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

Élaboration de tableaux de bord SSI

TDBSSI

SECTION 2
EXEMPLE D'APPLICATION

Version du 5 février 2004

51 boulevard de Latour-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

Table des matières

Introduction

Ce document constitue la section 2 du guide "Élaboration de tableaux de bord SSI".

Il présente une étude de cas qui suit la démarche d'élaboration des tableaux de bord SSI.

Un ministère a mené une étude de sécurité sur l'un de ses systèmes d'information (noté SYSTÈME) à l'aide de la méthode EBIOS. À l'issue de cette étude, un plan de recommandation a été élaboré. Il regroupe 42 actions dont l'application est accompagnée par une "charte de sécurité" cosignée par le directeur du personnel et le directeur des affaires financières et de l'administration générale.

En partenariat avec la direction centrale de la sécurité des systèmes d'information (DCSSI), le ministère participe au projet pilote d'élaboration de tableaux de bord SSI sur le système d'information en question. Cette démarche permettra de pérenniser les actions mises en œuvre et la gestion continue de la sécurité.

L'étude formalise ce projet en suivant la démarche préconisée dans la section 1 du guide "Élaboration de tableaux de bord SSI".

Étape 1 – pré-requis

Tâche 1 - Identification des destinataires des tableaux de bord SSI

La voie fonctionnelle SSI d'un ministère jusqu'au système étudié constitue la liste des destinataires potentiels des tableaux de bord SSI.

Ceci permet de remplir les deux premières colonnes du tableau relatif aux destinataires des tableaux de bord SSI figurant en bas de page.

Tâche 2 - Utilisation prévue des tableaux de bord SSI

Le choix des indicateurs dépendra du type d'utilisation prévue.

Cette tâche consiste à remplir la troisième colonne du tableau relatif aux destinataires des tableaux de bord SSI figurant en bas de page.

Tâche 3 - Expression de la périodicité souhaitée du tableau de bord SSI

La périodicité souhaitée d'un tableau de bord doit être définie avant sa conception de manière à ce que le choix des indicateurs y soit adapté

Cette tâche consiste à remplir la dernière colonne du tableau suivant.

Destinataires des tableaux de bord SSI			
Poste	Niveau d'utilisation	Utilisation prévue	Périodicité souhaitée
Haut fonctionnaire de défense et Fonctionnaire de sécurité des systèmes d'information	Stratégique	Point de situation permettant d'examiner un différentiel	1 an
Autorité qualifiée responsable de la maîtrise d'ouvrage	Stratégique et pilotage	Aide à la décision	6 mois
Autorité qualifiée responsable de la maîtrise d'œuvre	Stratégique et pilotage	Aide à la décision	1 mois
Responsable de la maîtrise d'ouvrage du sous-système PERSONNEL	Pilotage	Justification des moyens à accorder	1 mois
Responsable de la maîtrise d'ouvrage du sous-système CONCOURS	Pilotage	Justification des moyens à accorder	1 mois
Responsable de la maîtrise d'ouvrage du sous-système LIQUID	Pilotage	Justification des moyens à accorder	1 mois
Responsable de la maîtrise d'œuvre du système SYSTÈME	Opérationnel	Mesure de la performance en termes de SSI	1 semaine
Responsable de la maîtrise d'œuvre du domaine des systèmes	Opérationnel	Mesure de la performance en termes de SSI	1 semaine
Responsable du domaine des réseaux	Opérationnel	Mesure de la performance en termes de SSI	1 semaine
Responsable du domaine de la logistique	Opérationnel	Mesure de la performance en termes de SSI	1 semaine

Tâche 4 - Disponibilité des objectifs de sécurité

Les objectifs de sécurité sont issus d'une étude EBIOS du système étudié. Celle-ci a permis de rationaliser le contexte, les besoins de sécurité, les risques et les objectifs de sécurité qui les couvrent. De ce fait, les indicateurs qui en découleront seront parfaitement adaptés au système.

