PREMIER MINISTRE
Secrétariat général de la défense nationale
Direction centrale de la sécurité des systèmes d'information
Sous Direction des Opérations
Bureau Conseil

Élaboration de tableaux de bord SSI

MÉMENTO

Version du 5 février 2004

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

La problématique des tableaux de bord SSI

Pourquoi élaborer un tableau de bord ?

Un tableau de bord parfaitement adapté à chaque type de fonction de la "voie fonctionnelle SSI" est un atout pour améliorer la qualité des services de sécurité et maîtriser le niveau de sécurité global de sécurité des systèmes d'information.

Il constitue en effet **un outil de synthèse et de visualisation indispensable** pour suivre toutes les actions liées à la SSI. Il contribue à contrôler que la stratégie définie dans la politique de sécurité est mise en œuvre par les niveaux de pilotage et opérationnel, et à la remontée d'informations pertinentes jusqu'aux décideurs.

Pour le **niveau stratégique**, la mise en place d'un tableau de bord SSI permet :
- de suivre l'application de la politique de sécurité,
- d'établir des comparaisons avec d'autres organismes,
- de préparer les choix de mise en place des ressources (définition de priorités, réévaluation de la menace et du risque).

Pour le **niveau de pilotage**, la mise en place d'un tableau de bord SSI permet :
- de contrôler la réalisation des objectifs par le niveau opérationnel,
- d'améliorer la qualité de service.

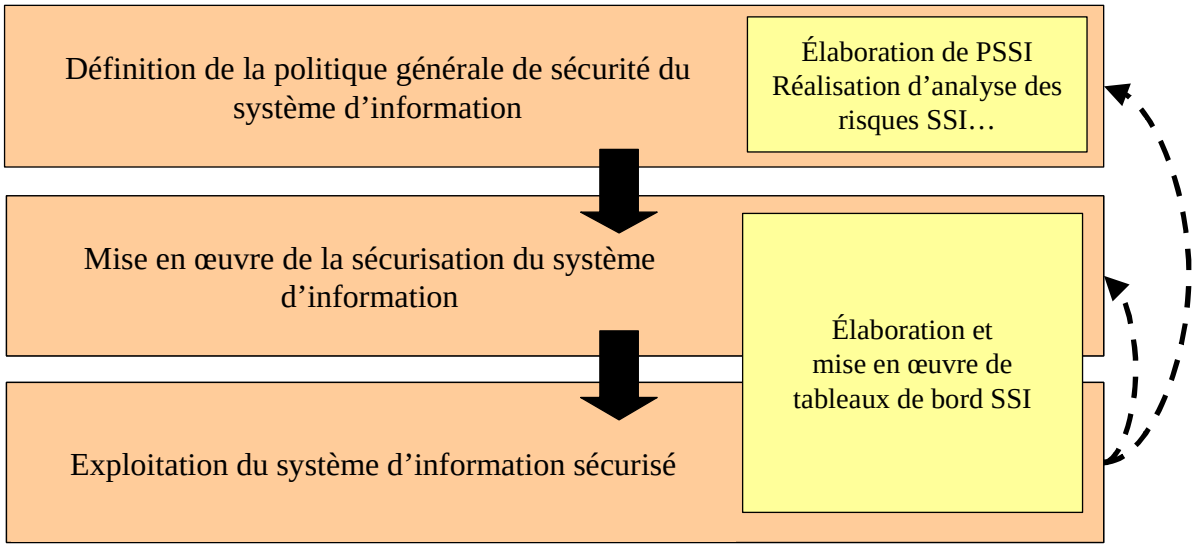
Pour le **niveau opérationnel**, la mise en place d'un tableau de bord SSI permet :
- de préciser les besoins opérationnels à mettre en œuvre,
- de mesurer la production et les efforts entrepris pour atteindre les objectifs visés en matière de production,
- de motiver et dynamiser les équipes.

Qu'est-ce qu'un tableau de bord SSI ?

Un tableau de bord SSI permet de disposer, aux différents niveaux décisionnels, de pilotage et opérationnels, d'une vision synthétique de la situation de la sécurité, que ce soit dans ses dimensions techniques ou fonctionnelles (couverture des risques, qualité de la politique de sécurité, suivi des audits, des actions et des alertes…). Cette vision renseigne sur l'état et les tendances de la SSI.

