Gestion de l'intégration de la SSI dans les projets (GISSIP)

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

conseil.dcssi@sgdn.pm.gouv.fr

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
Premier ministre
Secrétariat général de la défense nationale

Gestion de l'intégration de la SSI dans les projets (GISSIP)

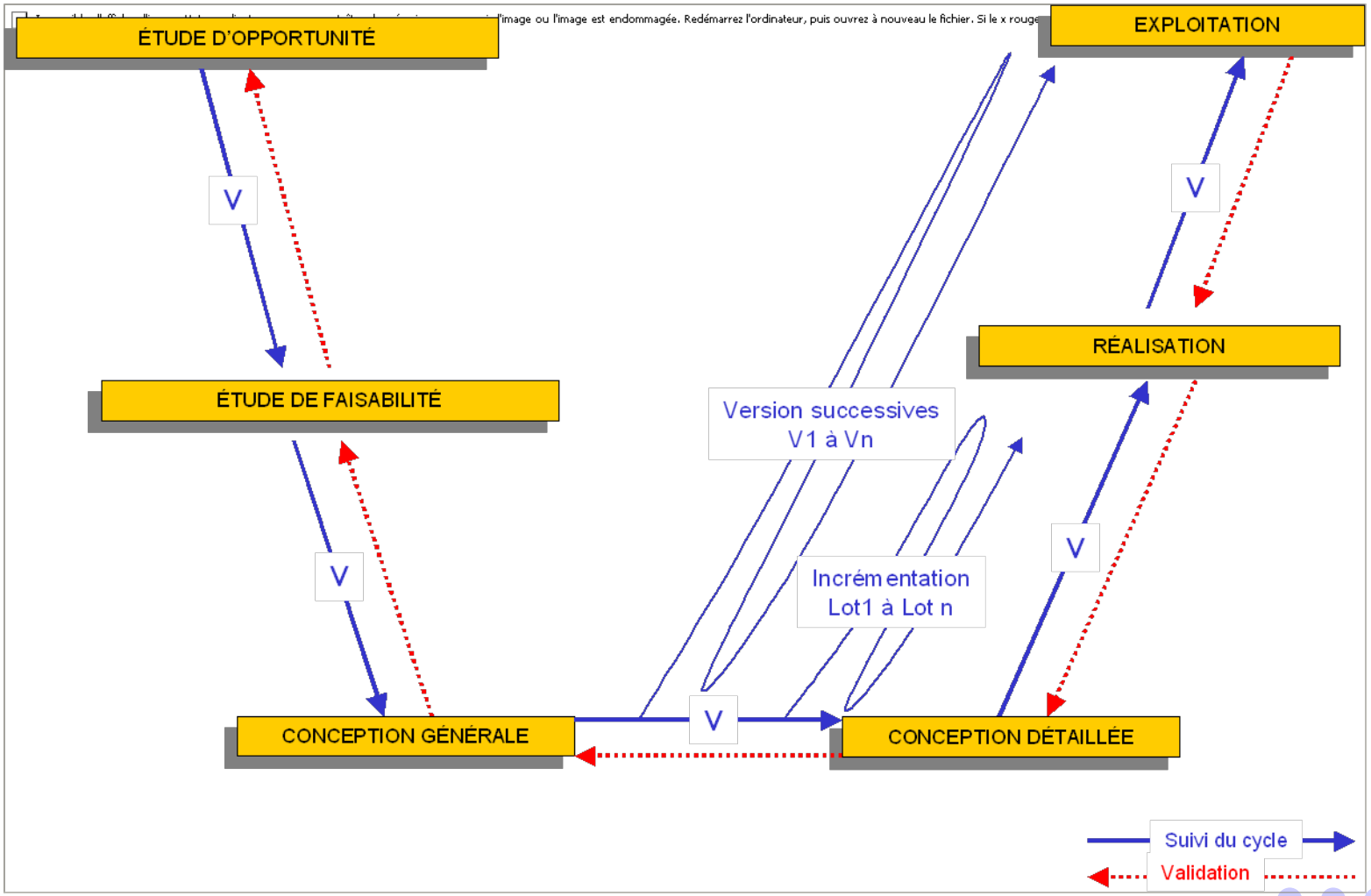
Plan de la présentation

1. Présentation du cycle de vie et des acteurs
2. Fondements de l'intégration de la sécurité dans le cycle de vie des SI
3. Actions SSI à mener par étape du cycle de vie des SI

Présentation du cycle de vie et des acteurs

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
Premier ministre
Secrétariat général de la défense nationale

