



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

Guide pour l'élaboration d'une politique de sécurité de système d'information

PSSI

SECTION 2 MÉTHODOLOGIE

Version du 3 mars 2004

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

Version	Objet de la modification	Statut
15/09/1994 (1.1)	Publication du guide d'élaboration de politique de sécurité interne (PSI).	Validé
2002	Révision globale : <ul style="list-style-type: none">- actualisation des références,- création d'une méthodologie,- enrichissement et reclassement des principes de sécurité,- séparation en 3 sections (méthodologie, principes de sécurité et compléments).	Draft
2003	Restructuration, remise en forme, amélioration de la méthode, mise en cohérence avec les outils méthodologiques et meilleures pratiques de la DCSSI suite à une consultation d'experts internes.	Prétest
23/12/2003	Séparation en 4 sections (introduction, méthodologie, principes de sécurité et références SSI) et améliorations diverses suite à une consultation d'experts externes (notamment le Club EBIOS) et à plusieurs mises en pratique (ministère de la Défense, CNRS, Direction des Journaux Officiels...).	Prétest pour validation
03/03/2004	Publication du guide pour l'élaboration d'une politique de sécurité de système d'information (PSSI)	Validé

Table des matières

SECTION 1 – INTRODUCTION (document séparé)

SECTION 2 – MÉTHODOLOGIE

INTRODUCTION	5
OBJET DU DOCUMENT	5
1 INTRODUCTION À LA MÉTHODE	6
1.1 PRÉSENTATION GÉNÉRALE DE LA DÉMARCHE	6
1.2 PRINCIPAUX RÉSULTATS DE LA MÉTHODE	6
1.3 LES SUITES D'UNE PSSI.....	7
2 DÉMARCHE D'ÉLABORATION D'UNE PSSI	8
2.1 CONVENTIONS D'ÉCRITURE	8
2.2 PHASE 0 : PRÉALABLES	9
2.2.1 <i>Tâche 1 : organisation projet</i>	10
2.2.2 <i>Tâche 2 : constitution du référentiel</i>	11
2.3 PHASE 1 : ÉLABORATION DES ÉLÉMENTS STRATÉGIQUES.....	12
2.3.1 <i>Tâche 1 : définition du périmètre de la PSSI</i>	13
2.3.2 <i>Tâche 2 : détermination des enjeux et orientations stratégiques</i>	14
2.3.3 <i>Tâche 3 : prise en compte des aspects légaux et réglementaires</i>	15
2.3.4 <i>Tâche 4 : élaboration d'une échelle de besoins</i>	16
2.3.5 <i>Tâche 5 : expression des besoins de sécurité</i>	18
2.3.6 <i>Tâche 6 : identification des origines des menaces</i>	19
2.4 PHASE 2 : SÉLECTION DES PRINCIPES ET RÉDACTION DES RÈGLES	20
2.4.1 <i>Tâche 1 : choix des principes de sécurité</i>	21
2.4.2 <i>Tâche 2 : élaboration des règles de sécurité</i>	22
2.4.3 <i>Tâche 3 : élaboration des notes de synthèse</i>	23
2.5 PHASE 3 : FINALISATION	24
2.5.1 <i>Tâche 1 : finalisation et validation de la PSSI</i>	25
2.5.2 <i>Tâche 2 : élaboration et validation du plan d'action</i>	26
3 PLAN-TYPE D'UNE PSSI	27
FORMULAIRE DE RECUEIL DE COMMENTAIRES	28

SECTION 3 – PRINCIPES DE SÉCURITÉ (document séparé)

SECTION 4 – RÉFÉRENCES SSI (document séparé)

Introduction

Le guide PSSI est décomposé en quatre sections :

- l'introduction permet de situer la place de la PSSI dans le référentiel normatif de la SSI au sein de l'organisme et de préciser les bases de légitimité sur lesquelles elle s'appuie ;
- la méthodologie (ce document) présente, de façon détaillée, la conduite de projet d'élaboration d'une PSSI, ainsi que des recommandations pour la construction des règles de sécurité ;
- le référentiel de principes de sécurité ;
- une liste de documents de références de la SSI (critères d'évaluation, textes législatifs, normes, codes d'éthiques, notes complémentaires...).

L'attention du lecteur est attirée sur le fait que les sections composant le guide PSSI seront mises à jour indépendamment.

Un formulaire de recueil de commentaires figure en annexe de chaque guide afin de renvoyer des propositions et remarques à la DCSSI.

Objet du document

Cette section présente la méthode d'élaboration de politiques de sécurité des systèmes d'information (PSSI).

La démarche d'élaboration de PSSI se déroule en 4 phases successives :

- **Phase 0** : préalables
 - o Tâche 1 : organisation projet
 - o Tâche 2 : constitution du référentiel
- **Phase 1** : élaboration des éléments stratégiques
 - o Tâche 1 : définition du périmètre de la PSSI
 - o Tâche 2 : détermination des enjeux et orientations stratégiques
 - o Tâche 3 : prise en compte des aspects légaux et réglementaires
 - o Tâche 4 : élaboration d'une échelle de besoins
 - o Tâche 5 : expression des besoins de sécurité
 - o Tâche 6 : identification des origines des menaces
- **Phase 2** : sélection des principes et rédaction des règles
 - o Tâche 1 : choix des principes de sécurité
 - o Tâche 2 : élaboration des règles de sécurité
 - o Tâche 3 : élaboration des notes de synthèse
- **Phase 3** : finalisation
 - o Tâche 1 : finalisation et validation de la PSSI
 - o Tâche 2 : élaboration et validation du plan d'action

1 Introduction à la méthode

1.1 Présentation générale de la démarche

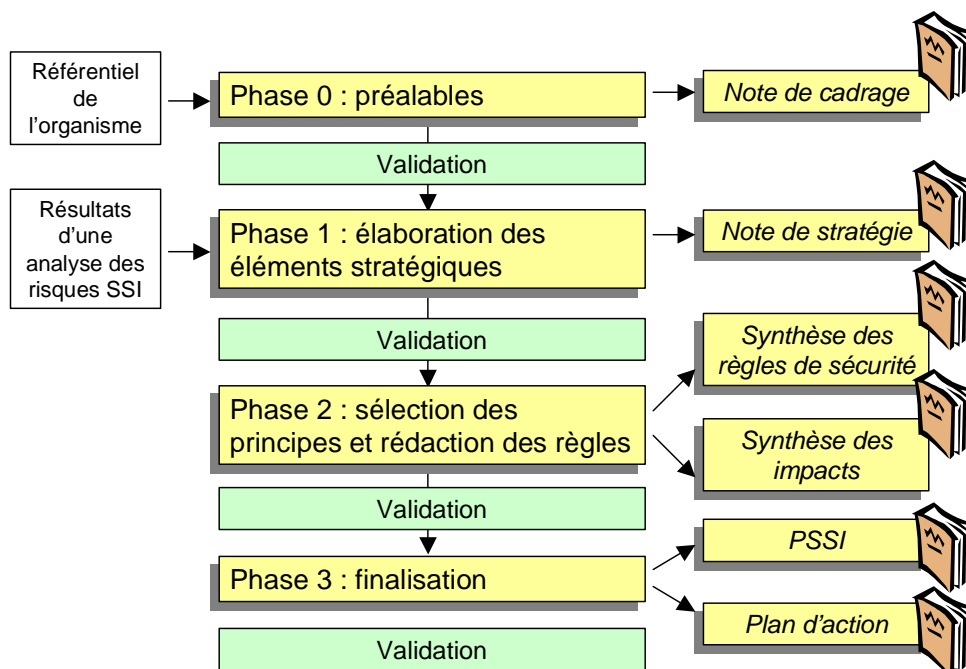
La démarche, qui est menée sous la forme d'un "projet PSSI", se base sur le référentiel de l'organisme et une analyse des risques SSI.

