis et suivis (ex : tableaux de bord projets intégrant la SSI, audits…) ; le processus est devenu standard et davantage automatisé.
5. Le processus d'intégration de la SSI dans le cycle de vie des systèmes est généralisé, bien automatisé, utilisé par tous les autres processus SSI, intégré aux processus métiers, bien accepté et s'améliore continuellement.

La démarche fournit pour chaque étape un ensemble d'action SSI à mener et de livrables à produire, chaque étape étant décrite sous la forme de fiches contenant les informations suivantes :

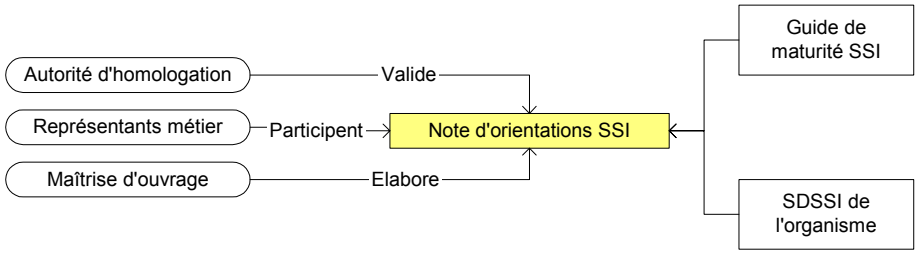
Étape	*Étape du cycle de vie générique des SI et niveau de maturité SSI visé*
Objectif	*Objectif général de l'étape en terme de SSI*
Préalables	*Actions ou documents nécessaires en entrée de l'étape*
Description	*Description des actions SSI à mener lors de l'étape*
Livrables	*Documents livrables en sortie de l'étape*
Outils	*Outils (méthodes, catalogues…) pouvant aider à la réalisation de l'étape*
Synthèse	*Schéma présentant les principaux acteurs, outils et livrables (composant le dossier de sécurité)* 

4.1 Étape 1 – Étude d'opportunité

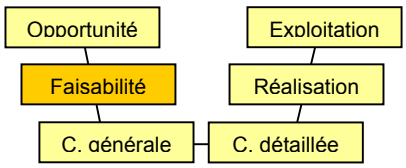


La genèse du projet est constituée par le lancement d'une étude d'opportunité fonctionnelle.

Au cours de cette étape, il convient de déterminer le niveau de maturité SSI adéquat pour l'ensemble du cycle de vie du système. Cette étape constitue une analyse de risques macroscopique du projet. Elle doit être réalisée pour tous les projets.

Étape 1	Étude d'opportunité (tous les niveaux)
Objectif	L'objectif de cette étape est de déterminer le niveau de maturité SSI adéquat pour le système à concevoir. De ce niveau de maturité SSI adéquat dépend le processus d'intégration de la SSI dans la conduite du projet.
Préalables	❑ Identification du directeur de projet ❑ Identification de l'autorité d'homologation
Description	❑ Une analyse des enjeux de sécurité doit être réalisée. Elle est menée à l'aide d'un entretien avec, si possible, le directeur de l'organisme, le directeur informatique, le directeur financier et le directeur des ressources humaines. Cette analyse consiste à apprécier rapidement les risques SSI en fonction des enjeux stratégiques que présente le projet vis-à vis de l'organisme. Il convient de commencer à dresser une liste de contraintes générales pesant sur l'organisme et de références réglementaires applicables à l'organisme.
Livrables	❑ Une note d'orientations SSI doit être rédigée. Elle doit synthétiser l'analyse des enjeux de sécurité, proposer un niveau de maturité SSI adéquat et présenter la manière dont sera intégrée la SSI dans le cycle de vie du système en fonction de ce niveau. Il est judicieux de mettre en évidence l'adéquation au schéma directeur SSI de l'organisme.
Outils	❑ Guide de maturité SSI ❑ Schéma directeur SSI (SDSSI) de l'organisme
Synthèse	

4.2 Étape 2 – Étude de faisabilité

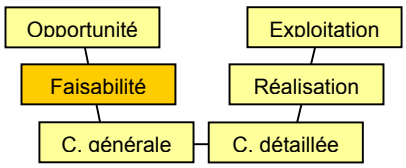


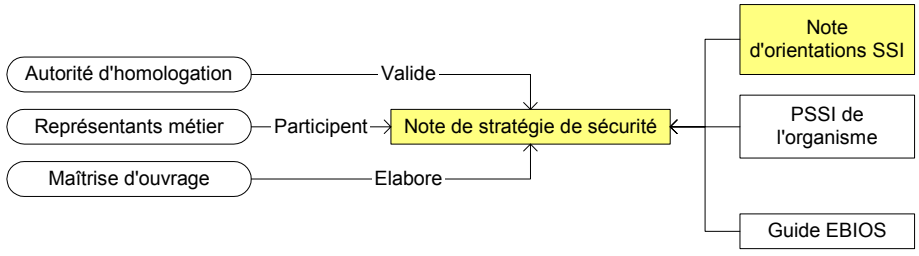
L'étude de faisabilité vise à analyser la faisabilité économique, organisationnelle et technique d'un projet. On s'interrogera notamment sur la faisabilité du projet en termes de produits, de rendement, de ressources, de compétences, de capacité, de financement et de risques induits.

4.2.1 Niveaux 1 à 2

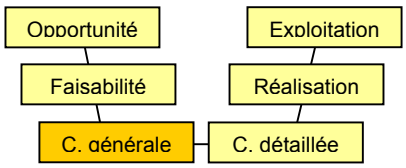
Dans le cas où la note d'orientations SSI statue sur le fait que le projet devrait être mené avec un faible niveau de maturité SSI adéquat (type 1 ou 2), aucune action SSI n'est requise lors de cette étape.

4.2.2 Niveaux 3 à 5



Étape 2	Étude de faisabilité (niveaux 3 à 5)
Objectif	L'objectif de cette étape est d'enrichir l'analyse des enjeux de sécurité de manière à formaliser les éléments de stratégie de sécurité. À l'issue, le contexte du projet est parfaitement connu, ainsi que les éléments nécessaires à l'expression des besoins de sécurité et à l'étude des menaces.
Préalables	❑ Note d'orientations SSI
Description	❑ L'étude du contexte doit être affinée. Elle doit formaliser des informations sur l'organisme (description, orientations stratégiques, contraintes et références réglementaires…) et sur le système à concevoir (description, enjeux, hypothèses, contraintes et références réglementaires, règles de sécurité, éléments essentiels…) pour délimiter le périmètre d'étude et mettre en évidence les enjeux SSI concernant le projet. ❑ Les éléments nécessaires à l'expression des besoins de sécurité doivent être formalisés. Il convient notamment de déterminer les impacts redoutés par l'organisme et une échelle de besoins (en termes de disponibilité, d'intégrité, de confidentialité…). ❑ Les éléments nécessaires à l'étude des menaces doivent être formalisés. Il convient notamment de mener une réflexion sur les méthodes d'attaque et sur les éléments menaçants susceptibles de les employer.
Livrables	❑ Une note de stratégie de sécurité doit être réalisée. Cette note doit présenter tous les éléments décrivant l'organisme et le système à concevoir, les éléments nécessaires à l'expression des besoins de sécurité et les éléments nécessaires à l'étude des menaces. Elle doit être conforme à la PSSI de l'organisme. Elle doit être validée par l'autorité d'homologation.
Outils	❑ PSSI de l'organisme ❑ Méthode de gestion des risques SSI (par exemple [EBIOS])
Synthèse	

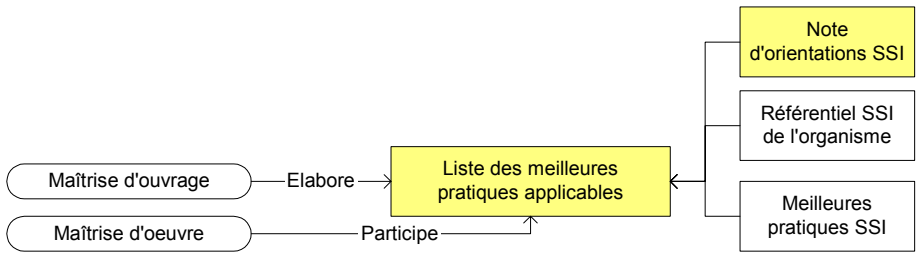
4.3 Étape 3 – Conception générale



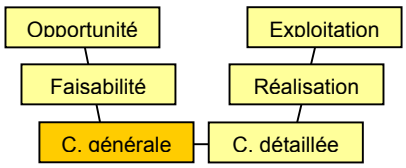
4.3.1 Niveau 1

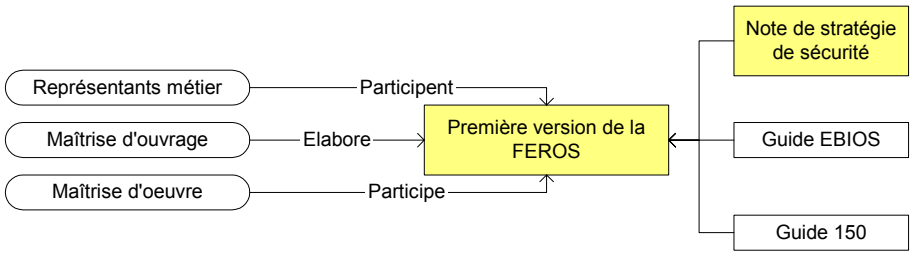
Dans le cas où la note de stratégie de sécurité statue sur le fait que le projet devrait être mené avec un très faible niveau de maturité SSI (type 1), aucune action SSI n'est à mener lors de cette étape.