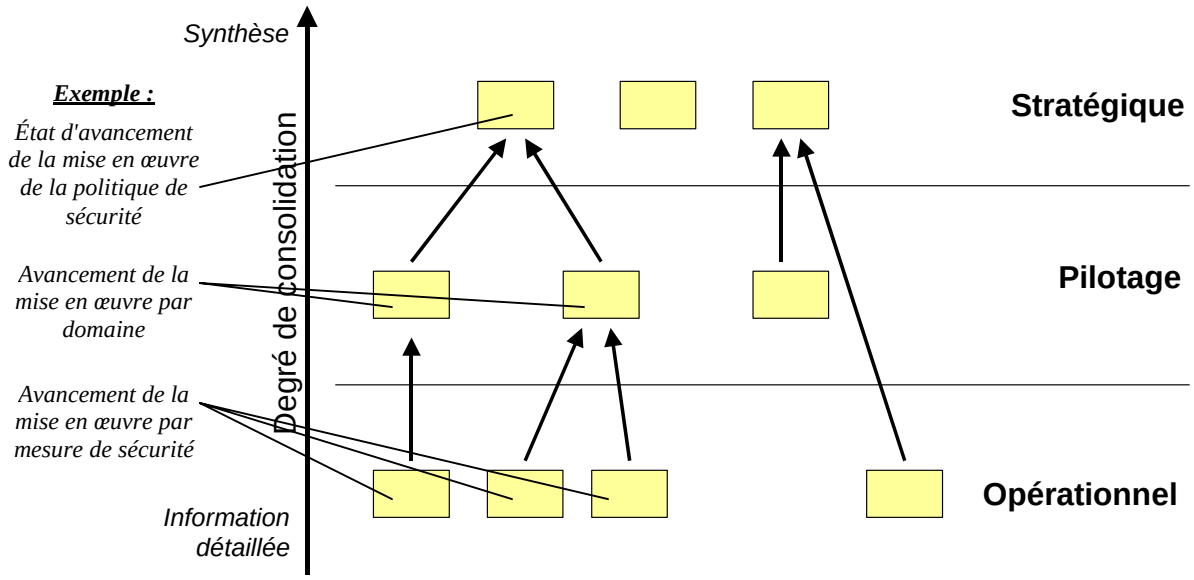
Les tableaux de bord SSI peuvent être constitués à partir :
- d'objectifs de sécurité issus d'une analyse de risques (par exemple à l'aide de la méthode EBIOS®),
- de règles de sécurité issues d'une politique de sécurité,
- d'actions de sécurité issues d'un plan d'action.

Dans une démarche structurée de la sécurité des systèmes d'information, les tableaux de bord SSI représentent la suite logique de l'élaboration d'une politique de sécurité et de l'identification des objectifs de sécurité.



En outre, d'autres éléments externes (résultats d'audits, évolution du contexte sécurité, évolution technique du SI…) peuvent impliquer une adaptation des tableaux de bord SSI. Cet outil reste ainsi en évolution tout au long de l'existence du SI qu'il couvre.

La remontée des indicateurs d'un tableau de bord SSI peut se représenter comme suit :



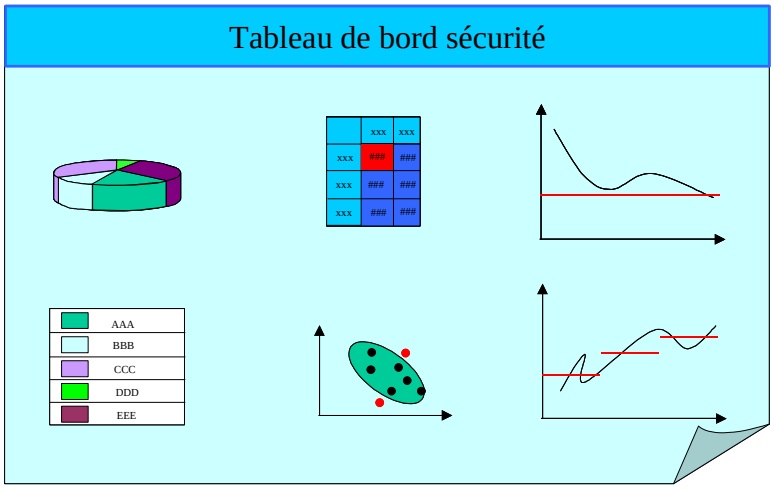
Différents indicateurs pourront être élaborés en parfaite cohérence avec les objectifs de sécurité :