Le référentiel SSI de l'organisme (schéma directeur, meilleures pratiques, directives internes...) et une analyse des risques préalables fournissent en effet les éléments permettant d'effectuer et de justifier les choix, de légitimer l'action et de garantir la cohérence avec le contexte particulier de l'organisme.

L'objectif de la méthode consiste à construire un document de politique comprenant des éléments stratégiques et des règles de sécurité pour un organisme ou un système d'information.

La validation successive des différentes phases vise à faciliter l'implication de la Direction générale et l'adhésion de tous les intervenants.

La figure suivante présente la démarche en 4 phases :



1.2 Principaux résultats de la méthode

L'élaboration de la PSSI doit permettre de :

- (1) Disposer d'un cadre de référence et de cohérence pour l'ensemble des activités et des acteurs de l'organisme.

Ce cadre de sécurité doit notamment permettre la mise en évidence des objectifs, obligations et engagements de l'organisme vis-à-vis de ses partenaires, clients et sous-traitants, ainsi que les principes de sécurité régissant la protection de son propre patrimoine.

Ce cadre fondamental et fédérateur doit exprimer les responsabilités de l'ensemble des acteurs, ainsi que les principes et règles de sécurité minimaux à respecter pour l'ensemble des activités et des systèmes.

Il doit offrir les directives nécessaires, notamment pour tout choix technique mais aussi organisationnel ou contractuel, en matière de sécurité, et permet d'assurer la cohérence et la pérennité des actions de sécurité.

(2) Constituer un document général diffusable

La Politique de Sécurité des Systèmes d'Information doit être connue de l'ensemble des acteurs internes, ainsi que, le cas échéant, de l'ensemble des personnes accédant au SI de l'organisme (prestataires, sous-traitants, stagiaires).

Le document doit être largement diffusé, éventuellement sous une forme simplifiée et didactique (le langage utilisé doit être approprié aux destinataires), à l'ensemble du personnel. Cette diffusion sera, le cas échéant, accompagnée d'une sensibilisation de l'ensemble du personnel portant sur le rappel des principes, de l'organisation et des règles de sécurité.

Le plan type d'une PSSI figure en partie 3 de ce document. D'une manière générale, il doit évoquer les points suivants :

- pourquoi protéger et susciter la confiance : enjeux, aspects réglementaires, menaces ;
- que protéger : biens à protéger et échelle de besoins ;
- qui protège : organisation, responsabilités et gestion de la SSI ;
- comment protéger : ensemble cohérent et opérationnel de règles de sécurité ;
- quand protéger : considération de l'ensemble du cycle de vie.

La PSSI doit être complétée par un plan d'action pour assurer sa mise en œuvre. Il comprendra deux principaux volets :

- des actions de type méthodologique, organisationnelle ou procédurale, applicable à l'ensemble de l'organisme participant au périmètre de l'étude ;
- des actions de type technique, concernant les éléments fédérateurs du système d'information.

Ces actions pourront être accompagnées de recommandations concernant les outils et méthodes de mise en œuvre.

Ce plan d'action est destiné à "vivre". Il doit être tenu à jour et ses priorités doivent être revues en fonction de l'évolution des services offerts par le SI, des budgets attribués, de l'organisation, des missions, etc...

1.3 Les suites d'une PSSI

Les suites à donner à l'élaboration d'une PSSI s'articulent autour de quatre axes fondamentaux.

- (1) Assurer une déclinaison opérationnelle des règles de la PSSI, notamment sous la forme de procédures, applicables directement aux différents systèmes et applications.
- (2) Constituer une entité de suivi et de pilotage du plan d'action prioritaire défini à l'issue de cette démarche. La vision dynamique, nécessaire pour prendre en compte la sécurité dans un contexte mouvant, peut conduire à remettre en question des priorités du plan d'action et donc à réitérer au moins la fin de la démarche.
- (3) L'audit de la PSSI, notamment construit autour de contrôles réguliers à plusieurs niveaux de l'application opérationnelle ou à l'aide de tableaux de bord SSI, est un élément fondamental pour assurer l'efficacité de la couverture des risques jugés inacceptables. Ainsi, les résultats obtenus à l'issue de ces audits (organisationnels et techniques) pourront, le cas échéant, demander une révision des règles de sécurité.
- (4) Enfin, la mise en place d'une organisation d'alerte et de veille technologique est nécessaire à assurer la maintenance du niveau de sécurité et son efficacité dans le temps.

2 Démarche d'élaboration d'une PSSI

Le déroulement de la méthode exige principalement :


- une implication forte de l'encadrement au plus haut niveau ;
- de disposer de moyens humains significatifs, non seulement pour le chef de projet responsable du projet mais aussi pour l'ensemble des acteurs impliqués (techniques, fonctionnels et décisionnels) ;
- une implication active et une motivation réelle de l'ensemble des acteurs, notamment celle des responsables techniques et fonctionnels ;
- la prise en compte de moyens financiers et humains pour la mise en œuvre future du plan d'action produit par l'étude ;
- la prise en compte des pratiques et usages du système d'information par les différents profils d'acteur pour éviter de révolutionner les méthodes de travail qui ont, dans la plupart des cas, fait leur preuve.

Il est précisé en outre que ce type de démarche n'a de sens que si :

- elle est menée de façon consensuelle avec des points de validation successifs réguliers ;
- les éléments étudiés le sont dans leur globalité, c'est à dire que l'étude doit s'intéresser, pour un système donné, à l'ensemble des risques et à l'ensemble des moyens de sécurité à mettre en œuvre tous les aspects des systèmes et de leur environnement tant physique qu'organisationnel ;
- elle est réalisée par un tiers (prestation d'assistance) qui, de par sa position de neutralité, pourra faire émerger les éléments nécessaires à l'élaboration d'une PSSI en franchissant plus facilement les barrières interpersonnelles.