Un cycle de vie générique



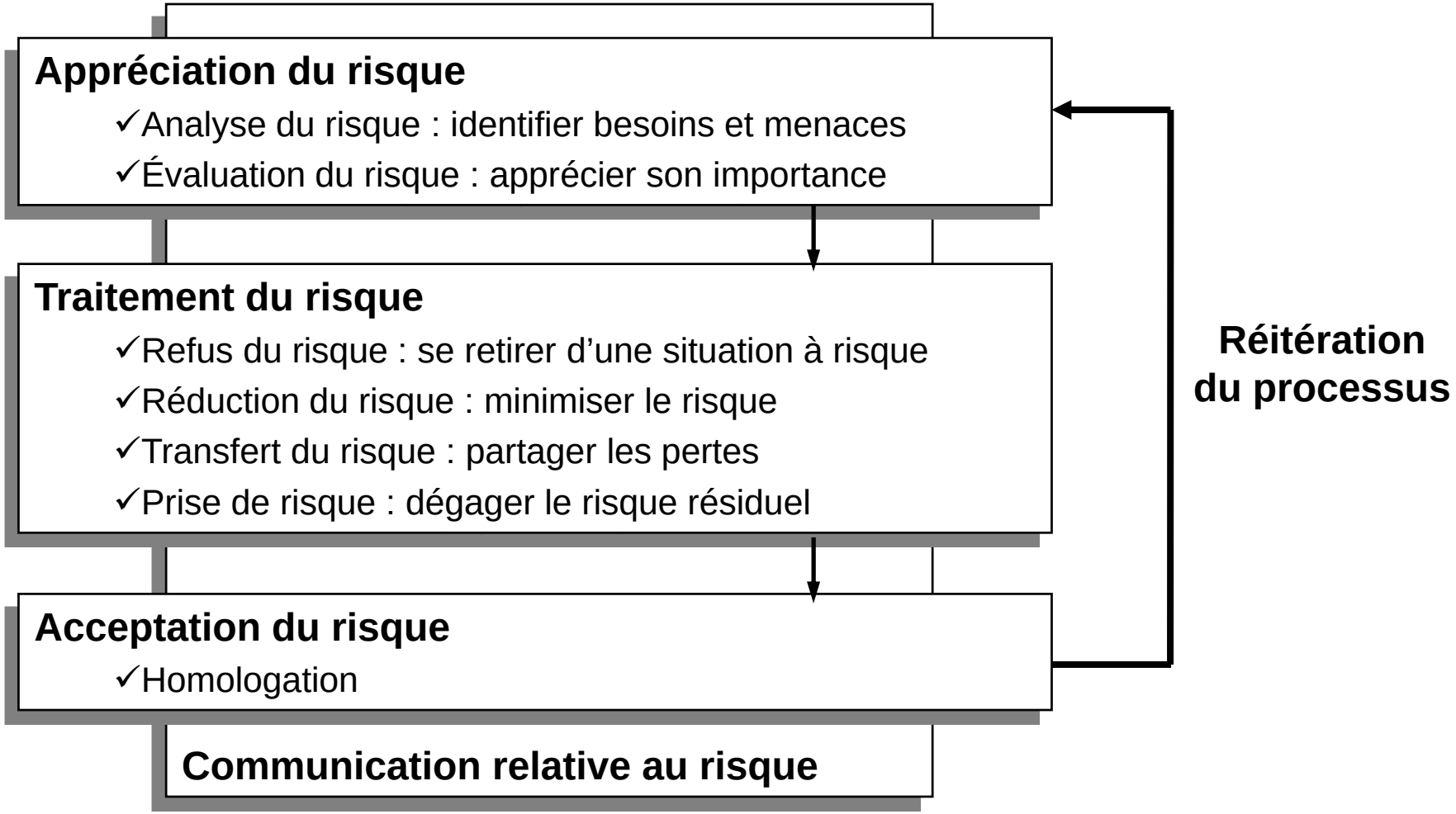
Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
Premier ministre
Secrétariat général de la défense nationale

Des rôles génériques

- Les utilisateurs
  - ✓ à l'origine des besoins
- La maîtrise d'ouvrage
  - ✓ responsable de la définition des besoins, de l'identification des objectifs de sécurité et du pilotage du projet
- La maîtrise d'œuvre
  - ✓ responsable des propositions techniques, de la détermination des exigences de sécurité et de leur mise en œuvre
- L'autorité d'homologation
  - ✓ valide le compromis entre la sécurité et les contraintes du projet sur la base du dossier de sécurité
- Le responsable SSI
  - ✓ généralement chargé de la définition et de l'application de la PSSI
- Les experts techniques
  - ✓ soutien technique tout au long du projet
- Le comité de pilotage
  - ✓ prend les décisions stratégiques sur le projet, arbitre
- La commission d'homologation
  - ✓ fournit à l'autorité d'homologation les éléments nécessaires à sa prise de décision

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

Le processus continu de gestion des risques SSI



Un niveau d'intégration de la SSI qui varie selon les enjeux de sécurité

- L'intégration de la SSI se fait en adéquation avec les enjeux de sécurité du système :
  - ✓ une **note d'orientations SSI**, validée par l'autorité d'homologation, définit la stratégie de sécurité à adopter.
- 5 niveaux de maturité SSI cumulatifs :

1. la mise en œuvre de la SSI 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).