Documents relatifs aux objectifs de sécurité		
Nom	Référence	Emplacement
Plan d'action	Plan d'action v2.1	Cédérom "Étude de sécurité du système d'information" édité par le prestataire
Charte de sécurité (document d'accompagnement)	Charte de sécurité pour l'hébergement du système SYSTÈME v3.3	Ressource partagée

Tâche 5 - Disponibilité des objectifs de progression de SSI

Certains objectifs de sécurité ne sont pas immédiatement couverts par des mesures de sécurité. En effet, des contraintes budgétaires, techniques et conjoncturelles ne permettent pas toujours de les réaliser à court terme. Par ailleurs, l'impact plus ou moins important des actions de sécurité sur les risques qu'elles couvrent permet aussi de hiérarchiser les priorités.

Pour le système SYSTÈME, un plan d'action a été défini de manière à prévoir sur un calendrier la mise en œuvre progressive des mesures de sécurité.

Une échelle de priorité de 1 à 4 y est présentée :

1. une priorité 4 indique que l'action doit être menée en priorité, compte tenu de son effet en réduction d'un risque grave ;
2. une priorité 3 indique que l'action accompagne une action de priorité 4, par exemple, les actions d'audit accompagnent la mise en place de moyens de contrôle d'accès ou de sauvegarde ;
3. une priorité 2 indique une action de mise en cohérence, à mener une fois que les actions de priorité 4 et 3 ont été mises en place ;
4. une priorité 1 indique une action complémentaire de sécurité qui n'est pas à mener immédiatement car les risques couverts n'ont pas un impact important.

Documents relatifs aux objectifs de progression de SSI		
Nom	Référence	Emplacement
Plan d'action	Plan d'action v2.1	Cédérom "Étude de sécurité du système d'information SYSTÈME"

Tâche 6 - Connaissance du système d'information ciblé

L'essentiel des renseignements collectés est issu de l'étude du contexte définie par la méthode EBIOS, de la documentation existante et des interviews sur les domaines concernés. Ces informations permettent d'obtenir une bonne compréhension du système, de ses enjeux et de ses évolutions.

Le périmètre de l'étude couvre l'ensemble du système SYSTÈME, soit :

- la gestion des concours (sous-système CONCOURS) ;
- la gestion du personnel (sous-système PERSONNEL) ;
- la gestion de la pre-liquidation de la LIQUID (sous-système LIQUID).

Le tableau suivant présente les contacts et documents utiles à la connaissance du système.

Système d'information		
CONTACTS		
Poste	Périmètre couvert	
Chef de projet Tableaux de bord SSI / coordinateur	Ensemble du projet	
Selon les besoins, le chef de projet pourra faire appel au responsable de la maîtrise d'ouvrage du sous-système PERSONNEL	Gestion du personnel	
Selon les besoins, le chef de projet pourra faire appel au responsable de la maîtrise d'ouvrage du sous-système CONCOURS	Gestion centrale des concours et examens	
Selon les besoins, le chef de projet pourra faire appel au responsable de la maîtrise d'ouvrage du sous-système LIQUID	Pré-liquidation de la paye	
Selon les besoins, le chef de projet pourra faire appel au responsable de la maîtrise d'œuvre du système SYSTÈME	Ensemble du système	
DOCUMENTATION		
Nom	Référence	Emplacement
Schéma directeur du ministère	Schéma directeur du ministère	Ressource partagée
Étude EBIOS du système SYSTÈME	Note initiale de prise de connaissance v1.1	Cédérom "Étude de sécurité du système d'information SYSTÈME"

Tâche 7 - Connaissance des possibilités d'obtention de données sources

Une liste de personnes susceptibles de participer à la collecte des données utiles à la mise en œuvre de tableaux de bord SSI est dressée sans pour autant être exhaustive :

- le responsable de l'exploitation des plates-formes informatiques pour le système SYSTÈME,
- le responsable de la gestion des réseaux,
- le responsable de la gestion des serveurs NT,
- le responsable de la cellule d'exploitation SYSTÈME,
- le responsable de la cellule bureautique, de la gestion des postes.

L'ensemble de ces personnes est en mesure d'intervenir dans le cadre du projet.