2.1 Conventions d'écriture

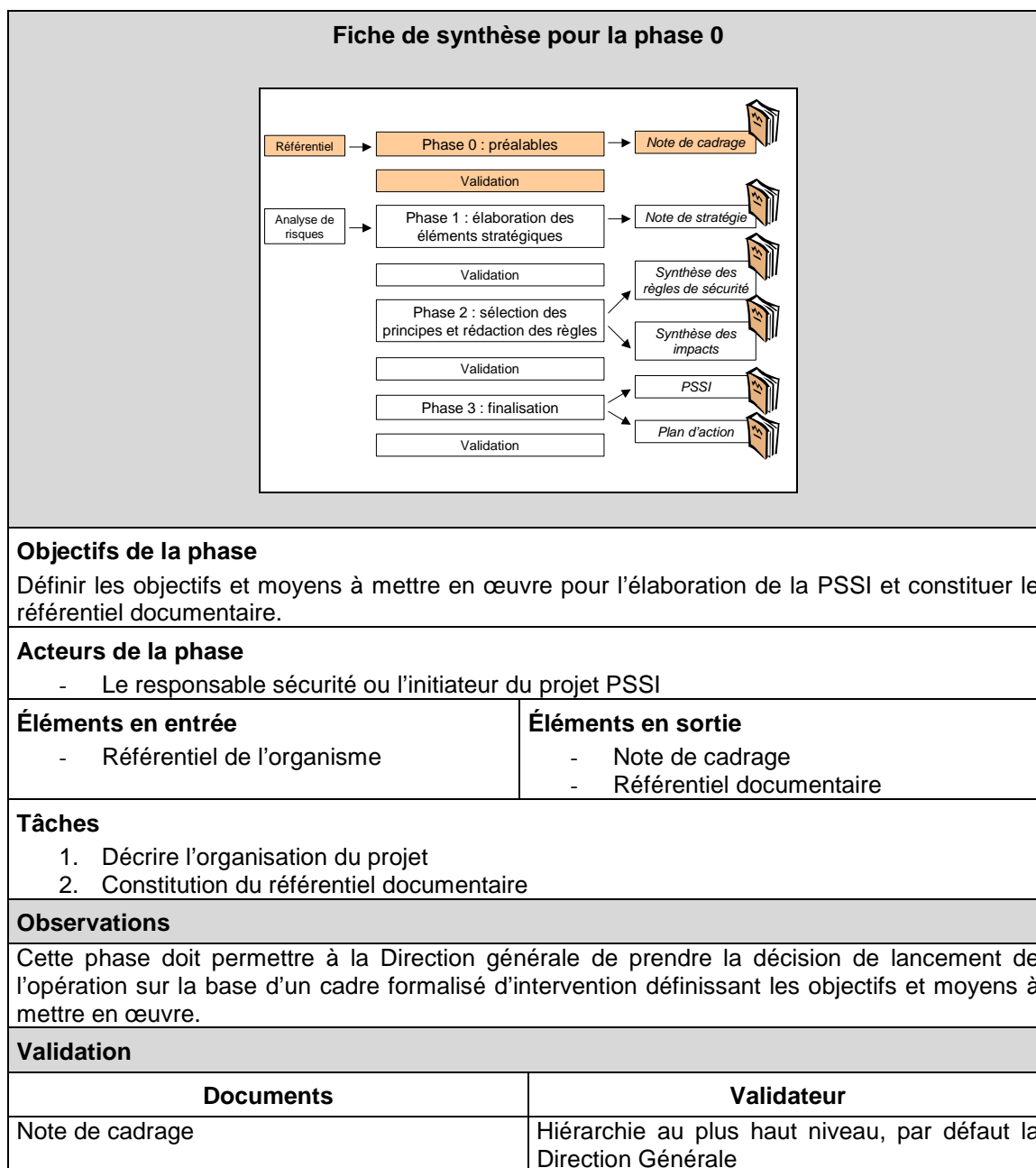
Les symboles suivants sont utilisés dans la suite du document :

 : *Conseil pratique*

 : *Écueil et recommandation*

2.2 Phase 0 : préalables

Cette phase préliminaire doit permettre la présentation du projet au niveau de la Direction générale et de faire valider ainsi ses objectifs et les moyens qu'il convient d'y consacrer.



2.2.1 Tâche 1 : organisation projet

Objectif

Cette tâche consiste à définir l'organisation du "projet PSSI" afin d'élaborer le cadre de réalisation.

Démarche

L'élaboration de la PSSI doit être conduite comme un projet à part entière et notamment il faut :

- nommer un chef de projet, missionné au plus haut niveau ;
- constituer un comité de pilotage, composé des principaux représentants des maîtrises d'ouvrage et des maîtrises d'œuvre, animé par le RSSI. Cette structure de pilotage pourra par la suite devenir le comité de sécurité chargé notamment de maintenir l'efficacité et la cohérence du document ;
- constituer un groupe d'experts, compétents pour traiter des thèmes à développer dans le périmètre de la PSSI (experts juridiques, experts en organisation de la SSI en entreprise, experts techniques des systèmes, architecte réseau...);
- attribuer un budget ;
- formaliser des objectifs détaillés ;
- établir un calendrier.

Une étape préliminaire de gestion de projet doit être conduite pour déterminer l'ensemble des éléments nécessaires au déroulement du projet.

Cette étape préliminaire comporte trois volets complémentaires :

- la description macroscopique de l'organisation du projet, des systèmes d'information en place, et des domaines d'application (cible du projet) ;
- la formalisation et la validation du cadre complet d'intervention (méthode précise, acteurs impliqués, calendrier, résultats attendus, champ d'application de la démarche...);
- la rédaction d'une note de cadrage du projet, reprenant l'ensemble des éléments à analyser et décrivant les objectifs et la cible du projet, validée par la Direction générale et diffusée.



Conseil pratique :

Que la PSSI soit globale ou qu'elle concerne une application particulière, le cadre doit être défini clairement dès le départ. La composition de l'organisation du projet et du budget (temps, argent, ressources) en dépendent fortement.



Attention :

L'aspect indispensable de cette tâche est de constituer un comité de pilotage dont les membres sont suffisamment représentatifs de la maîtrise d'ouvrage et légitimes pour prendre les décisions.

2.2.2 Tâche 2 : constitution du référentiel

Objectif

Cette tâche consiste à identifier le référentiel documentaire de l'organisme (SI, SSI, aspects déontologiques et contractuels) qui servira de base à la suite de la démarche.