- au **niveau stratégique** :
  - l'état d'avancement de la mise en œuvre de la politique de sécurité,
  - l'évolution des incidents liés à la SSI,
  - …
- au **niveau fonctionnel** :
  - l'avancement de la sécurisation par domaine (organisationnel, logiciels, applications, réseaux, sécurité physique, aspects humains),
  - le suivi des actions de sécurité (études, audits, mise en œuvre, formation),
  - …
- au **niveau opérationnel** :
  - la disponibilité des réseaux,
  - l'avancement de la mise en œuvre des mesures de sécurité,
  - l'identification des incidents,
  - suivi des contrôles de sécurité,
  - …

Les données constitutives seront elles-aussi collectées de manière cohérente avec les objectifs de sécurité, principalement au niveau opérationnel. Il peut s'agir par exemple :

- d'analyses des journaux (pare-feu, antivirus, traces…),
- de rapports de mise en œuvre,
- de fiches d'incidents,
- de rapports de contrôles ou d'audit,
- …

Les indicateurs utilisés pour la constitution des tableaux de bord SSI s'appuient sur des données, dont une partie est issue des divers éléments du système d'information et notamment des dispositifs de sécurisation (pare-feu, antivirus, analyse des traces…).



Le guide d'élaboration de tableaux de bord SSI

La réalisation d'indicateurs permettant de renseigner un tableau de bord est un travail complexe. Un guide d'élaboration de tableau de bord SSI a donc été réalisé par la DCSSI afin de faciliter ce travail et d'homogénéiser les méthodes.

Ce guide propose **une démarche et des outils directement utilisables**. Il est suffisamment souple pour être facilement adapté à des besoins spécifiques.

Section 1 – Méthodologie

La démarche d'élaboration est décomposée en cinq étapes successives décrites ci-après. Cette démarche itérative permet de garantir la cohérence des tableaux de bord SSI avec les objectifs stratégiques et les évolutions du contexte (du SI, des risques, des destinataires…).

Lors de la première itération, les étapes sont généralement réalisées successivement. Par la suite, les étapes d'exploitation et d'évolution des tableaux de bord peuvent donner lieu à de nouvelles itérations.

Étape 1 - Pré-requis

La première étape consiste à **rassembler des éléments préalables** à l'élaboration de tableaux de bord SSI :

- identification des destinataires des tableaux de bord SSI,
- formalisation des utilisations prévues,
- formalisation des périodicités souhaitées,
- expression des objectifs de sécurité (issus d'une analyse des risques SSI),
- expression des objectifs de progression du niveau de SSI (issus d'un plan d'action),
- informations sur le SI,
- identification des sources de données possibles,
- bilan sur le budget et les moyens mis en œuvre.

Étape 2 - Mise en place du projet "Tableaux de bord SSI"

La mise en place consiste ensuite à **identifier et mobiliser les acteurs** pour constituer des groupes de travail :

- un groupe "*utilisation*" définit le besoin en tableaux de bord SSI en partant des besoins fonctionnels identifiés,
- un groupe "*technique*" valide la faisabilité des tableaux de bord SSI ainsi que de leur pertinence par rapport aux réalités techniques du système d'information,
- un groupe "*pilotage*" maîtrise les coûts et charges récurrents associés aux tableaux de bord SSI en phase de production,
- un groupe "*exploitation*" s'assure que les tableaux de bord SSI et les procédures associées pourront être exploités aisément autant dans leur aspect constitution que dans leur aspect utilisation.

Étape 3 - Élaboration des tableaux de bord SSI

L'étape suivante permet de **construire les tableaux de bord SSI** en se basant sur les différents objectifs identifiés :

- formalisation des objectifs mesurables,
- sélection des sources de données exploitables,
- élaboration des indicateurs correspondants,
- constitution des tableaux de bord SSI à partir des indicateurs,
- élaboration des procédures d'alimentation des tableaux de bord SSI,
- validation de l'applicabilité des tableaux de bord SSI.

Étape 4 - Exploitation des tableaux de bord SSI

Cette étape consiste à **éditer et exploiter les tableaux de bord SSI** selon les périodicités prévues. Il s'agit donc de :

- recueillir les données constitutives :
  - collationnement,
  - traitement,
  - calcul des indicateurs ;
- d'utiliser les tableaux de bord SSI dans le processus de décision.