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
Premier ministre
Secrétariat général de la défense nationale

Une condition à la mise en œuvre des SI : l'homologation de sécurité

- L'homologation de sécurité est la déclaration, par l'autorité d'homologation, conformément à la 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 et que les risques résiduels sont acceptés et maîtrisés

- Le contenu du dossier de sécurité peut comporter les éléments suivants :
  - ✓ une fiche d'expression rationnelle des objectifs de sécurité (FEROS),
  - ✓ une cible de sécurité,
  - ✓ une politique de sécurité du système d'information (PSSI),
  - ✓ la documentation relative aux tests (recette, qualification…),
  - ✓ la documentation relative aux évaluations de sécurité,
  - ✓ les tableaux de bord SSI (TDBSSI).

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

Étape 1 : l'étude d'opportunité

Niveau de maturité SSI	Actions	Livrables
1	Analyse des enjeux de sécurité	Note d'orientations SSI
2		
3		
4		
5		

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
Premier ministre
Secrétariat général de la défense nationale

Étape 2 : l'étude de faisabilité

Niveau de maturité SSI	Actions	Livrables
1	Aucune	Aucun
2		
3	Étude du contexte Expression des besoins de sécurité Étude des menaces	Note de stratégie de sécurité
4		
5		

Étape 3 : la conception générale

Niveau de maturité SSI	Actions	Livrables
1	Aucune	Aucun
2	Inventaire des meilleures pratiques SSI applicables Estimation de l'impact de leur application	Liste des meilleures pratiques SSI applicables
3	Identification des objectifs de sécurité	Première version de la FEROS
4		
5		

Étape 4 : la conception détaillée

Niveau de maturité SSI	Actions	Livrables
1	Aucune	Aucun
2	Revue des choix des meilleures pratiques SSI et négociation Réflexion sur la nature des niveaux de garantie	Liste des meilleures pratiques SSI négociées
3	Affinage de l'étude de sécurité Formalisation des règles de sécurité Précision du traitement des risques SSI	FEROS PSSI Première version de la cible de sécurité
4	Idem que le niveau 3 Élaboration des TDBSSI	FEROS PSSI Première version de la cible de sécurité Documentation d'élaboration des TDBSSI
5		

Étape 5 : la réalisation

Niveau de maturité SSI	Actions	Livrables
1	Mise en œuvre des meilleures pratiques SSI	Aucun
2		
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	Cible de sécurité Documents d'application PSSI Documentation relative aux tests Documentation relative aux évaluations
4	Idem que le niveau 3 Alimentation des TDBSSI	Cible de sécurité Documents d'application PSSI Documentation relative aux tests Documentation relative aux évaluations Première version de TDBSSI
5		

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
Premier ministre
Secrétariat général de la défense nationale

Étape 6 : l'exploitation

Niveau de maturité SSI	Actions	Livrables
1	Homologation	Aucun
2	Homologation Accompagnement Mise en œuvre des meilleures pratiques SSI	Décision d'homologation
3	Homologation Mise en œuvre des règles Tenue à jour de la gestion des risques SSI	Décision d'homologation Dossier de sécurité enrichi
4	Idem que le niveau 3 Alimentation des TDBSSI	Décision d'homologation Dossier de sécurité enrichi TDBSSI
5	Idem que le niveau 4 Révision des documents d'application et TDBSSI	

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
Premier ministre
Secrétariat général de la défense nationale

CONCLUSION

- GISSIP permet une intégration de la SSI structurée, complète et adaptée aux enjeux de sécurité de chaque SI.
- La méthode aide à déterminer les actions SSI à entreprendre et les documents à produire tout au long du cycle de vie des SI, et ce, en fonction du niveau de maturité SSI adéquat.
- L'approche est à considérer avec souplesse afin de l'appliquer en cohérence avec les pratiques et outils de chaque organisme.
- Il convient de réévaluer régulièrement les enjeux de sécurité, et donc le niveau de maturité SSI adéquat pour vérifier que les actions entreprises apportent bien le niveau de confiance le plus approprié.

AVEZ-VOUS DES QUESTIONS ?