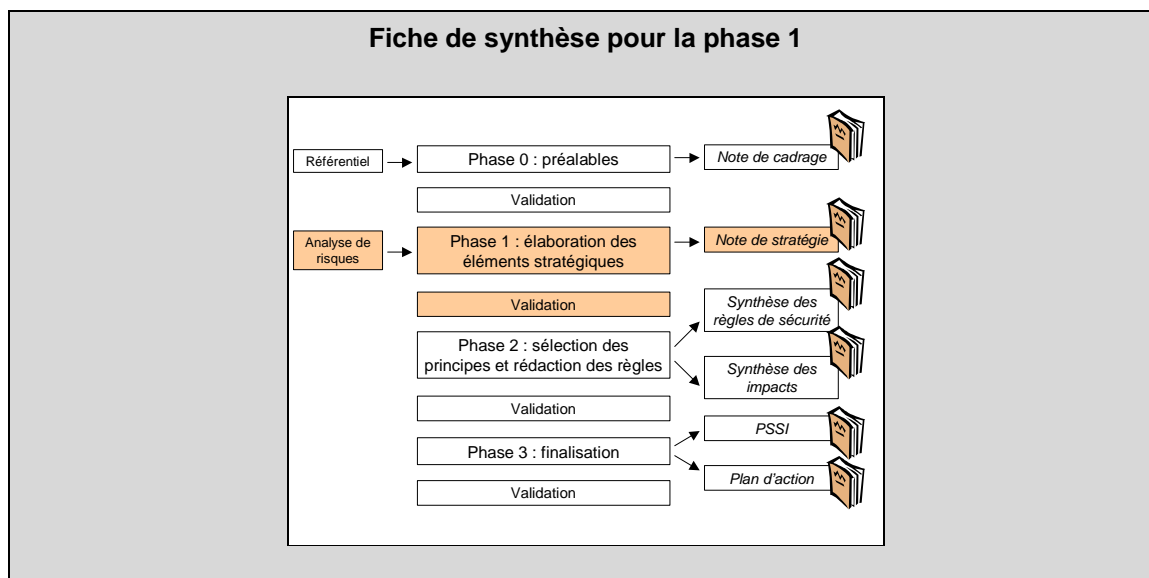
Démarche

La réalisation d'une politique de sécurité doit se construire de façon adaptée au contexte particulier de chaque organisme. Ce contexte diffère d'un organisme à un autre et doit donc pouvoir être appréhendé le plus tôt possible. Pour y parvenir, le groupe de projet doit constituer dès le début une base documentaire regroupant :

- aspects légaux et réglementaires :
 - o les textes législatifs majeurs, qui sont décrits en annexe, dont la loi informatique et liberté, la loi sur la protection des droits d'auteur, la loi relative à la fraude informatique, la loi sur le secret des communications, les lois sur la cryptologie ;
 - o les textes et recommandations énoncées au plan national et international dont une liste de références se trouve en annexe ;
 - o le règlement intérieur, qui peut également contenir des exigences concernant le système d'information ;
 - o la préservation des intérêts vitaux de l'État sur le plan de la protection des informations sensibles relevant ou non du secret de défense,
 - o le droit d'auteur ;
 - o la propriété intellectuelle et du copyright ;
 - o l'utilisation de moyens cryptographiques ;
 - o la protection des consommateurs ;
 - o obligations réglementaires spécifiques à l'organisme concerné...
- grands principes d'éthique :
 - o au plan national, la protection de la vie privée ;
 - o les clauses particulières dans les contrats régissant les relations de l'organisme avec ses partenaires et/ou clients ;
 - o les codes éthiques des métiers des technologies de l'information dont une liste des références est proposée en annexe...
- obligations contractuelles auxquelles l'organisme s'est engagé vis à vis de ses clients ou partenaires spécifiques :
 - o contrat de coopération ou de partenariat avec d'autres organismes ;
 - o contrat de prestation de service à d'autres organismes ;
 - o conditions de garantie applicables aux produits ou services proposés ;
 - o conventions bilatérales (comme par exemple des conventions de preuve)...
- obligations contractuelles des prestataires ou partenaires,
- le référentiel de sécurité interne :
 - o schéma directeur informatique et SSI ;
 - o analyses de risques ;
 - o résultats d'audits de sécurité ...
- le référentiel du ou des systèmes d'information.

Tous ces éléments sont fournis à titre d'exemple et la liste ne prétend pas à l'exhaustivité, il conviendra de l'adapter en fonction du domaine de chaque organisme.

2.3 Phase 1 : élaboration des éléments stratégiques



Objectifs de la phase

Cette phase, dont les résultats et conclusions doivent impérativement être validés par la Direction Générale, consiste à déterminer les axes stratégiques et les premières grandes orientations à partir desquelles sera déclinée la PSSI.

Pour cela, elle doit obligatoirement identifier et prendre en compte le périmètre d'étude, le contexte, les enjeux et orientations stratégiques, le référentiel réglementaire, l'échelle de besoins, les besoins de sécurité des biens à protéger et les origines des menaces afin d'aboutir à une note de stratégie validée par la Direction fixant les grandes orientations de la SSI.

Acteurs de la phase

- Chef de projet
- Représentants de la maîtrise d'ouvrage
- Direction Générale
- Responsable juridique

Éléments en entrée

- Référentiel documentaire

Éléments en sortie

- Note de stratégie de sécurité

Tâches

1. Délimitation du périmètre
2. Identification des enjeux et orientations stratégiques
3. Recensement des lois et règlements applicables
4. Définition d'une échelle de besoins en termes de disponibilité, intégrité, confidentialité et éventuellement d'autres critères de sécurité
5. Expression des besoins de sécurité des biens à protéger
6. Identification des origines des menaces pesant sur l'organisme ou le système étudié (et éventuellement des principaux risques et objectifs de sécurité)

Observations

Il convient d'insister sur l'importance capitale de cette phase et sur la nécessité d'une implication forte de la Direction Générale tant lors de l'identification des besoins et menaces que lors de la validation de la cible et des principaux objectifs à atteindre.

Validation

Document	Validateur
Note de stratégie de sécurité	Comité de pilotage puis Direction générale

2.3.1 Tâche 1 : définition du périmètre de la PSSI

Objectif

Cette tâche consiste à décrire les **domaines d'activités** à couvrir et à affiner le périmètre, notamment les échanges entre les domaines et l'extérieur du périmètre.

Le champ d'application de la politique de sécurité du système d'information peut être tout système d'information de l'organisme ou le système d'information dans sa globalité, qu'il soit existant ou à développer, et en prenant en compte l'ensemble des thèmes de la sécurité (logique, physique, aspects humains, réglementaires...).

Des sous-périmètres demandant un traitement spécifique peuvent être identifiés lors de cette tâche.



Conseil pratique :

La réalisation rigoureuse de cette étape est fondamentale. Le résultat doit être validé par la hiérarchie au plus haut niveau. Ce résultat conditionne notamment la détermination des biens à protéger et, par voie de conséquence, le choix des personnes à impliquer dans l'étude.

Démarche

La démarche consiste en premier lieu à formaliser une vision globale du système d'information concerné.

À partir de cette représentation, il est nécessaire de :

- lister l'ensemble des domaines d'activités jouant un rôle dans le système d'information de l'organisme ; cette liste doit inclure les métiers de l'organisme et les services internes de production, de gestion, de support (réseau d'entreprise, info-gérance...) ;
- sélectionner et décrire les domaines d'activités essentiels au fonctionnement de l'organisme, ainsi que leurs interactions et éventuellement les aspects sécurité (dont les éléments sont issus du référentiel de sécurité identifié dans la phase préalable) ;
- identifier ceux qui constituent le périmètre de la PSSI et ceux qui en sont exclus ;
- dans la mesure du possible, les **fonctions** et **informations** de chaque domaine d'activité sont identifiées.

Le périmètre précis sera alors exprimé clairement dans la PSSI.