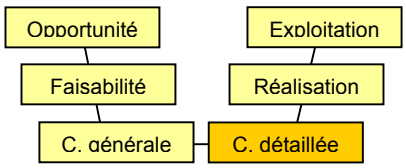
4.3.2 Niveau 2

Étape 3	Conception générale (niveau 2)
Objectif	La conception générale doit permettre de construire un cahier des charges. Il convient de choisir les meilleures pratiques SSI qui devront être appliquées et celles que le système cible devra mettre en œuvre.
Préalables	❑ Note d'orientations SSI
Description	❑ Un inventaire des meilleures pratiques SSI applicables doit être réalisé. Il convient de mener cette opération en fonction du contexte de l'organisme, des fonctionnalités du système et des entités qui le composeront (logiciels, matériels, réseaux, organisations, personnels et locaux). Pour cela, les référentiels exploitables sont en premier lieu ceux de l'organisme (notamment sa politique de sécurité) et en second lieu ceux d'autres référentiels (notamment les normes). Les meilleures pratiques peuvent prendre la forme d'exigences fonctionnelles, d'exigences d'assurance, de principes, de règles, de mesures, de contre-mesures ou de contrôles de sécurité selon les référentiels. ❑ Une estimation de l'impact de l'application des meilleures pratiques SSI doit être réalisée. La réflexion doit porter sur les aspects calendaires, financiers et humains. Elle doit contribuer au choix des meilleures pratiques qui ne remettent pas en cause les objectifs du projet.
Livrables	❑ Une liste des meilleures pratiques SSI applicables dans le cadre du projet doit être établie et validée par le directeur de projet.
Outils	❑ Référentiel SSI de l'organisme ❑ Meilleures pratiques SSI
Synthèse	

4.3.3 Niveaux 3 à 5



Étape 3	Conception générale (niveaux 3 à 5)
Objectif	La conception générale doit permettre de construire le cahier des charges. Ce cahier des charges SSI sera constitué d'un ensemble d'objectifs de sécurité auxquels devra répondre le système et les procédures organisationnelles associées.
Préalables	❑ Note de stratégie de sécurité
Description	❑ Cette étape permet d'identifier les objectifs de sécurité en fonction des éléments de stratégie recueillis. Il convient d'approfondir le contenu de la note de stratégie de sécurité. Ainsi, la description du système est affinée à mesure que sa conception s'affine (notamment les entités qui le composent), les éléments essentiels (patrimoine informationnel) sont parfaitement identifiés, leurs besoins de sécurité exprimés, les vulnérabilités sont étudiées si l'état d'avancement de la conception le permet, les menaces sont rédigées et les risques sont déterminés afin d'identifier les objectifs de sécurité.
Livrables	❑ Une première version de fiche d'expression rationnelle des objectifs de sécurité (FEROS) du projet doit être rédigée et validée par le directeur de projet.
Outils	❑ Méthode de gestion des risques SSI (par exemple [EBIOS]) ❑ Guide de rédaction de FEROS (par exemple [Guide 150])
Synthèse	

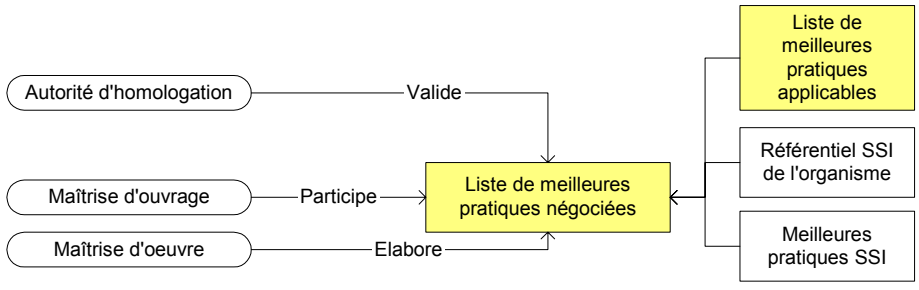


4.4 Étape 4 – Conception détaillée

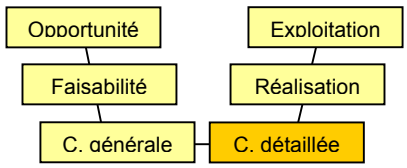
4.4.1 Niveau 1

Dans le cas où la note de stratégie de sécurité statuerait sur le fait que le projet doit être mené avec un très faible niveau de maturité SSI (type 1), aucune action SSI n'est à mener lors de cette étape.

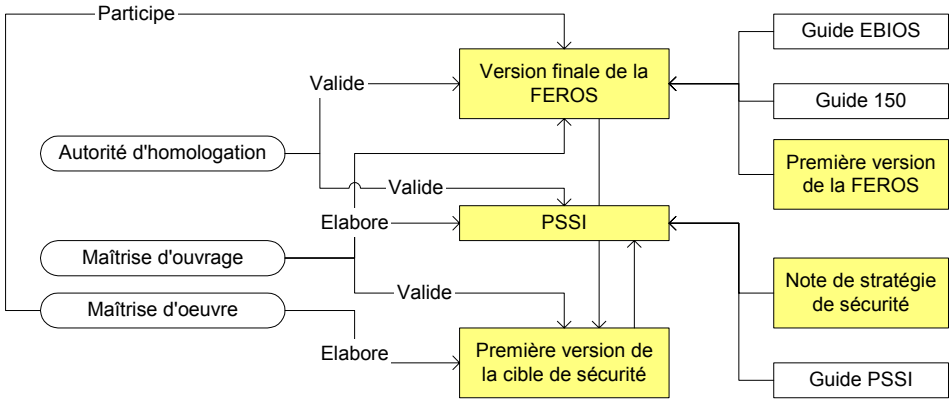
4.4.2 Niveau 2

Étape 4	Conception détaillée (niveau 2)
Objectif	Lors de la conception détaillée, la maîtrise d'œuvre est identifiée, l'objectif est alors de décrire l'engagement des deux parties en terme de meilleures pratiques SSI applicables dans le cadre du projet. Cette étape permet d'aboutir à un cahier des clauses techniques particulières (CCTP) ou équivalent.
Préalables	❑ Liste des meilleures pratiques applicables
Description	❑ Les choix effectués lors de la conception générale doivent être revus et négociés lors de la finalisation du contrat avec la maîtrise d'œuvre, notamment des éléments sur la sécurité des développeurs, l'environnement de production, la gestion de configuration. Cette négociation est faite sur la base des éléments de coûts fournis lors du choix du maître d'œuvre. ❑ On définira également la nature des niveaux de garantie que l'on souhaite pour les éléments matériels ou logiciels SSI du projet. Par exemple, la maîtrise d'ouvrage peut imposer des produits qualifiés au niveau standard pour les fonctions de filtrages.
Livrables	❑ La liste des meilleures pratiques SSI négociées doit être élaborée et affinée pour être jointe au CCTP après validation par le directeur de projet.
Outils	❑ Référentiel SSI de l'organisme ❑ Meilleures pratiques SSI
Synthèse	

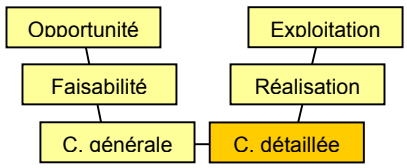
4.4.3 Niveau 3



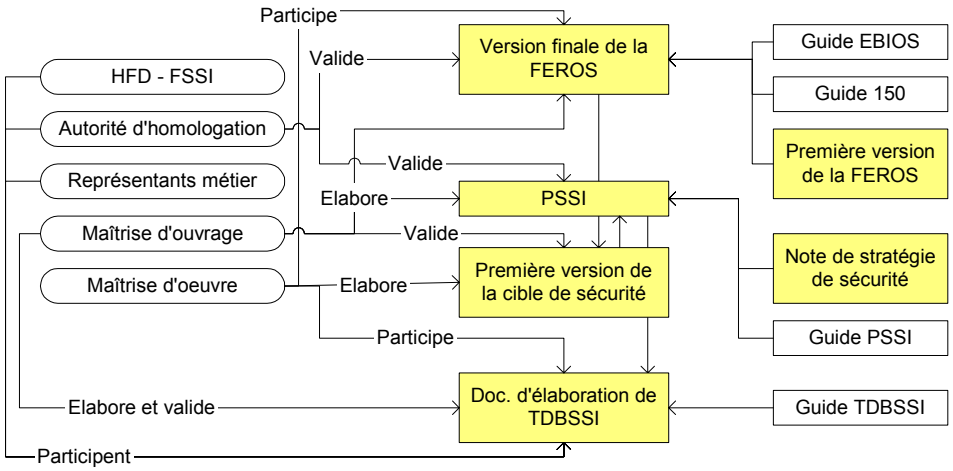
Étape 4	Conception détaillée (niveau 3)
Objectif	L'objectif est ici de décrire l'engagement entre la maîtrise d'œuvre et la maîtrise d'ouvrage en termes d'exigences de sécurité. Cette étape permet d'aboutir à un cahier des clauses techniques particulières (CCTP) intégrant les spécifications SSI.
Préalables	❑ Note de stratégie de sécurité ❑ Première version de FEROS
Description	❑ L'étude de sécurité doit être affinée en conséquence du raffinement de la conception. Il convient de détailler les entités composant le système et d'étudier leurs vulnérabilités précisément avec la maîtrise d'œuvre. Ceci permet d'approfondir les menaces, les risques et les objectifs de sécurité. ❑ Les règles de sécurité doivent être formalisées en fonction de la note de stratégie de sécurité et des objectifs de sécurité. Seules les règles spécifiques par rapport à la PSSI de l'organisme sont formalisées (déclinaison de règles générales, nouvelles règles ou exceptions). ❑ Le traitement des risques doit être précisé par la détermination d'exigences de sécurité fonctionnelles permettant de couvrir les objectifs de sécurité. Il convient d'en démontrer la couverture, de préciser si elles sont techniques ou organisationnelles et de faire émerger les risques résiduels. Des exigences d'assurance augmentent la confiance envers les fonctions de sécurité (un niveau d'assurance, selon l'[ISO 15408], pourra être choisi pour certains composants du projets qui devront être évalués).
Livrables	❑ Une version finale de la FEROS doit être rédigée. Elle doit être validée par le directeur de projet. Elle pourra être annexé au CCTP. ❑ Une première version de cible de sécurité doit être rédigée et validée par le directeur de projet. ❑ Une politique de sécurité du système d'information (PSSI), composée de la note de stratégie de sécurité et des règles de sécurité spécifiques au projet, doit être élaborée, et doit être validée par l'autorité d'homologation.
Outils	❑ Méthode de gestion des risques SSI (par exemple [EBIOS]) ❑ Guide de rédaction de FEROS (par exemple [Guide 150]) ❑ Méthode d'élaboration de PSSI (par exemple [PSSI])