Étape 5 - Évolution des tableaux de bord SSI

Le suivi des tableaux de bord SSI permet de **vérifier s'ils nécessitent une évolution**, du fait d'une observation parmi les suivantes :

- défaut de qualité des indicateurs (ergonomie, cohérence, pertinence…),
- évolution du contexte,
- évolution des objectifs de sécurité,
- inadéquation des indicateurs par rapport aux objectifs de sécurité,
- changement des destinataires,
- …

Section 2 – Exemple d'application

Un projet pilote concernant un **système de gestion des concours et du personnel** est fourni en annexe du guide d'élaboration des tableaux de bord SSI. Il offre un exemple concret de l'application complète de la démarche.

Les tableaux de bord SSI concernent **une dizaine de destinataires** à différents niveaux opérationnels, fonctionnels et stratégiques en suivant la voie fonctionnelle SSI (haut fonctionnaire de défense, fonctionnaire de sécurité des systèmes d'information, autorité qualifiée responsable de la maîtrise d'ouvrage, autorité qualifiée responsable de la maîtrise d'œuvre, responsable du domaine des réseaux…).

La démarche repose sur une analyse des risques réalisée à l'aide de la méthode EBIOS®. Elle a permis d'identifier **44 objectifs de sécurité** du système et des actions de sécurité ont été déterminées. Par exemple :

- *des règles doivent être définies sur le pare-feu,*
- *des contrôles et audits réguliers doivent avoir lieu sur le pare-feu,*
- *un suivi régulier des activités de contrôle des traces doit être assuré,*
- *des moyens d'analyse des délais d'échanges doivent être mis en place,*
- *le système doit garantir une indisponibilité maximale de 24h,*
- *un suivi des failles sur les systèmes UNIX et Windows NT doit être assuré,*
- *les informations et supports d'information doivent être protégés,*
- *les utilisateurs doivent être sensibilisés (sur politique de sécurité, consignes de protection contre les dégâts des eaux…),*
- *mettre en œuvre un suivi des accès de télémaintenance,*
- *…*

Une fois les acteurs identifiés, les groupes de travail créés, le projet lancé et planifié, des **objectifs mesurables** ont été définis à partir des objectifs de sécurité identifiés. Par exemple :

- *le nombre d'incidents relatifs aux règles du pare-feu (usurpation d'un compte depuis l'extérieur, tentatives d'intrusion, divulgation de mot de passe par écoute sur le réseau, accès malveillant aux commandes d'administration) doit diminuer,*
- *les traces doivent être contrôlées régulièrement,*
- *les personnels techniques doivent être formés,*
- *les utilisateurs doivent être sensibilisés régulièrement,*
- *le nombre d'incidents liés à la gestion et protection des supports magnétiques doit diminuer,*
- *les délais d'échanges doivent être suivis afin de prévenir les saturations,*
- *il ne doit pas exister de compte inutilisé,*
- *la proportion des tâches d'administration réalisées sous le compte ROOT doit être suivie,*
- *le nombre d'échecs de basculement du serveur sur le serveur de secours doit être minimal,*
- *…*

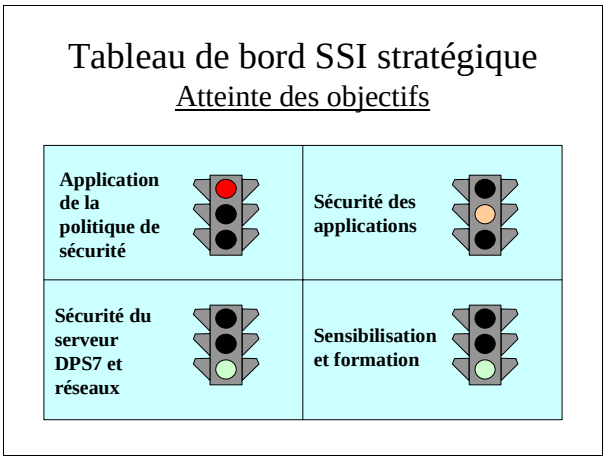
Des **indicateurs** ont été élaborés afin de mesurer ces objectifs mesurables. Seule une partie d'entre eux a été développée dans l'étude de cas. Par exemple :