Attention :

Dans le cas d'une PSSI globale, on ne pourra pas toujours étudier tous les systèmes d'information. On ne pourra même pas traiter toutes les fonctions ou tous les processus. S'il faut en faire une liste assez complète, il faudra aussi sélectionner un échantillon représentatif sur lequel l'étude portera. Les systèmes d'information non étudiés pourront hériter des mesures prises au profit des autres.



Conseils pratiques :

Obtenir une modélisation conceptuelle du système permettra de clarifier la situation et de faciliter la communication et la validation au sujet du périmètre.

Il est conseillé de sélectionner des domaines d'activités pour lesquels l'application de règles de sécurité pourra être imposée par un responsable unique.

2.3.2 Tâche 2 : détermination des enjeux et orientations stratégiques

Objectif

Cette tâche consiste à présenter les **enjeux** et **orientations stratégiques** liés au périmètre de la PSSI. Elle permet aussi d'identifier les **contraintes** générales pesant sur l'organisme.

Elle découle d'une connaissance des éléments stratégiques de l'organisme : contexte métier, missions, patrimoine et valeurs de l'organisme.

Démarche

La définition des enjeux et orientations stratégiques, dont les éléments sont majoritairement issus du schéma directeur, doit prendre en compte les éléments suivants :

- les scénarios d'évolution du système d'information ;
- la contribution du système d'information à long terme ;
- la contribution du système d'information à la qualité du service rendu ;
- la satisfaction des contraintes externes ;
- la rentabilité économique du projet ;
- les contraintes (techniques, financières, d'environnement...) et exigences (techniques ou organisationnelles) de l'organisme et du système d'information.

La démarche consiste à identifier tous ces éléments afin de les rationaliser sous la forme d'une synthèse qui figurera dans la PSSI.



Conseils pratiques :

L'exploitation d'un schéma directeur existant facilite la réalisation de cette tâche.

Les résultats d'une analyse des risques SSI appliquée au périmètre délimité pour la PSSI permettent généralement d'identifier les enjeux et orientations stratégiques de l'organisme.

2.3.3 Tâche 3 : prise en compte des aspects légaux et réglementaires

Objectif

Cette tâche consiste à présenter l'ensemble du **référentiel légal, réglementaire et contractuel** applicable au périmètre de la PSSI.

Démarche

Le but de cette tâche est de disposer d'une liste précise des obligations et donc des textes de lois et règlements applicables, de l'ensemble des clauses contractuelles, ainsi que les rôles et responsabilités qui peuvent impacter la sécurité.

D'une part, il est nécessaire de prendre en compte l'ensemble des éléments issus majoritairement du référentiel identifié dans la phase préalable :

- aspects légaux et réglementaires ;
- grands principes d'éthique ;
- obligations contractuelles ;
- obligations contractuelles des prestataires ou partenaires ayant un impact sur le périmètre de la PSSI.

D'autre part, cette tâche doit aussi mettre en évidence les rôles et responsabilités liés à la sécurité des systèmes d'information.

L'ensemble de ces éléments fera l'objet d'une synthèse dans la PSSI.



Conseils pratiques

La prise en compte des obligations contractuelles et de leur traduction en matière d'exigences voire de règles, d'avenant à des contrats ou même de solutions est transverse à tous les domaines.

Il est difficile, mais fondamental, de s'assurer que l'ensemble des engagements contractuels est connu et qu'une déclinaison (exigences et règles) ad-hoc en est faite.

Seule une synthèse du résultat de cette tâche sera incluse dans la politique de sécurité du système d'information. Néanmoins, elle pourra constituer une annexe utile.

Les résultats d'une analyse des risques SSI appliquée au périmètre délimité pour la PSSI permettent généralement d'identifier le référentiel applicable.

Au besoin, il est conseillé de faire appel à une prestation juridique pour donner l'inventaire des exigences réglementaires applicables.

2.3.4 Tâche 4 : élaboration d'une échelle de besoins

Objectif

Cette tâche consiste à définir une échelle de mesure utile à l'expression des besoins de sécurité pour les domaines d'activités identifiés dans la PSSI ou les fonctions et informations identifiées dans les études de sécurité dans le périmètre de la PSSI.

Les mesures de sécurité étant souvent coûteuses et contraignantes, leur mise en œuvre doit être adaptée à de réels enjeux pour l'organisme. Elle doit donc obéir à un principe de gradation des moyens, qui consiste à protéger tous les domaines d'activités selon leur besoins de sécurité et les menaces qui peuvent les affecter. Il est ainsi possible d'adapter les mesures de sécurité aux enjeux réels, tout en optimisant leur efficacité et les coûts inhérents.



Attention :

La définition d'une classification ne permet pas de résoudre l'ensemble des règles de sécurité, elle fixe seulement des obligations et est un indicateur pour juger de leur besoins de sécurité.

Démarche

Dans le cas où une classification existerait déjà dans l'organisme, celle-ci sert de base à la réflexion et peut même être employée directement pour définir l'échelle de besoins. La démarche présentée ici permet en effet d'élaborer une échelle objective qui permet d'affecter une valeur explicite aux biens à protéger.

Tout d'abord, il est nécessaire de sélectionner les **critères de sécurité** à prendre en compte. Les critères de sécurité couramment utilisés sont la disponibilité, l'intégrité et la confidentialité, mais il peut être pertinent d'en ajouter d'autres tels que la preuve, le contrôle, l'anonymat, la fiabilité... L'échelle de besoins sera déterminée en fonction de ces critères de sécurité.



Conseils pratiques :

Les résultats d'une analyse des risques SSI appliquée au périmètre de la PSSI permettent généralement d'élaborer l'échelle de besoins. La définition d'une classification générale sur le plan de la disponibilité et de l'intégrité n'est pas toujours pertinente. Dans certains contextes, où ces objectifs concernent peu d'informations ou de fonctions, il est parfois plus simple de définir des règles au cas par cas.

Une gradation de ces critères de sécurité peut alors être élaborée. Pour cela, une **pondération** et des **valeurs de référence** doivent être déterminées pour chacun des critères de sécurité sélectionnés.

Par exemple, une échelle pour la confidentialité pourrait être la suivante :

- 0 = public,
- 1 = restreint,
- 2 = confidentiel avec les partenaires,
- 3 = confidentiel et interne (ce niveau pourrait inclure les informations classifiées de défense au niveau confidentiel défense),
- 4 = secret (ce niveau pourrait inclure les informations classifiées de défense au niveau secret défense).



Conseils pratiques :

L'échelle présente généralement une pondération entre 0 (aucune atteinte) et 4 (atteinte très importante). Il est néanmoins envisageable de définir une échelle avec moins de valeurs. Le nombre de pondérations est généralement le même pour chaque critère de sécurité. Dans la mesure du possible, les valeurs de références doivent être objectives, explicites, propres à l'organisme et liées à ses orientations

*stratégiques et comprendre un ensemble de valeurs bornées.
Ce travail est généralement réalisé dans un tableau à double entrée, avec les critères de sécurité en colonnes et la pondération en lignes, les valeurs de référence devant être indiquées à chaque intersection.*

Il est ensuite souhaitable de déterminer une liste d'**impacts** pertinents pour l'organisme. Ces impacts reflètent les axes stratégiques de l'organisme. Il peut s'agir par exemple de perte d'image de marque, d'infraction aux lois, de pertes financières, de révocation de personnels... Ils permettront d'envisager différents domaines pouvant être impactés et d'apporter des éléments de justification des besoins de sécurité.