Étape 4	Conception détaillée (niveau 3)
Synthèse	

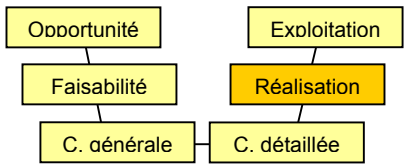
4.4.4 Niveaux 4 à 5



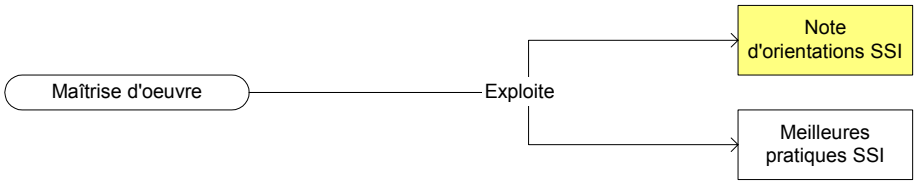
Étape 4	Conception détaillée (niveaux 4 à 5)
Objectif	L'objectif est ici de décrire l'engagement entre la maîtrise d'œuvre et la maîtrise d'ouvrage en termes d'exigences de sécurité. Cette étape permet d'aboutir à un cahier des clauses techniques particulières (CCTP) intégrant les spécifications SSI. C'est sur cette base que seront élaborés les tableaux de bord SSI.
Préalables	❑ Note de stratégie de sécurité ❑ Première version de FEROS
Description	❑ L'étude de sécurité doit être affinée en conséquence du raffinement de la conception. Il convient de détailler les entités composant le système et d'étudier leurs vulnérabilités précisément avec la maîtrise d'œuvre. Ceci permet d'approfondir les menaces, les risques et les objectifs de sécurité. ❑ Les règles de sécurité doivent être formalisées en fonction de la note de stratégie de sécurité et des objectifs de sécurité. Seules les règles spécifiques par rapport à la PSSI de l'organisme sont formalisées (déclinaison de règles générales, nouvelles règles ou exceptions). ❑ Le traitement des risques doit être précisé par la détermination d'exigences de sécurité fonctionnelles permettant de couvrir les objectifs de sécurité. Il convient d'en démontrer la couverture, de préciser si elles sont techniques ou organisationnelles et de faire émerger les risques résiduels. Des exigences d'assurance augmentent la confiance envers les fonctions de sécurité (un niveau d'assurance, selon l'[ISO 15408], pourra être choisi pour certains composants du projets qui devront être évalués). ❑ Des tableaux de bord SSI doivent être élaborés pour les niveaux stratégiques, de pilotage et opérationnel, en fonction des règles de sécurité (ou des objectifs de sécurité ou des exigences de sécurité selon ce qui est jugé le plus pertinent). Il convient pour cela d'organiser des groupes de travail et de déterminer les objectifs mesurables, les points-clés et les indicateurs qui en découlent afin de décrire les tableaux de bord SSI et leurs procédures d'alimentation.
Livrables	❑ Une version finale de la FEROS doit être rédigée. Elle doit être validée par le directeur de projet. Elle pourra être annexé au CCTP. ❑ Une première version de cible de sécurité doit être rédigée et validée par le directeur de projet. ❑ Une politique de sécurité du système d'information (PSSI), composée de la note de stratégie de sécurité et des règles de sécurité spécifiques au projet, doit être élaborée, et doit être validée par l'autorité d'homologation. ❑ Une documentation d'élaboration des tableaux de bord SSI (TDBSSI) doit être rédigée. Elle doit être validée par le directeur de projet.

Étape 4	Conception détaillée (niveaux 4 à 5)
Outils	❑ Méthode de gestion des risques SSI (par exemple [EBIOS]) ❑ Guide de rédaction de FEROS (par exemple [Guide 150]) ❑ Méthode d'élaboration de PSSI (par exemple [PSSI]) ❑ Méthode d'élaboration de TDBSSI (par exemple [TDBSSI])
Synthèse	

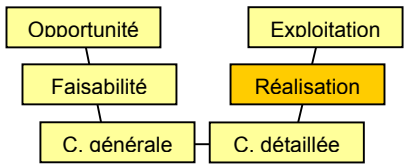
4.5 Étape 5 – Réalisation

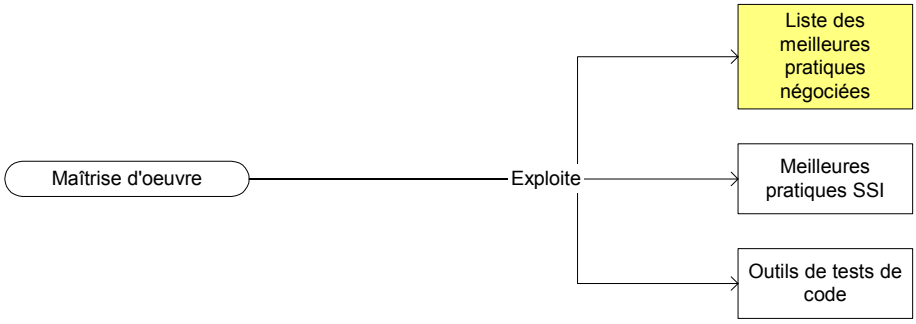


4.5.1 Niveau 1

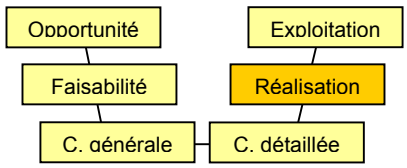
Étape 5	Réalisation (niveau 1)
Objectif	L'objectif de la réalisation est de mettre en œuvre les meilleures pratiques en matière de sécurité informatique, notamment en terme de développement.
Préalables	❑ Note d'orientations SSI
Description	❑ La maîtrise d'œuvre doit mettre en œuvre les meilleures pratiques SSI de conception, développement, la gestion de configuration, d'une manière occasionnelle et informelle.
Livrables	❑ Aucun livrable particulier pour cette étape
Outils	❑ Meilleures pratiques SSI
Synthèse	

4.5.2 Niveau 2

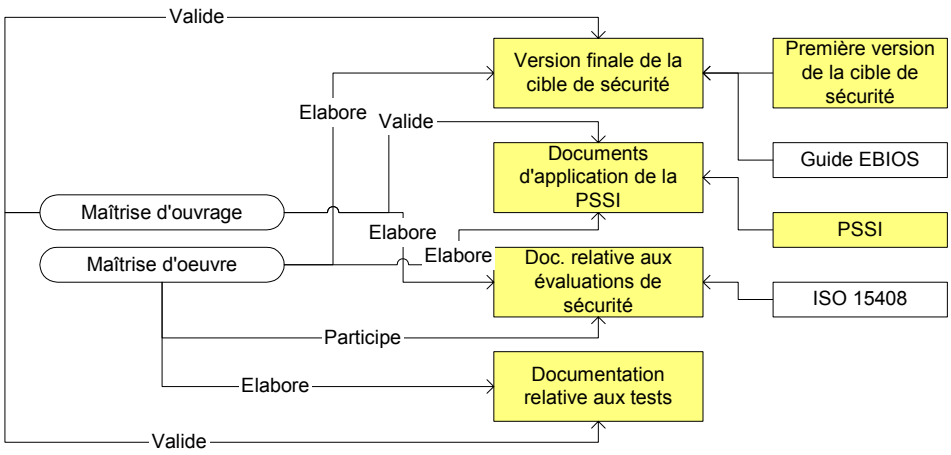


Étape 5	Réalisation (niveau 2)
Objectif	L'objectif de la réalisation est l'application des meilleures pratiques SSI, leur vérification par la maîtrise d'œuvre et la vérification de conformité par rapport aux attentes de la maîtrise d'ouvrage.
Préalables	❑ Liste des meilleures pratiques négociées
Description	❑ Lors de la phase de **développement**, la maîtrise d'œuvre doit mettre en œuvre les meilleures pratiques SSI de conception, de développement et de gestion de configuration qui auront été retenues lors de la phase de conception détaillée. ❑ Lors de la phase de **codage**, les développeurs doivent mettre en œuvre les meilleures pratiques SSI de codage qui auront été retenues lors de la phase de conception détaillée. Ils rechercheront à mettre en œuvre les fonctions de sécurité (contrôle d'accès, filtrage…) conformément à l'état de l'art. Des tests unitaires et/ou des revues de code doivent également être réalisés. ❑ Lors de la phase d'**intégration**, les développeurs doivent mettre en œuvre les meilleures pratiques SSI d'intégration qui auront été retenues lors de la phase de conception détaillée. ❑ Lors de la phase de **qualification**, la maîtrise d'œuvre doit vérifier la bonne application des meilleures pratiques SSI retenues, vérifier le bon fonctionnement du système et confirmer les performances SSI attendues. ❑ Lors de la phase de **recette**, la maîtrise d'ouvrage doit vérifier que l'application des meilleures pratiques SSI retenues dans le cadre du développement du projet est conforme à ses attentes exprimées dans la note de stratégie de sécurité. Elle peut aussi valider la conformité de l'intégration du progiciel, ses paramétrages et ses interfaces à partir de jeux d'essai.
Livrables	❑ Aucun livrable particulier pour cette étape.
Outils	❑ Meilleures pratiques SSI ❑ Outils de tests de code
Synthèse	