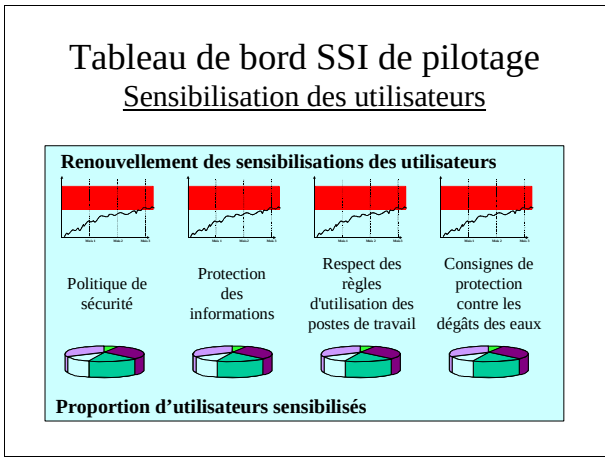
- ***Proportion de traces contrôlées***
  - *Calcul : Volume des traces contrôlées x 100 / volume des traces*
  - *Valeur cible : 100%*
  - *Représentations graphiques proposées :*
    - *Répartition sectorielle (traces contrôlées, traces non contrôlées)*
    - *Historique : courbe d'évolution quantitative (proportion de traces contrôlées)*

- ***Évolution du nombre de comptes inutilisés***
  - *Calcul : Nombre de comptes inutilisés*
  - *Valeur cible : 0*
  - *Représentation graphique proposée :*
    - *Historique : courbe d'évolution quantitative (nombre de comptes inutilisés)*

- ***Renouvellement des sensibilisations et informations des personnels techniques***
  - *Calcul : Somme des délais écoulés depuis la dernière sensibilisation ou information de chaque personnel technique / nombre de personnels techniques*
  - *Valeur seuil : délai moyen maximal à fixer*
  - *Représentation graphique proposée :*
    - *Historique : courbe d'évolution quantitative (moyenne des délais écoulés depuis la dernière sensibilisation ou formation des personnels techniques)*

Les indicateurs élaborés sont ensuite décrits précisément sous la forme de fiches et de procédures d'alimentation. Ils sont enfin regroupés en **tableaux de bord SSI** thématiques. Leurs procédures d'alimentation sont définies, les tableaux de bord SSI font l'objet d'une validation et sont enfin exploités. Voici deux exemples de maquettes validées :





Les tableaux de bord SSI ainsi constitués seront régulièrement révisés afin d'intégrer les évolutions du contexte, de nouveaux objectifs et les ajustements demandés.

Section 3 – Proformae

Des fiches sont fournies en annexe du guide afin de faciliter le travail d'élaboration des tableaux de bord SSI. Elles permettent de **recueillir progressivement les renseignements nécessaires au déroulement de la démarche**.

Les proformae fournis sont les suivants :

- *Destinataires des tableaux de bord SSI* : permet d'identifier les destinataires, les utilisations prévues et périodicités souhaitées.

- *Documents relatifs aux objectifs de sécurité* : permet d'identifier les documents où sont formalisés les objectifs de sécurité ou équivalents.

- *Documents relatifs aux objectifs de progression de SSI* : permet d'identifier les documents où sont formalisés les objectifs de progression de la SSI (plan d'action…).

- *Système d'information* : permet d'identifier le référentiel relatif au système d'information.

- *Planning initial* : permet de présenter le planning détaillé du projet d'élaboration de tableaux de bord SSI

- *Formalisation des objectifs mesurables* : permet de transcrire les objectifs de sécurité et de progression de la SSI en objectifs mesurables.

- *Sélection des éléments de mesure* : permet d'identifier les points-clés et les données exploitables pour chaque objectif mesurable.

- *Élaboration des indicateurs* : permet une première spécification des indicateurs.

- *Constitution des tableaux de bord SSI* : permet une première spécification des tableaux de bord SSI à partir des indicateurs.

- *Fiche descriptive d'indicateur* : permet de spécifier synthétiquement un indicateur (fond, forme, interprétation…).

- *Procédure d'alimentation d'indicateur* : permet de formaliser synthétiquement les renseignements concernant la production et la diffusion de chaque indicateur.

- *Procédure d'alimentation de tableau de bord SSI* : permet de formaliser synthétiquement les renseignements concernant la production et la diffusion de chaque tableau de bord SSI.

Charges de travail et coûts récurrents : permet d'identifier les ressources nécessaires à l'élaboration des tableaux de bord SSI.