Conseils pratiques :

Le nombre d'impacts représentatifs est généralement compris entre 1 et 3.

Afin de rendre les impacts plus objectifs, il convient de fournir des exemples explicites de chacun d'eux en termes de conséquences envisageables.

Tous ces éléments figureront dans la PSSI.

2.3.5 Tâche 5 : expression des besoins de sécurité

Objectif

L'objectif de cette tâche est d'identifier de manière générale les **besoins de sécurité** associés à chaque domaine d'activités (et éventuellement chaque fonction et information concernée) défini dans le périmètre de la PSSI. Ces besoins de sécurité seront utiles dans l'élaboration des règles de sécurité et dans toute étude de sécurité dans le périmètre de la PSSI afin d'identifier des objectifs de sécurité d'un système particulier.

Démarche

La démarche exploite les résultats précédents :

- la liste des domaines d'activités (et éventuellement des fonctions et informations) définissant le périmètre de la PSSI ;
- la liste des critères de sécurité retenus ;
- l'échelle de besoins (impacts et valeurs de référence).

Pour chacun des domaines d'activités et chaque critère de sécurité (par exemple disponibilité, intégrité et confidentialité), il faut déterminer la valeur correspondante à l'échelle de besoins pour les impacts retenus. La valeur la plus importante pour les différents critères est retenue.

Exemples:

- si un domaine d'activités doit être confidentiel pour ne pas porter préjudice à son bon fonctionnement, la valeur correspondante pourrait être égale à 3 sur une échelle de 0 à 4 selon les valeurs de référence de l'échelle ;
- si un domaine d'activités nécessite de travailler en temps réel pour ne pas porter préjudice à son bon fonctionnement, la valeur correspondante pourrait être égale à 4 sur une échelle de 0 à 4 selon les valeurs de référence de l'échelle.



Conseil pratique :

Les résultats d'une analyse des risques SSI appliquée au périmètre de la PSSI permettent généralement d'exprimer les besoins de sécurité des éléments essentiels.

Les besoins de sécurité feront l'objet d'une synthèse figurant dans la PSSI.

2.3.6 Tâche 6 : identification des origines des menaces

Objectif

Cette tâche consiste à identifier et caractériser les origines des menaces qui pèsent sur le périmètre de la PSSI. Ces origines de menaces (**éléments menaçants** et **méthodes d'attaque**) seront utiles dans l'élaboration des règles de sécurité et dans toute étude de sécurité dans le périmètre de la PSSI afin d'identifier des objectifs de sécurité d'un système particulier.



Attention :

L'objectif n'est pas d'identifier les vulnérabilités du système d'information existant ou ses points faibles et de surcroît les risques qui pèsent sur lui, mais de décrire les origines des menaces qu'il conviendra de prendre en compte pour l'élaboration des règles de sécurité.

Démarche

La liste des méthodes d'attaque pertinentes pour le périmètre de la PSSI doit être établie indépendamment des besoins de sécurité. Elle représente les sources de l'exposition de l'organisme aux risques liés à la sécurité des systèmes d'information. Il peut s'agir notamment d'incendie, de vol de documents, d'altération des données... Une méthode d'attaque est retenue dans la mesure où sa réalisation a un impact sur le système étudié.



Conseil pratique :

Une méthode d'analyse des risques SSI fournit généralement une liste de méthodes d'attaque génériques.

Les méthodes d'attaque retenues sont ainsi caractérisées :

- les critères de sécurité qui peuvent être affectés sont identifiés ;
- les éléments menaçants qui pourraient les employer peuvent être caractérisés par :
 - o un **type** (naturel, humain, environnemental),
 - o une **cause** (si elle est accidentelle, alors il convient de préciser l'exposition et les ressources disponibles, si elle est délibérée, alors il convient de préciser l'expertise, les ressources disponibles et la motivation),
 - o un potentiel d'attaque estimé (qui résume la qualification de la cause) ;

L'ensemble des menaces non retenues fait enfin l'objet de justifications explicites.



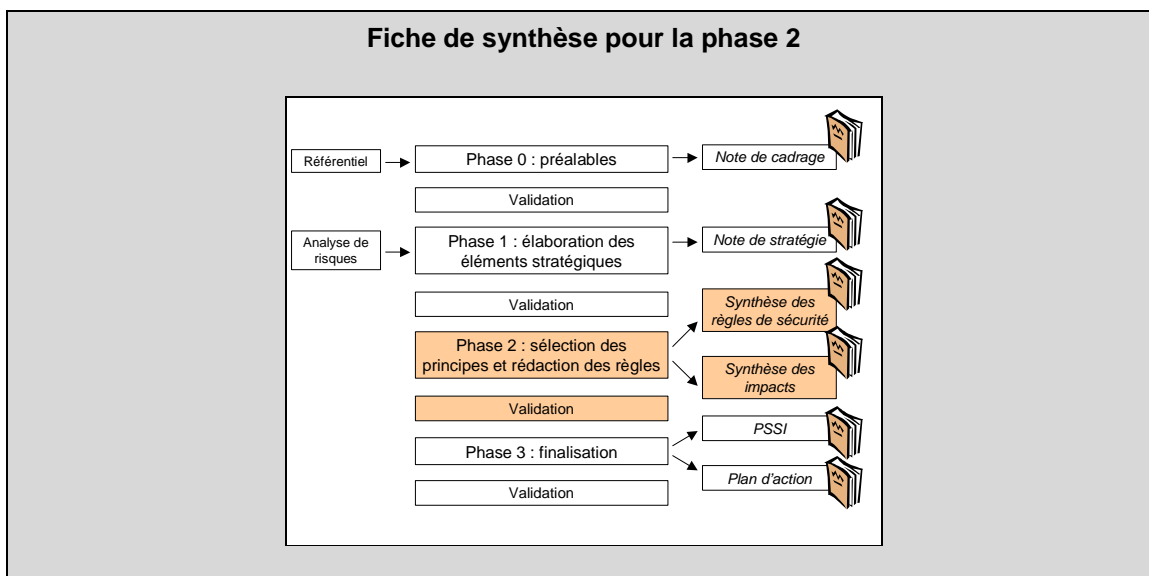
Conseils pratiques :

Les résultats d'une analyse des risques SSI appliquée au périmètre de la PSSI permettent généralement de sélectionner et caractériser les méthodes d'attaque et éléments menaçants.

Seules les méthodes d'attaque réellement significatives et concrètes doivent être retenues et décrites de manière non technique pour assurer une meilleure sensibilisation du lecteur. De plus, ne pas hésiter à illustrer les menaces par des exemples concrets puis dans le ou les métiers de l'organisme.