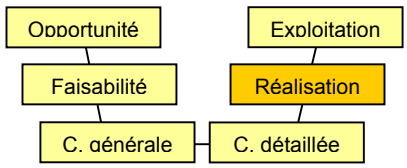
4.5.3 Niveau 3



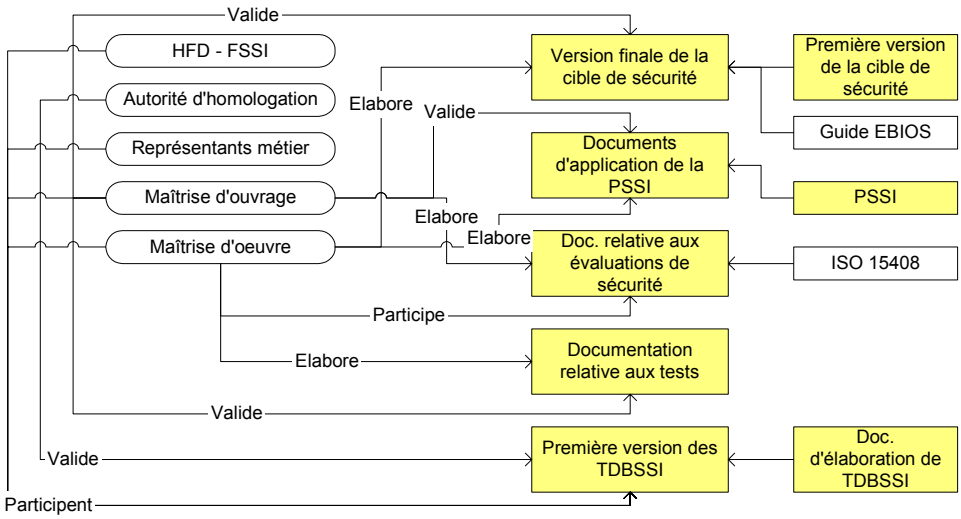
Étape 5	Réalisation (niveau 3)
Objectif	L'objectif de cette étape est d'affiner la réflexion de sécurité, de développer la documentation de sécurité, de mettre en œuvre les fonctions de sécurité spécifiées et d'en vérifier le bon fonctionnement. Cette étape peut aussi faire l'objet de la production de la documentation nécessaire aux évaluations de sécurité (selon l'[ISO 15408]) et aux évaluations elles-mêmes.
Préalables	❑ Première version de la cible de sécurité ❑ PSSI
Description	❑ Lors de la phase de **développement**, la maîtrise d'œuvre peut découper le projet en sous-systèmes et doit affiner la gestion des risques SSI pour les cibler sur des entités précises du SI, revoir la couverture des objectifs par des exigences de sécurité plus adaptées. Dans le cas où une partie du SI doit être évaluée, la maîtrise d'œuvre doit élaborer les documents nécessaires (spécifications cryptologiques, gestion de configuration…). ❑ Lors de la phase de **codage**, le développeur doit affiner l'analyse des fonctions de sécurité et renseigner les parties de la cible de sécurité dont il a la charge. Il doit également rédiger les livrables de son ressort, notamment les documents de tests unitaires et les livrables nécessaires si le sous-projet doit faire l'objet d'une évaluation. ❑ Lors de la phase d'**intégration**, les exigences de sécurité du SI doivent être complétées et affinées en fonction du développement et du codage. Par ailleurs, les règles de sécurité doivent être déclinées en documents d'application, notamment de procédures d'exploitation de sécurité (PES). ❑ Lors de la phase de **qualification**, la maîtrise d'œuvre doit passer en revue le cahier de recette. Elle doit également réaliser des tests concernant la qualité de la documentation associée et les vulnérabilités concernant les chevaux de Troie, le code incorrect (*buffer overflow*), les outils de développement mal configurés, les codes malveillants… ❑ Lors de la phase de **recette**, la maîtrise d'ouvrage doit réaliser les mêmes tests que la maîtrise d'œuvre. Elle peut aussi mener un audit de sécurité afin de vérifier la conformité à la PSSI. Cet audit peut être utilement mené par des experts extérieurs au projet. Durant cette phase, les éventuelles évaluations de sécurité doivent être terminées.

Étape 5	Réalisation (niveau 3)
Livrables	❑ Une version finale de cible de sécurité (éventuellement découpée en sous-systèmes) doit être rédigée. Elle doit être validée par le directeur de projet. ❑ Les documents d'application de la PSSI doivent être élaborés au fur et à mesure de l'avancement de la réalisation, notamment les procédures d'exploitation de sécurité (PES). ❑ La documentation relative aux évaluations de sécurité doit être réalisée dans le cas où certaines parties du SI feraient l'objet d'une évaluation de sécurité : o la documentation nécessaire à l'évaluation en fonction des exigences de sécurité retenues, o les rapports d'évaluation (rédigés par l'évaluateur). ❑ La documentation relative aux tests doit être rédigée : o cahier de recette, o documentation des tests unitaires, o compte-rendu de qualification, o compte-rendu de recette, o rapport d'audit de sécurité.
Outils	❑ Méthode de gestion des risques SSI (par exemple [EBIOS]) ❑ Norme pour l'évaluation (par exemple l'[ISO 15408])
Synthèse	

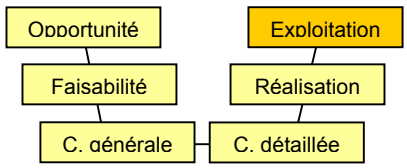
4.5.4 Niveaux 4 à 5



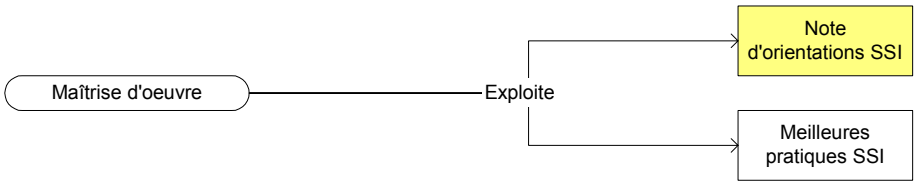
Étape 5	Réalisation (niveaux 4 à 5)
Objectif	L'objectif de cette étape est d'affiner la réflexion de sécurité, de développer la documentation de sécurité, de mettre en œuvre les fonctions de sécurité spécifiées et d'en vérifier le bon fonctionnement. Cette étape peut aussi faire l'objet de la production de la documentation nécessaire aux évaluations de sécurité (selon l'[ISO 15408]) et aux évaluations elles-mêmes.
Préalables	❑ Première version de la cible de sécurité ❑ PSSI ❑ Documentation d'élaboration de TDBSSI
Description	❑ Lors de la phase de **développement**, la maîtrise d'œuvre peut découper le projet en sous-systèmes et doit affiner la gestion des risques SSI pour les cibler sur des entités précises du SI, revoir la couverture des objectifs par des exigences de sécurité plus adaptées. Dans le cas où une partie du SI doit être évaluée, la maîtrise d'œuvre doit élaborer les documents nécessaires (spécifications cryptologiques, gestion de configuration…). ❑ Lors de la phase de **codage**, le développeur doit affiner l'analyse des fonctions de sécurité et renseigner les parties de la cible de sécurité dont il a la charge. Il doit également rédiger les livrables de son ressort, notamment les documents de tests unitaires et les livrables nécessaires si le sous-projet doit faire l'objet d'une évaluation. ❑ Lors de la phase d'**intégration**, les exigences de sécurité du SI doivent être complétées et affinées en fonction du développement et du codage. Par ailleurs, les règles de sécurité doivent être déclinées en documents d'application, notamment de procédures d'exploitation de sécurité (PES). ❑ Lors de la phase de **qualification**, la maîtrise d'œuvre doit passer en revue le cahier de recette. Elle doit également réaliser des tests concernant la qualité de la documentation associée et les vulnérabilités concernant les chevaux de Troie, le code incorrect (*buffer overflow*), les outils de développement mal configurés, les codes malveillants… Elle doit enfin renseigner les indicateurs SSI dont elle a la charge. ❑ Lors de la phase de **recette**, la maîtrise d'ouvrage doit réaliser les mêmes tests que la maîtrise d'œuvre. Elle peut aussi mener un audit de sécurité afin de vérifier la conformité à la PSSI. Cet audit peut être utilement mené par des experts extérieurs au projet. Durant cette phase, les éventuelles évaluations de sécurité doivent être terminées. Elle doit enfin renseigner les indicateurs SSI dont elle a la charge.

Étape 5	Réalisation (niveaux 4 à 5)
Livrables	❑ Une version finale de cible de sécurité (éventuellement découpée en sous-systèmes) doit être rédigée. Elle doit être validée par le directeur de projet. ❑ Les documents d'application de la PSSI doivent être élaborés au fur et à mesure de l'avancement de la réalisation, notamment les procédures d'exploitation de sécurité (PES). ❑ La documentation relative aux évaluations de sécurité doit être réalisée dans le cas où certaines parties du SI feraient l'objet d'une évaluation de sécurité : o la documentation nécessaire à l'évaluation en fonction des exigences de sécurité retenues, o les rapports d'évaluation (rédigés par l'évaluateur). ❑ La documentation relative aux tests doit être rédigée : o cahier de recette, o documentation des tests unitaires, o compte-rendu de qualification, o compte-rendu de recette, o rapport d'audit de sécurité. ❑ Une première version des TDBSSI doit être éditée sur la base de la documentation d'élaboration des TDBSSI.
Outils	❑ Méthode de gestion des risques SSI (par exemple [EBIOS]) ❑ Norme pour l'évaluation (par exemple l'[ISO 15408]) ❑ Méthode d'élaboration de TDBSSI (par exemple [TDBSSI])
Synthèse	

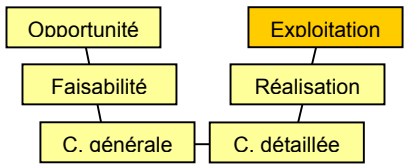
4.6 Étape 6 – Exploitation

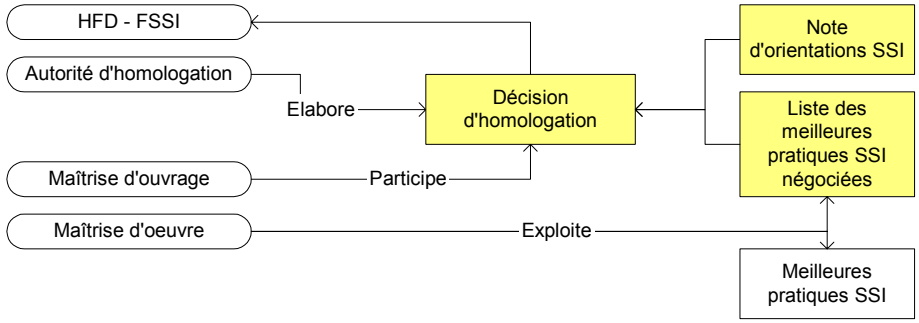


4.6.1 Niveau 1

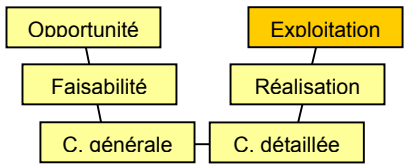
Étape 6	Exploitation (niveau 1)
Objectif	L'objectif de cette étape est de faire homologuer le SI afin de déclarer qu'il est apte à traiter des informations et que les risques de sécurité résiduels sont acceptés et maîtrisés. Le reste de l'exploitation consistera à mettre en œuvre des meilleures pratiques SSI de manière informelle tout au long du cycle de vie du SI.
Préalables	❑ Dossier de sécurité - Note d'orientations SSI
Description	❑ Lors de la phase d'**homologation**, la décision d'homologation doit être prononcée par l'autorité d'homologation sur la base de la note d'orientations SSI. ❑ Lors des phases de **déploiement**, de **mise en œuvre**, de **maintenance** et de **retrait de service**, des meilleures pratiques SSI peuvent être mises en œuvre de manière informelle.
Livrables	❑ Aucun livrable particulier pour cette étape.
Outils	❑ Meilleures pratiques SSI
Synthèse	

4.6.2 Niveau 2

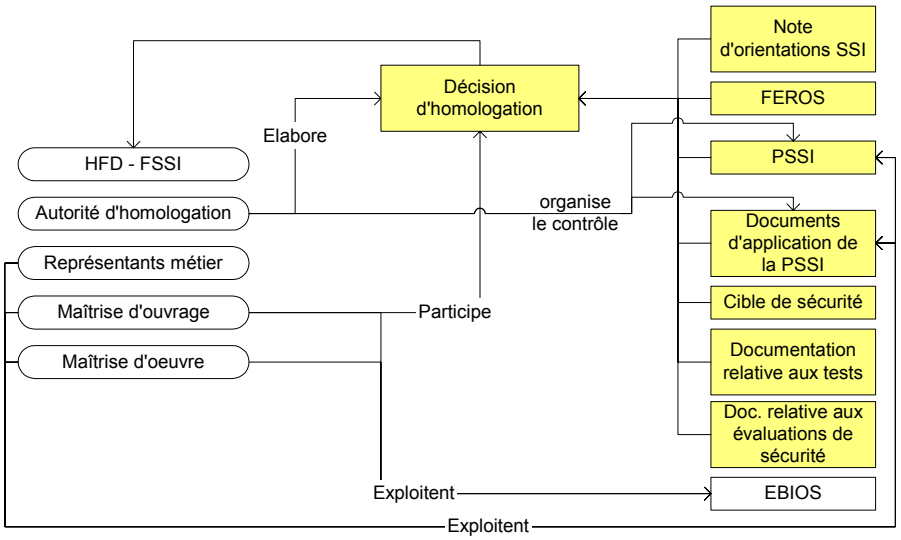


Étape 6	Exploitation (niveau 2)
Objectif	L'objectif de cette étape est de faire homologuer le SI afin de déclarer qu'il est apte à traiter des informations et que les risques de sécurité résiduels sont acceptés et maîtrisés. Le reste de l'exploitation consistera à mettre en œuvre des meilleures pratiques SSI de manière planifiée et suivie tout au long du cycle de vie du SI.
Préalables	❑ Dossier de sécurité - Note d'orientations SSI - Liste des meilleures pratiques SSI négociées
Description	❑ Lors de la phase d'**homologation**, la décision d'homologation doit être prononcée par l'autorité d'homologation conformément à la note d'orientations SSI et sur la base du dossier de sécurité du SI, qui contient l'ensemble de la documentation SSI produite depuis le début du projet. ❑ Lors de la phase de **déploiement**, il convient de former et d'assurer la prise en compte du changement auprès des utilisateurs en s'appuyant sur les meilleures pratiques. En outre, la prise en compte de la sécurité physique doit être traitée en s'appuyant sur les meilleures pratiques. ❑ Lors de la phase de **mise en œuvre**, les exploitants doivent mettre en œuvre les meilleures pratiques SSI retenues, notamment sur les sujets suivants : sauvegardes, formation, gestion des clés cryptographiques, gestion des utilisateurs et des privilèges, audits réguliers des journaux d'événements, mises à jour de sécurité des logiciels, revues régulières des protections physiques, revue des solutions de continuité et de stockage, revues régulières des garanties et contrat logiciels et matériel. ❑ Lors de la phase de **maintenance**, il convient de mettre en œuvre des meilleures pratiques SSI en terme de maintien en condition de sécurité (MCS), notamment en ce qui concerne l'application des mises à jour de sécurité, la définition des éléments de MCS dans le cadre des contrats… ❑ Lors de la phase de **retrait de service**, il convient de mettre en œuvre des meilleures pratiques SSI relatives à la fin de vie des SI.
Livrables	❑ L'autorité d'homologation doit rédiger une note formalisant sa décision d'homologation.
Outils	❑ Meilleures pratiques SSI
Synthèse	

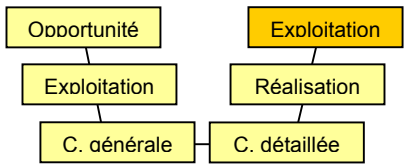
4.6.3 Niveau 3



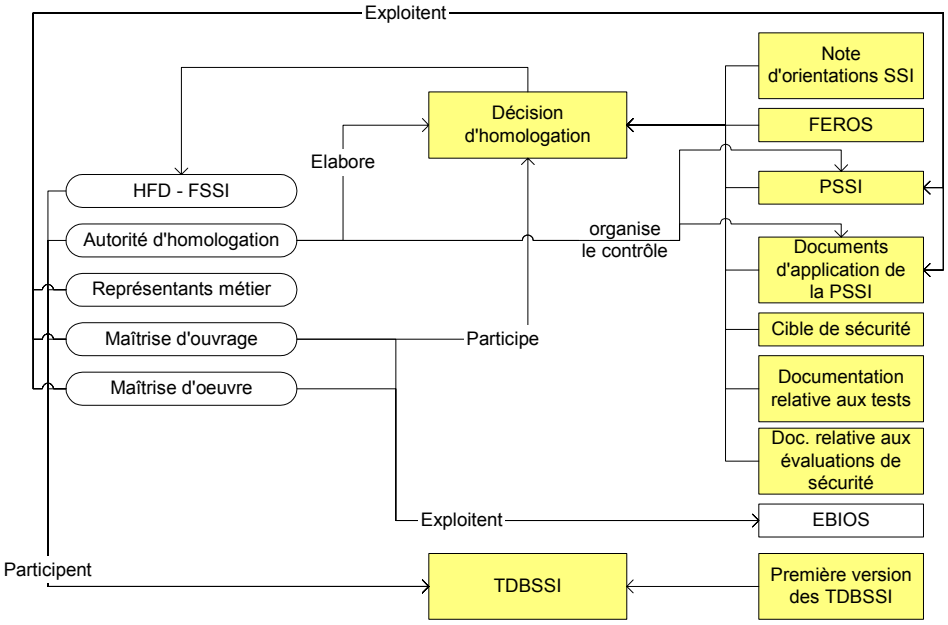
Étape 6	Exploitation (niveau 3)
Objectif	L'objectif de cette étape est de faire homologuer le SI afin de déclarer qu'il est apte à traiter des informations et que les risques de sécurité résiduels sont acceptés et maîtrisés. Le reste de l'exploitation consiste à mettre en œuvre les règles de sécurité de manière formalisée, coordonnée et cohérente avec les processus de l'organisme tout au long du cycle de vie du SI.
Préalables	❑ Dossier de sécurité - Note d'orientations SSI - FEROS - PSSI (note de stratégie de sécurité et règles de sécurité) - Documents d'application de la PSSI - Cible de sécurité - Documentation relative aux tests - Documentation relative aux évaluations de sécurité
Description	❑ Lors de la phase d'**homologation**, la décision d'homologation doit être prononcée par l'autorité d'homologation conformément à la note d'orientations SSI et sur la base du dossier de sécurité du SI, qui contient l'ensemble de la documentation SSI produite. ❑ Lors de la phase de **déploiement**, les mesures de sécurité définies doivent être mises en œuvre. Il convient d'informer sur les enjeux de sécurité du système, les risques SSI, les exigences de sécurité et notamment les responsabilités qui incombent à chacun des acteurs du SI. Le déploiement doit être réalisé conformément aux exigences de sécurité. ❑ Lors de la phase de **mise en œuvre**, les règles de sécurité de la politique de sécurité et de ses documents d'application doivent être appliquées. Par ailleurs, l'autorité d'homologation doit mettre en place des procédures de vérification de conformité par rapport à la PSSI et ses documents d'application. Ces contrôles (contrôles hiérarchiques, inspections, audits…) pourront être opérés par des experts extérieurs à l'organisme et porteront notamment sur les points suivants : sauvegardes, formation, gestion des clés cryptographiques, gestion des utilisateurs et des privilèges, audits réguliers des journaux d'événements, mises à jour de sécurité des logiciels, revues des protections physiques, revue des solutions de continuité et de stockage, revues des garanties et contrat logiciels et matériel. ❑ Lors de la phase de **maintenance**, les règles de sécurité de la politique de sécurité et de ses documents d'application doivent être appliquées. Par ailleurs, il convient de mettre à jour périodiquement les éléments de gestion des risques SSI de manière à prendre en compte les évolutions contextuelles (changement des entités du SI, réévaluation de la menace, revalorisation des besoins de sécurité…) qui pourraient nécessiter une remise en question des objectifs de sécurité. ❑ Lors de la phase de **retrait de service**, les règles de sécurité de la politique de sécurité et de ses documents d'application doivent être appliquées.