La liste des origines des menaces retenues et caractérisées, ainsi que la liste des origines des menaces non retenues avec des justifications, figureront dans la PSSI.

2.4 Phase 2 : sélection des principes et rédaction des règles



Objectifs de la phase

Le travail de cette phase consiste à sélectionner, concevoir, préparer, documenter et valider la déclinaison des principes généraux d'une PSSI et des choix stratégiques de l'organisme. Ce travail se traduit en l'élaboration d'un corpus de règles directement applicables.

Acteurs de la phase

- Direction générale
- Comité de pilotage
- Groupe d'experts

Éléments en entrée

- Note de cadrage
- Note de stratégie de sécurité

Éléments en sortie

- Note de synthèse justificative des choix de règles
- Note de synthèse des impacts organisationnel et financier

Tâches

1. Sélection des principes
2. Construction des règles
3. Synthèse et validation

Observations

Les points essentiels à prendre en compte sont la cohérence des règles, leur applicabilité et enfin l'auditabilité de l'ensemble.

Validation

Documents	Valideur
Note de synthèse justificative des choix de règles Note de synthèse des impacts organisationnel et financier	Comité de pilotage puis Direction générale

2.4.1 Tâche 1 : choix des principes de sécurité

Objectif

Cette tâche consiste à sélectionner les principes de sécurité qu'il conviendra de développer et instancier en règles de sécurité lors de la tâche suivante.

Démarche

Le choix des principes de sécurité s'effectue sur la base des éléments suivants :

- dans la note de cadrage :
 - o le référentiel du système d'information ;
- dans la note de stratégie de sécurité
 - o la définition du périmètre de la PSSI ;
 - o la liste de besoins de sécurité identifiés ;
 - o la liste des origines de menaces retenues.

Tout d'abord, le référentiel du système d'information renseigne sur les entités présentes (logiciels, matériels, réseaux, organisation, sites personnel). Les principes de sécurité pour lesquels il n'existe aucune entité dans l'organisme sont écartés.

D'autre part, la définition du périmètre de la PSSI permet d'affiner la sélection précédente en écartant éventuellement d'autres principes de sécurité de l'étude.

L'expression des besoins de sécurité contribue elle-aussi au choix des principes de sécurité. En effet, les domaines d'activités ou les fonctions et informations reposent sur des entités techniques ou non techniques. Si le lien entre les éléments essentiels et les entités est établi, il convient de ne retenir que les principes de sécurité pour lesquels une entité est porteuse d'informations ou de fonctions pour l'organisme.

Enfin, puisque les éléments menaçants exploitent les vulnérabilités des entités selon des méthodes d'attaque particulières pour se réaliser, on affine à nouveau la sélection des principes de sécurité en écartant ceux qui ne concernent pas les entités pertinentes au regard des origines des menaces retenues.

En fonction de cette analyse, le comité de pilotage statue sur la liste des principes de sécurité à retenir.



Conseils pratiques :

Cette analyse, qui doit être réalisée de façon macroscopique, privilégie la conservation des principes de sécurité en cas de doute sur leur pertinence.

Elle permet de justifier systématiquement chaque principe de sécurité écarté. La traçabilité ainsi assurée permet de maîtriser l'impact de l'évolution des besoins sur les travaux d'élaboration de la PSSI.

2.4.2 Tâche 2 : élaboration des règles de sécurité

Objectif

Cette tâche consiste à instancier les principes de sécurité retenus en règles de sécurité selon les éléments contenus dans la note de cadrage et la note de stratégie de sécurité. Chaque principe de sécurité retenu doit être décliné en une ou plusieurs règles de sécurité adaptées au contexte du périmètre de la PSSI.

Démarche

L'instanciation des principes de sécurité en règles de sécurité débute par un affinage et une décomposition de chaque principe. D'une part, la formulation des règles de sécurité doit refléter la couverture des origines des menaces retenues. D'autre part, elle doit aussi refléter les critères de sécurité (disponibilité, intégrité, confidentialité...) que les origines de menaces concernées peuvent affecter.

Le niveau des règles de sécurité est alors déterminé en fonction des besoins de sécurité. En effet, la sensibilité des domaines d'activités ou des fonctions et informations doit impacter le niveau de sécurité des règles de sécurité de telle sorte qu'il soit en adéquation avec le risque encouru.

Le référentiel identifié dans la note de cadrage (aspects réglementaires et contractuels, référentiel du système d'information, référentiel de sécurité...) permet quant à lui d'établir la cohérence avec les moyens existants, notamment en termes techniques et budgétaires. Les règles doivent être suffisamment précises afin de les adapter parfaitement au contexte du périmètre de la PSSI.

Une consolidation des règles de sécurité doit enfin être effectuée par des entretiens avec les responsables de leur mise en œuvre.



Conseils pratiques :

L'expertise du groupe de travail permet la réalisation de cette tâche difficile qui requiert une bonne maîtrise de l'état de l'art.

La pertinence des règles de sécurité est garantie par un rapport entre l'impact et l'efficacité.

L'implication de la maîtrise d'œuvre et des différents responsables permet de garantir l'applicabilité des règles de sécurité et l'adhésion des différents acteurs.

L'élaboration des règles de sécurité doit faire l'objet d'une argumentation systématique se basant sur les éléments stratégiques.

Il est nécessaire de mettre en évidence les rapports coûts-bénéfices, en estimant les coûts de mise en œuvre des règles de sécurité, afin d'effectuer des choix cohérents avec les ressources de l'organisme.

Cette tâche est l'occasion de discuter et argumenter des résultats de la démarche de gestion des risques et permet de définir des exigences précises.

2.4.3 Tâche 3 : élaboration des notes de synthèse

Objectif

Cette tâche consiste à synthétiser le travail effectué afin d'en obtenir la validation, ce qui permettra ensuite de finaliser la PSSI. La validation concerne d'une part les règles de sécurité et d'autre part les impacts de leur mise en œuvre.

Démarche

Le groupe d'experts doit élaborer une note de synthèse, à destination du comité de pilotage, qui présente la justification des choix concernant la sélection des principes de sécurité et la déclinaison en règles de sécurité. La liste des principes de sécurité est fournie en annexe de ce guide.

Le comité de pilotage, s'il entérine ces choix, propose alors une note de synthèse à destination de la direction générale. Cette note de synthèse doit permettre d'exposer à la direction générale les choix réalisés ainsi que leur impact organisationnel et financier. Cette note lui permet de valider les orientations retenues dans la PSSI, au regard des enjeux particuliers de l'organisme.



Conseils pratiques :

La note de synthèse à destination du comité de pilotage doit permettre la prise de décision pour la mise en œuvre des règles retenues.

La note de synthèse à destination de la direction générale doit permettre la prise de décision pour la mise en œuvre de la PSSI en présentant très clairement les enjeux et les coûts associés de celle-ci.

L'analyse des coûts induits sera menée de façon macroscopique.