Étape 6	Exploitation (niveau 3)
Livrables	❑ L'autorité d'homologation doit rédiger une note formalisant la décision d'homologation. ❑ Le dossier de sécurité doit être enrichi par des documents de communication (information, sensibilisation ou formation) et des rapports de vérification de conformité. Par ailleurs, il peut nécessiter des mises à jour reflétant l'évolution des éléments de la gestion des risques SSI. Ces mises à jour peuvent remettre en question l'homologation de sécurité.
Outils	❑ Méthode de gestion des risques SSI (par exemple [EBIOS])
Synthèse	

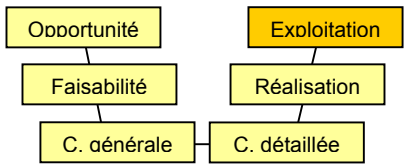
4.6.4 Niveau 4



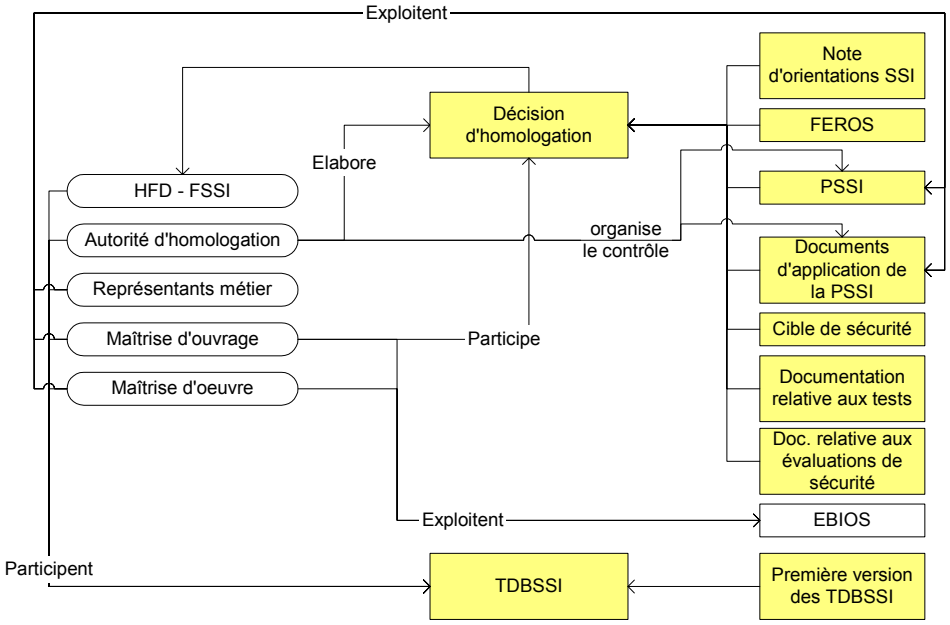
Étape 6	Exploitation – Homologation (niveau 4)
Objectif	L'objectif de cette étape est de faire homologuer le SI afin de déclarer qu'il est apte à traiter des informations et que les risques de sécurité résiduels sont acceptés et maîtrisés. Le reste de l'exploitation consiste à mettre en œuvre les règles de sécurité de manière formalisée, coordonnée, cohérente avec les processus de l'organisme et contrôlée qualitativement tout au long du cycle de vie du SI.
Préalables	❑ Dossier de sécurité - Note d'orientations SSI - FEROS - PSSI (note de stratégie de sécurité et règles de sécurité) - Documents d'application de la PSSI - Cible de sécurité - Documentation relative aux tests - Documentation relative aux évaluations de sécurité - Première version des TDBSSI
Description	❑ Lors de la phase d'**homologation**, la décision d'homologation doit être prononcée par l'autorité d'homologation conformément à la note d'orientations SSI et sur la base du dossier de sécurité du SI, qui contient l'ensemble de la documentation SSI produite. ❑ Lors de la phase de **déploiement**, les mesures de sécurité définies doivent être mises en œuvre. Il convient d'informer sur les enjeux de sécurité du système, les risques SSI, les exigences de sécurité et notamment les responsabilités qui incombent à chacun des acteurs du SI. Le déploiement doit être réalisé conformément aux exigences de sécurité. ❑ Lors de la phase de **mise en œuvre**, les règles de sécurité de la politique de sécurité et de ses documents d'application doivent être appliquées. Par ailleurs, l'autorité d'homologation doit mettre en place des procédures de vérification de conformité par rapport à la PSSI et ses documents d'application. Ces contrôles (contrôles hiérarchiques, inspections, audits…) pourront être opérés par des experts extérieurs à l'organisme et porteront notamment sur les points suivants : sauvegardes, formation, gestion des clés cryptographiques, gestion des utilisateurs et des privilèges, audits réguliers des journaux d'événements, mises à jour de sécurité des logiciels, revues régulières des protections physiques, revue des solutions de continuité et de stockage, revues des garanties et contrat logiciels et matériel. Les tableaux de bord SSI doivent être alimentés. ❑ Lors de la phase de **maintenance**, les règles de sécurité de la politique de sécurité et de ses documents d'application doivent être appliquées. Par ailleurs, il convient de mettre à jour périodiquement les éléments de gestion des risques SSI de manière à prendre en compte les évolutions contextuelles (changement des entités du SI, réévaluation de la menace, revalorisation des besoins de sécurité…) qui pourraient nécessiter une remise en question des objectifs de sécurité. ❑ Lors de la phase de **retrait de service**, les règles de sécurité de la PSSI et de ses documents d'application doivent être appliquées.

Étape 6	Exploitation – Homologation (niveau 4)
Livrables	❑ L'autorité d'homologation doit rédiger une note formalisant la décision d'homologation. ❑ Le dossier de sécurité doit être enrichi par des documents de communication (information, sensibilisation ou formation) et des rapports de vérification de conformité. Par ailleurs, il peut nécessiter des mises à jour reflétant l'évolution des éléments de la gestion des risques SSI. Ces mises à jour peuvent remettre en question l'homologation de sécurité. ❑ Les TDBSSI doivent être alimentés et diffusés régulièrement.
Outils	❑ Méthode de gestion des risques SSI (par exemple [EBIOS]) ❑ Méthode d'élaboration de TDBSSI (par exemple [TDBSSI])
Synthèse	

4.6.5 Niveau 5

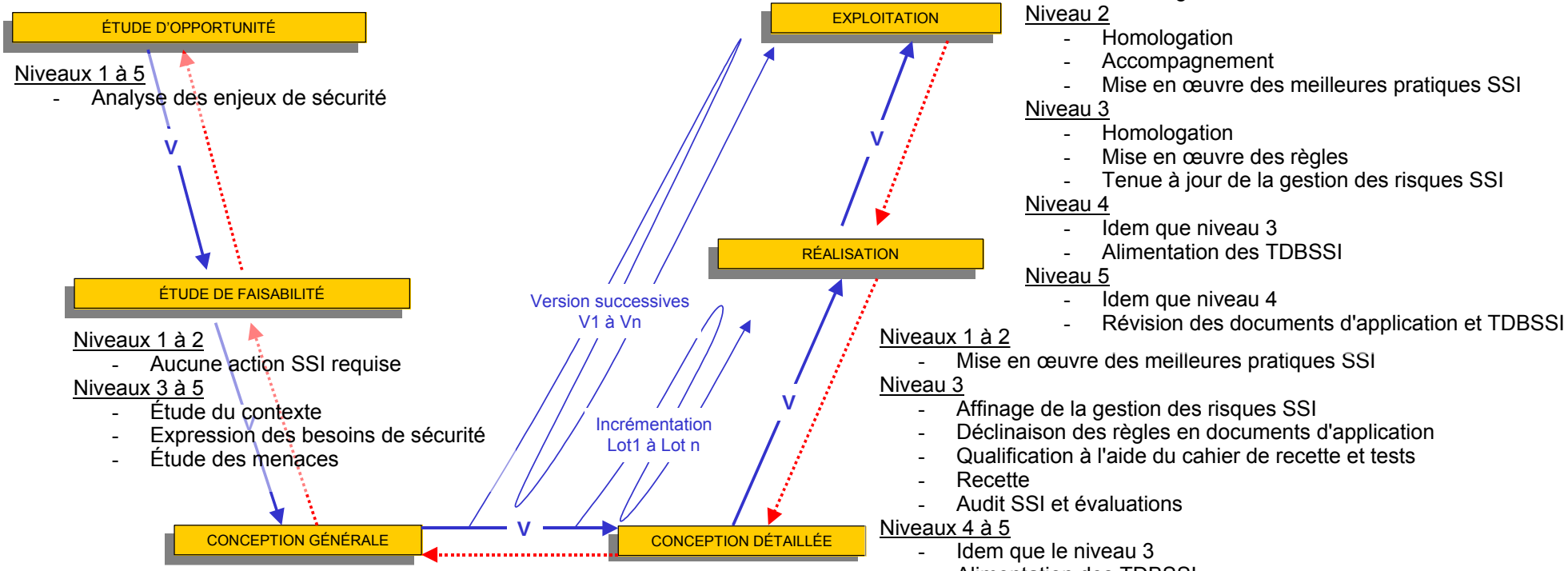


Étape 6	Exploitation – Homologation (niveau 5)
Objectif	L'objectif de cette étape est de faire homologuer le SI afin de déclarer qu'il est apte à traiter des informations et que les risques de sécurité résiduels sont acceptés et maîtrisés. Le reste de l'exploitation consiste à mettre en œuvre les règles de sécurité de manière formalisée, coordonnée, cohérente avec les processus de l'organisme, contrôlée qualitativement et continuellement améliorée tout au long du cycle de vie du SI.
Préalables	❑ Dossier de sécurité - Note d'orientations SSI - FEROS - PSSI (note de stratégie de sécurité et règles de sécurité) - Documents d'application de la PSSI - Cible de sécurité - Documentation relative aux tests - Documentation relative aux évaluations de sécurité - Première version des TDBSSI
Description	❑ Lors de la phase d'**homologation**, la décision d'homologation doit être prononcée par l'autorité d'homologation conformément à la note d'orientations SSI et sur la base du dossier de sécurité du SI, qui contient l'ensemble de la documentation SSI produite. ❑ Lors de la phase de **déploiement**, les mesures de sécurité définies doivent être mises en œuvre. Il convient d'informer sur les enjeux de sécurité du système, les risques SSI, les exigences de sécurité et notamment les responsabilités qui incombent à chacun des acteurs du SI. Le déploiement doit être réalisé conformément aux exigences de sécurité. ❑ Lors de la phase de **mise en œuvre**, les règles de sécurité de la politique de sécurité et de ses documents d'application doivent être appliquées. Par ailleurs, l'autorité d'homologation doit mettre en place des procédures de vérification de conformité par rapport à la PSSI et ses documents d'application. Ces contrôles (contrôles hiérarchiques, inspections, audits…) pourront être opérés par des experts extérieurs à l'organisme et porteront notamment sur les points suivants : sauvegardes, formation, gestion des clés cryptographiques, gestion des utilisateurs et des privilèges, audits réguliers des journaux d'événements, mises à jour de sécurité des logiciels, revues des protections physiques, revue des solutions de continuité et de stockage, revues des garanties et contrat logiciels et matériel. Les tableaux de bord SSI doivent être alimentés et régulièrement revus afin d'améliorer l'efficacité des processus SSI. ❑ Lors de la phase de **maintenance**, les règles de sécurité de la politique de sécurité et de ses documents d'application doivent être appliquées. Par ailleurs, il convient de mettre à jour périodiquement les éléments de gestion des risques SSI de manière à prendre en compte les évolutions contextuelles (changement des entités du SI, réévaluation de la menace, revalorisation des besoins de sécurité…) qui pourraient nécessiter une remise en question des objectifs de sécurité. Les documents d'application de la PSSI, notamment les PES, doivent être régulièrement revues afin d'améliorer l'efficacité des processus SSI. ❑ Lors de la phase de **retrait de service**, les règles de sécurité de la PSSI et de ses documents d'application doivent être appliquées.

Étape 6	Exploitation – Homologation (niveau 5)
Livrables	❑ L'autorité d'homologation doit rédiger une note formalisant la décision d'homologation. ❑ Le dossier de sécurité doit être enrichi par des documents de communication (information, sensibilisation ou formation) et des rapports de vérification de conformité. Par ailleurs, il peut nécessiter des mises à jour reflétant l'évolution des éléments de la gestion des risques SSI. Ces mises à jour peuvent remettre en question l'homologation de sécurité. ❑ Les TDBSSI doivent être alimentés, diffusés et revus régulièrement.
Outils	❑ Méthode de gestion des risques SSI (par exemple [EBIOS]) ❑ Méthode d'élaboration de TDBSSI (par exemple [TDBSSI])
Synthèse	

4.7 Synthèse des actions SSI à mener par étape et par niveau de maturité SSI adéquat

Le schéma suivant présente de manière synthétique les actions SSI à mener pour chaque étape du cycle de vie des SI.



Niveaux 1 à 5
- Analyse des enjeux de sécurité

Niveaux 1 à 2
- Aucune action SSI requise

Niveaux 3 à 5
- Étude du contexte
- Expression des besoins de sécurité
- Étude des menaces

Niveau 1
- Aucune action SSI requise

Niveau 2
- Inventaire des meilleures pratiques SSI applicables
- Estimation de l'impact de leur application

Niveaux 3 à 5
- Identification des objectifs de sécurité

Niveau 1
- Aucune action SSI requise

Niveau 2
- Revue des choix des meilleures pratiques SSI et négociation
- Réflexion sur la nature des niveaux de garantie

Niveau 3
- Affinage de l'étude de sécurité
- Formalisation des règles de sécurité
- Précision du traitement des risques SSI

Niveaux 4 à 5
- Idem que le niveau 3
- Élaboration des TDBSSI

Niveaux 1 à 2
- Mise en œuvre des meilleures pratiques SSI

Niveau 3
- Affinage de la gestion des risques SSI
- Déclinaison des règles en documents d'application
- Qualification à l'aide du cahier de recette et tests
- Recette
- Audit SSI et évaluations

Niveaux 4 à 5
- Idem que le niveau 3
- Alimentation des TDBSSI

Niveau 1
- Homologation

Niveau 2
- Homologation
- Accompagnement
- Mise en œuvre des meilleures pratiques SSI

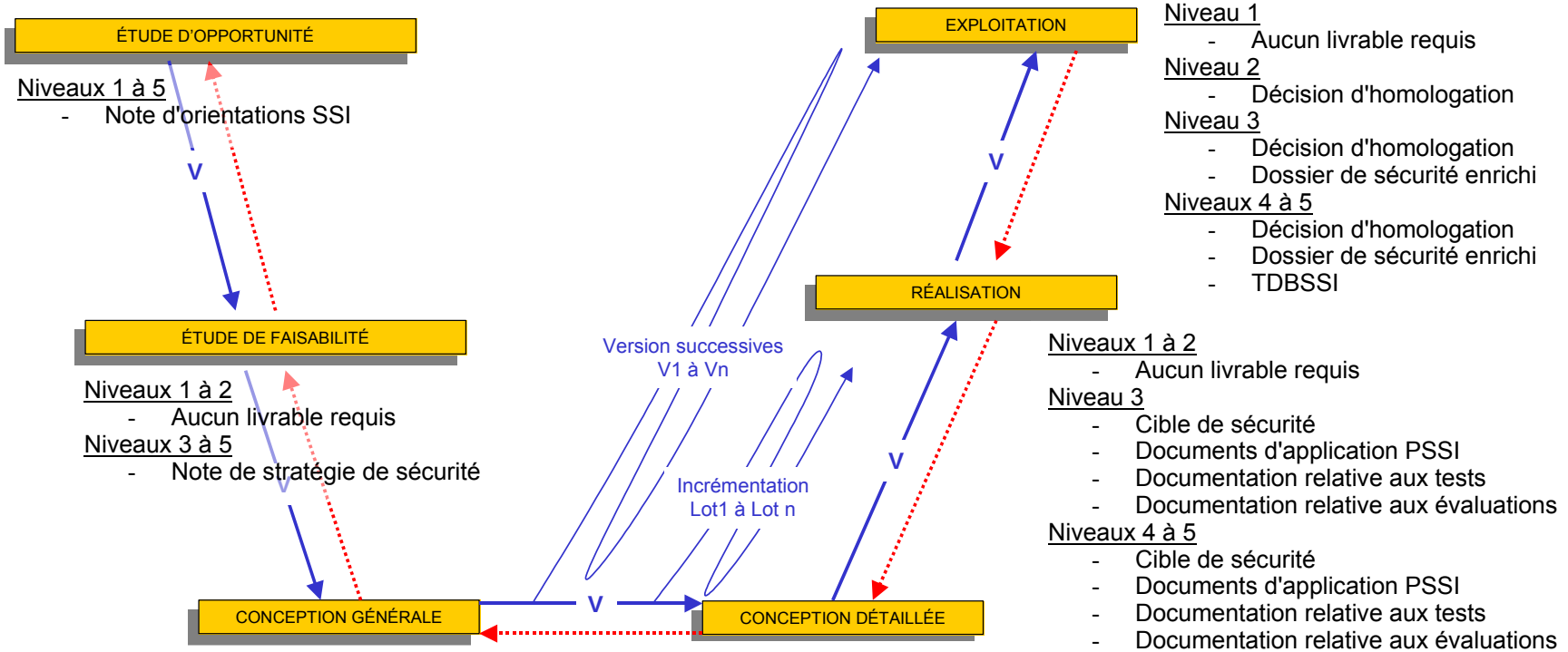
Niveau 3
- Homologation
- Mise en œuvre des règles
- Tenue à jour de la gestion des risques SSI

Niveau 4
- Idem que niveau 3
- Alimentation des TDBSSI

Niveau 5
- Idem que niveau 4
- Révision des documents d'application et TDBSSI

4.8 Synthèse des livrables par étape et par niveau de maturité SSI adéquat

Le schéma suivant présente de manière synthétique les livrables SSI à produire pour chaque étape du cycle de vie des SI.



Niveaux 1 à 5
- Note d'orientations SSI

Niveaux 1 à 2
- Aucun livrable requis

Niveaux 3 à 5
- Note de stratégie de sécurité

Niveau 1
- Aucun livrable requis

Niveau 2
- Liste des meilleures pratiques SSI applicables

Niveaux 3 à 5
- Première version de la FEROS

Niveau 1
- Aucun livrable requis

Niveau 2
- Liste des meilleures pratiques SSI négociées

Niveau 3
- FEROS
- PSSI
- Première version de la cible de sécurité

Niveaux 4 à 5
- FEROS
- PSSI
- Première version de la cible de sécurité
- Documentation d'élaboration de TDBSSI

Niveaux 1 à 2
- Aucun livrable requis

Niveau 3
- Cible de sécurité
- Documents d'application PSSI
- Documentation relative aux tests
- Documentation relative aux évaluations

Niveaux 4 à 5
- Cible de sécurité
- Documents d'application PSSI
- Documentation relative aux tests
- Documentation relative aux évaluations
- Première version de TDBSSI

Niveau 1
- Aucun livrable requis

Niveau 2
- Décision d'homologation

Niveau 3
- Décision d'homologation
- Dossier de sécurité enrichi

Niveaux 4 à 5
- Décision d'homologation
- Dossier de sécurité enrichi
- TDBSSI

4.9 Récapitulatif global des actions et livrables SSI

Le tableau suivant présente de manière synthétique les actions (précédées d'un carré) et livrables SSI (précédés d'une flèche) à produire pour chaque étape du cycle de vie des SI.

Étapes du cycle de vie	Niveau de maturité SSI adéquat				
	1	2	3	4	5
1 Étude d'opportunité	❑ Analyse des enjeux de sécurité → Note d'orientations SSI				
2 Étude de faisabilité	Aucune action SSI requise	Aucune action SSI requise	❑ Étude du contexte ❑ Expression des besoins de sécurité ❑ Étude des menaces → Note de stratégie de sécurité		
3 Conception générale	Aucune action SSI requise	❑ Inventaire des meilleures pratiques applicables ❑ Estimation de l'impact de leur application → Liste des meilleures pratiques applicables	❑ Identification des objectifs de sécurité → Première version de la FEROS		
4 Conception détaillée	Aucune action SSI requise	❑ Revue des choix des meilleures pratiques et négociation ❑ Réflexion sur la nature des niveaux de garantie → Liste des meilleures pratiques négociées	❑ Affinage de l'étude de sécurité → FEROS ❑ Formalisation des règles de sécurité → PSSI ❑ Précision du traitement des risques → Première version de la cible de sécurité	❑ Affinage de l'étude de sécurité → FEROS ❑ Formalisation des règles de sécurité → PSSI ❑ Précision du traitement des risques → Première version de la cible de sécurité ❑ Élaboration des tableaux de bord SSI → Documentation d'élaboration de TDBSSI	
5 Réalisation	❑ Mise en œuvre des meilleures pratiques		❑ Affinage de la gestion des risques → Cible de sécurité ❑ Déclinaison des règles en documents d'application → Documents d'application PSSI ❑ Qualification à l'aide du cahier de recette et tests ❑ Recette ❑ Audit et évaluations → Documentation relative aux tests → Documentation relative aux évaluations	❑ Affinage de la gestion des risques → Cible de sécurité ❑ Déclinaison des règles en documents d'application → Documents d'application PSSI ❑ Qualification à l'aide du cahier de recette et tests ❑ Recette ❑ Audit et évaluations → Documentation relative aux tests → Documentation relative aux évaluations ❑ Alimentation des TDBSSI → Première version de TDBSSI	
6 Exploitation	❑ Homologation	❑ Homologation → Décision d'homologation ❑ Accompagnement ❑ Mise en œuvre des meilleures pratiques	❑ Homologation → Décision d'homologation ❑ Mise en œuvre des règles ❑ Tenue à jour de la gestion des risques → Dossier de sécurité enrichi	❑ Homologation → Décision d'homologation ❑ Mise en œuvre des règles ❑ Tenue à jour de la gestion des risques → Dossier de sécurité enrichi ❑ Alimentation des TDBSSI → TDBSSI	❑ Homologation → Décision d'homologation ❑ Mise en œuvre des règles ❑ Tenue à jour de la gestion des risques → Dossier de sécurité enrichi ❑ Alimentation des TDBSSI ❑ Révision des documents d'application et TDBSSI → TDBSSI

5 Conclusion

GISSIP permet une intégration de la SSI structurée, complète et adaptée aux enjeux de sécurité de chaque SI. Cette méthode aide en effet les acteurs du SI à déterminer les actions SSI à entreprendre et les documents à produire tout au long du cycle de vie des systèmes, et ce, en fonction du niveau de maturité SSI le plus adéquat.