2.5 Phase 3 : finalisation

Fiche de synthèse pour la phase 3	
Objectifs de la phase	
La finalité de cette phase est de conduire une étape ultime de validation de la PSSI et du plan d'action associé par la direction générale	
Acteurs de la phase	
<ul style="list-style-type: none"> - Comité de pilotage - Groupe d'experts 	
Éléments en entrée	Éléments en sortie
<ul style="list-style-type: none"> - Les règles retenues validées 	<ul style="list-style-type: none"> - La PSSI validée - Plan d'application de la PSSI proposant en particulier un plan d'action selon les priorités définies
Tâches	
<ol style="list-style-type: none"> 1. Finalisation et validation de la PSSI 2. Élaboration et validation du plan d'action 	
Observations	
<p>Une fois la PSSI revue et validée par le comité de pilotage, un document de synthèse devra être élaboré pour soutenir la présentation de la PSSI à la hiérarchie en vue de sa validation. L'implication des différents acteurs, notamment des futurs responsables de la mise en œuvre de la PSSI, est fondamentale pour disposer par la suite des ressources humaines et financières adéquates et prévoir les délais.</p> <p>C'est à ce niveau que se mesure l'importance de l'implication des experts lors de la déclinaison des principes et objectifs généraux dans les différents domaines. Cela montre également l'importance de l'applicabilité comme critère essentiel lors du choix et de la formalisation des règles.</p> <p>La validation du plan d'action doit passer par une étape de simplification de la PSSI pour transmettre les messages forts à la Direction Générale.</p>	
Validation	
Documents	Validateur
PSSI Plan d'action	Comité de Pilotage puis Direction générale

2.5.1 Tâche 1 : finalisation et validation de la PSSI

Objectif

L'objectif de cette phase est de produire le document validé exprimant la Politique de Sécurité des Systèmes d'Information de l'organisme. Ce document devra être validé et signé par la hiérarchie.



Conseil pratique :

Il est souvent conseillé de constituer un comité de sécurité qui sera chargé de valider le contenu de la PSSI et de s'assurer de son évolution dans le temps.

Démarche

Avant de procéder à une validation finale du document, une étape de revue doit être programmée pour s'assurer de la cohérence de l'ensemble.

Cette étape consiste à vérifier :

- la cohérence des règles énoncées,
- l'exhaustivité de la couverture des risques jugés comme significatifs,
- la traduction complète de l'ensemble des principes et règles, jugés pertinents pour l'organisme et énoncés dans le référentiel présenté en annexe au présent document,
- l'applicabilité des exigences et règles en fonction des pratiques en vigueur au sein de l'organisme,

Enfin, cette étape de revue peut également conduire à réaliser une normalisation, voir une simplification des éléments énoncés dans la politique, notamment dans un document de synthèse qui permettra une meilleure implication de la hiérarchie.

2.5.2 Tâche 2 : élaboration et validation du plan d'action

Objectif

Cette phase consiste à assurer l'application de la PSSI au système d'information de l'organisme.

Elle poursuit plusieurs objectifs :

- faire en sorte que la mise en œuvre de la PSSI s'accompagne de consultations, d'une coordination et coopération entre les différents acteurs du système d'information,
- convenir le plus rapidement possible d'initiatives spécifiques en vue de l'application de la PSSI et en particulier établir un premier plan d'action prioritaire,
- donner une large diffusion aux principes et aux règles de la PSSI,
- diffuser la PSSI à l'ensemble des acteurs interne et externe,
- accompagner la diffusion d'une communication adaptée à l'organisme de manière à sensibiliser et faire adhérer les personnels.



Conseil pratique :

Néanmoins, pour être applicable et rester utilisable par tous, son contenu et sa forme doivent être adaptés selon les destinataires.

- réexaminer la PSSI en fonction des événements majeurs affectant la mission ou la vie de l'organisme, ou une fois au moins tous les cinq ans, pour vérifier l'adéquation des règles par rapport à l'évolution du système d'information de l'organisme.

La PSSI est mise en œuvre au niveau de chaque site, division, service ou unité opérationnelle au moyen d'un plan de sécurité qui décline les principes et les règles de sécurité en mesures de sécurité techniques et non techniques adaptées aux moyens, à l'environnement et au fonctionnement du système d'information de l'échelon considéré.

Il appartient aux autorités identifiées dans la PSSI, responsables de chaque unité opérationnelle, de définir ces différentes mesures et de veiller à leur bonne application.

Démarche

Chaque responsable d'unité opérationnelle et le responsable de la sécurité du système d'information (pour ce qui concerne les actions d'ordre général) doit établir un plan d'action qui détermine par rapport à l'existant, les actions prioritaires à entreprendre sur le SI.

La priorité est fixée pour s'assurer de la prise en compte des risques jugés les plus significatifs.

Le plan d'action sera soumis pour validation au comité de sécurité chargé de la validation et de l'évolution de la politique.

Pour chaque action doit présenter les éléments suivants :

- l'objectif de l'action et le responsable de l'action ;
- la démarche à suivre, présentant la liste détaillée des tâches à mener ;
- la dépendance vis-à-vis des résultats d'étapes précédentes ;
- une estimation du planning et un budget ;
- les modalités de validation.



Conseil pratique :

Pour obtenir une planification cohérente, il est nécessaire de se baser non seulement sur la PSSI définissant l'objectif à atteindre, mais aussi sur la situation actuelle. C'est ici que les contraintes organisationnelles et le référentiel légal prennent toute leur importance, ainsi que la capacité du personnel d'avancer vers le but. Il faut programmer toutes les actions, parallèles, simultanées ou concurrentes et tenir compte des chronologies et hiérarchies logiques.

3 Plan-type d'une PSSI

Le plan qui suit est une proposition de plan générique et compatible avec la démarche méthodologique d'élaboration de politique de sécurité des systèmes d'information.

Ce plan peut être adapté, essentiellement selon les destinataires de la PSSI.

- Partie I - Éléments stratégiques

o Chapitre 1 - Périmètre de la PSSI

Ce chapitre délimite le champ d'application de la PSSI, par exemple en termes de domaines d'activités ou de systèmes d'information.

o Chapitre 2 - Enjeux et orientations stratégiques

Ce chapitre formalise les enjeux liés au périmètre défini dans le chapitre précédent.

o Chapitre 3 - Aspects légaux et réglementaires

Ce chapitre identifie le référentiel légal et réglementaire lié au périmètre de l'étude.

o Chapitre 4 - Échelle de besoins

Ce chapitre présente une échelle de besoins comportant une pondération et des valeurs de référence selon les critères de sécurité choisis, ainsi qu'une liste d'impacts enrichis d'exemples.

o Chapitre 5 - Besoins de sécurité

Ce chapitre expose les besoins de sécurité des domaines d'activité de l'organisme (ou des éléments essentiels), selon l'échelle de besoins présentée dans le chapitre précédent.

o Chapitre 6 – Origines des menaces

Ce chapitre décrit l'ensemble des origines de menaces retenues et non retenues pour le périmètre de l'étude, avec des justifications.

- Partie II - Règles de sécurité

Ce chapitre présente l'ensemble des règles de sécurité classées par thème. Ces règles sont déclinées des principes de sécurité fournis en annexe du présent guide.

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