Comme toute approche méthodologique généraliste, il convient évidemment de la considérer avec souplesse afin de l'appliquer de manière cohérente avec les pratiques et outils de chaque organisme.

Il convient également de réévaluer régulièrement les enjeux de sécurité, et donc le niveau de maturité SSI adéquat, dans le but de vérifier que les actions entreprises apportent bien le niveau de confiance le plus approprié.

Annexes

Analogies avec l'homologation en France et à l'OTAN

Le tableau suivant présente les analogies qu'il est possible d'établir entre les livrables de la démarche générique de GISSIP et ceux des démarches spécifiques d'homologation en France ([IGI 900], [II 920], [IGI 1300]) et à l'OTAN ([OTAN-1014], [OTAN-1015], [OTAN-1021]) :

GISSIP (approche générique)	Homologation France	Homologation OTAN
Note d'orientation SSI	❑ Note d'orientation SSI	❑ Processus structuré validé par l'homologation de sécurité du SI ❑ Saisine de l'Autorité nationale de sécurité (ANS)
Note de stratégie de sécurité	❑ Note de stratégie de sécurité	❑ Note de stratégie de sécurité
FEROS	❑ FEROS	❑ *System-specific Security Requirement Statement* (SSRS)
Liste de meilleures pratiques	❑ Aucun	❑ Aucun
PSSI	❑ PSSI ❑ Protocole d'accord ❑ PSSI communautaire ❑ PSSI d'interconnexion	❑ SSRS ❑ *Community Security Requirement Statement* (CSRS) ❑ Accords de sécurité ❑ *System Interconnection Security Requirement Statement* (SISRS)
Cible de sécurité	❑ Cible de sécurité système ❑ Plan de sécurité système selon l'avancement du projet	❑ SSRS
Documents d'application de la PSSI	❑ PSSI du système ❑ Procédures d'exploitation de sécurité (PES)	❑ *Security OPerating ProcedureS* (SecOPs)
Documentation relative aux tests	❑ Plan Test générique	❑ Plan Test approuvé ❑ Rapport d'inspection de sécurité
Documentation relative aux évaluations	❑ Cible de sécurité produit	❑ *System-specific Electronic Information Security Requirement Statement* (SEISRS)
Décision d'homologation	❑ Décision d'homologation	❑ Proposition de *Statement of Compliance* (SoC) d'homologation
TDBSSI	❑ Aucun	❑ Aucun

Références bibliographiques

[Chartier 1999] Chartier-Kastler C., *Précis de conduite de projet informatique*, Les Éditions d'Organisation, Collection Ingénierie des Systèmes d'Information (1999).

[EBIOS] *Expression des Besoins et Identification des Objectifs de Sécurité (EBIOS)* – SGDN/DSCSSI (2004).

[FEROS] *Fiche d'Expression Rationnelle des Objectifs de Sécurité des systèmes d'information (FEROS)* – SGDN/ SCSSI (1991).

[IGI 1300] *Instruction générale interministérielle sur la protection du secret de la défense nationale* – N°1300 / SGDN / PSE / SSD (2003).

[IGI 900] *La sécurité des systèmes d'information qui font l'objet d'une classification de défense pour eux-mêmes ou pour les informations traitées* – SGDN et DISSI (1993).

[II 920] *Instruction interministérielle relative aux systèmes traitant des informations classifiées de défense de niveau confidentiel défense* – N°II 920 / SGDN / DCSSI (2005).

[ISO 15408] *Critères Communs pour l'évaluation de la sécurité des Technologies de l'Information*, – International Organization for Standardization (ISO) – version 2.0 (1998).

[ISO 21827] *Systems Security Engineering – Capability Maturity Model* - International Organization for Standardization (ISO) (2001).

[ISO Guide 73] *Management du risque – Vocabulaire – Principes directeurs pour l'utilisation dans les normes* – International Organization for Standardization (ISO) (2002).

[Kettani 1998] Kettani, Mignet, Paré & Rosenthal-Sabroux, *De MERISE à UML*, Eyrolles (1998).

[OCDE] *Lignes directrices de l'OCDE régissant la sécurité des systèmes et réseaux d'information : vers une culture de la sécurité* – Organisation de coopération et de développement économiques (OCDE) (2002).

[OTAN-1014] *Lignes directrices concernant la structure et le contenu de la procédure d'exploitation de sécurité (SecOp) des systèmes d'information et de communication (SIC)* – AC/35-D/1014 – Comité de sécurité de l'OTAN (2000).

[OTAN-1015] *Lignes directrices pour l'établissement des énoncés des impératifs de sécurité* – AC/35-D/1015 – Comité de sécurité de l'OTAN (1996).

[OTAN-1021] *Lignes directrices pour l'approbation ou l'homologation de sécurité des systèmes d'information et de communication (SIC)* – AC/35-D/1021 – Comité de sécurité de l'OTAN (2003).

[PMI 2000] PMI (Project Management Institute), *Management de projet, un référentiel de connaissances*, AFNOR (2000).

[PSSI] *Guide d'élaboration de politique de sécurité de système d'information* – SGDN/DCSSI (2004).

[2] D'après par exemple [Chartier 1999], [Kettani 1998], [PMI 2000].

[REC 901] *Recommandation pour la protection des systèmes d'information traitant des informations sensibles non classifiées de défense* – SGDN et DISSI (1994).

[TDBSSI] *Guide d'élaboration de tableaux de bord de sécurité de système d'information* – SGDN/DCSSI (2004).

Glossaire[3]

La traduction en anglais des termes du glossaire figure entre parenthèses pour chaque terme. Le texte souligné dans les définitions correspond aux concepts définis dans le présent document.

Besoin de sécurité (sensitivity)	Définition précise et non ambiguë des niveaux correspondant aux critères de sécurité (disponibilité, confidentialité, intégrité…) qu'il convient d'assurer à un élément essentiel.
Exigence de sécurité (security requirement)	Spécification fonctionnelle ou d'assurance sur le système d'information ou sur l'environnement de celui-ci, portant sur les mécanismes de sécurité à mettre en œuvre et couvrant un ou plusieurs objectifs de sécurité.
Gestion du risque (risk management)	Activités coordonnées visant à diriger et piloter un organisme vis-à-vis du risque. La gestion du risque inclut typiquement l'appréciation du risque, le traitement du risque, l'acceptation du risque et la communication relative au risque. [ISO Guide 73]
Menace (threat)	Attaque possible d'un élément menaçant sur des biens.
Mesure de sécurité (security measure)	Moyen destiné à améliorer la sécurité, spécifié par une exigence de sécurité et à mettre en œuvre pour la satisfaire. Il peut s'agir de mesures de prévision ou de préparation, de dissuasion, de protection, de détection, de confinement, de "lutte", de récupération, de restauration, de compensation…
Objectif de sécurité (security objective)	Expression de l'intention de contrer des menaces ou des risques identifiés (selon le contexte) et/ou de satisfaire à des politiques de sécurité organisationnelles et à des hypothèses ; un objectif peut porter sur le système-cible, sur son environnement de développement ou sur son environnement opérationnel.
Politique de sécurité de système d'information (information systems security policy)	Ensemble, formalisé dans un document applicable, des éléments stratégiques, des directives, procédures, codes de conduite, règles organisationnelles et techniques, ayant pour objectif la protection du (des) système(s) d'information de l'organisme. [PSSI]
Règle de sécurité (organisational security policy)	Règle, procédure, code de conduite ou ligne directrice de sécurité qu'une organisation impose pour son fonctionnement. [ISO 15408]
Risque (risk)	Combinaison d'une menace et des pertes qu'elle peut engendrer, c'est-à-dire : de l'opportunité de l'exploitation d'une ou plusieurs vulnérabilités d'une ou plusieurs entités par un élément menaçant employant une méthode d'attaque ; et de l'impact sur les éléments essentiels et sur l'organisme.
Risque résiduel (residual risk)	Risque subsistant après le traitement du risque. [ISO Guide 73]
Sécurité des systèmes d'information (SSI) (information security)	Protection des systèmes d'information, et en particulier des éléments essentiels, contre toute atteinte des critères de sécurité non autorisée, qu'elle soit accidentelle ou délibérée.
Système d'information (SI) (information system)	Ensemble d'entités organisé pour accomplir des fonctions de traitement d'information.

[3] D'après la méthode [EBIOS]

Acronymes

BCS	Bureau Conseil en Sécurité des systèmes d'information
CCTP	Cahier des Clauses Techniques Particulières
DCSSI	Direction Centrale de la Sécurité des Systèmes d'Information
EBIOS	Expression des Besoins et Identification des Objectifs de Sécurité
FEROS	Fiche d'Expression Rationnelle des Objectifs de Sécurité des SI
GISSIP	Guide d'Intégration de la Sécurité des Systèmes d'Information dans les Projets
MOA	Maîtrise d'OuvrAge
MOE	Maîtrise d'Œuvre
PES	Procédures d'Exploitation de Sécurité
PP	(*Protection Profile*) – Profil de protection
PSSI	Politique de Sécurité des Systèmes d'Information
ROI	(*Return On Investment*) – Retour sur investissement
RSSI	Responsable de la Sécurité des Systèmes d'Information
SDO	Sous-Direction des Opérations
SGDN	Secrétariat Général de la Défense Nationale
SI	Système d'Information
SSI	Sécurité des Systèmes d'Information
TDBSSI	Tableau De Bord de Sécurité des Systèmes d'Information

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