Tâche 8 - Prise en compte de la dimension budget et moyens

Un budget a été alloué pour les phases de définition, de mise en œuvre et d'exploitation (alimentation) des tableaux de bord SSI. Un budget supplémentaire pourra être alloué pour une phase d'automatisation après une période d'essai.
Les moyens adéquats (personnels intervenant dans le cadre du projet et matériels nécessaires à l'alimentation, au calcul et à l'édition des tableaux de bord) ont été rendus disponibles.

→ La validation de l'étape est assurée par :

- les personnes en charge de la préparation du projet de tableaux de bord SSI,
- les destinataires des tableaux de bord SSI,
- la personne en charge de la prise en compte des objectifs de sécurité au sein du système étudié,
- les interlocuteurs fonctionnels et techniques du système étudié,
- les responsables du budget pour l'évolution et le fonctionnement du système étudié.

→ À l'issue de la première étape, une **synthèse des prérequis** est rédigée. Celle-ci présente l'ensemble des éléments recueillis dans les 8 tâches de l'étape.

Étape 2 – Mise en place du projet tableau de bord SSI

Tâche 1 - Identification et mobilisation des acteurs

L'ensemble des acteurs (destinataires, acteurs sécurité, acteurs système d'information, acteurs financiers,) a été identifié.

Une information sera réalisée afin de les sensibiliser aux objectifs, à l'utilisation, à l'intérêt et aux enjeux pour l'organisme des tableaux de bord SSI.

Un **annuaire des acteurs** sera créé et des **supports de communication** spécifiques à chaque type d'acteur seront réalisés et diffusés par différents vecteurs.

Tâche 2 - Constitution des groupes de travail

D'une part, le chef de projet Tableaux de bord SSI assurera la coordination entre les groupes, et l'animation de ceux ci.

D'autre part, des groupes de travail ont été constitués.

- Groupe de travail "utilisation"

  Associé à toutes les étapes fonctionnelles du projet, le groupe de travail « utilisation » s'assure que les tableaux de bord SSI élaborés correspondent aux besoins fonctionnels identifiés et qu'ils sont d'une utilisation aisée.

  Il regroupe des destinataires, des acteurs sécurité au niveau fonctionnel et la maîtrise d'ouvrage.

  Ce groupe est composé des personnes suivantes :
  - sous-directeur,
  - chefs de bureau,
  - responsables d'unités,
  - chef de projet maîtrise d'ouvrage,
  - chef de projet Tableaux de bord SSI.

- Groupe de travail "technique"

  Associé à toutes les étapes en relation avec l'aspect technique du système d'information, le groupe de travail « technique » s'assure de la faisabilité des tableaux de bord ainsi que de leur pertinence par rapport aux réalités techniques du système d'information.

  Il regroupe des acteurs système d'information, des acteurs sécurité ainsi que la maîtrise d'œuvre.

  Ce groupe est composé des personnes suivantes :
  - pôle d'exploitation du système d'information,
  - responsable systèmes et d'exploitation,
  - responsable des serveurs,
  - responsable réseaux,
  - chef de projet Tableaux de bord SSI.

- Groupe de travail "pilotage"

  Associé au suivi du projet d'élaboration des tableaux de bord SSI, le groupe de travail « pilotage » s'assure aussi de la maîtrise des coûts et des charges récurrents associés aux tableaux de bord SSI en phase de production.

  Il regroupe des représentants de la hiérarchie, des acteurs budgétaires, ainsi que la maîtrise d'œuvre et la maîtrise d'ouvrage.

  Ce groupe est composé des personnes suivantes :
  - sous-directeur,
  - chefs de bureau,
  - responsables d'unités,
  - FSSI,
  - chef de projet Tableaux de bord SSI.

- Groupe de travail "exploitation"

  Regroupant des représentants des acteurs impliqués dans la phase de production du projet tableaux de bord de sécurité, le groupe de travail « 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.

  Il regroupe des représentants des acteurs système d'information ainsi que des représentants des destinataires.

  Ce groupe est composé des personnes suivantes :
  - pôle d'exploitation du système d'information,
  - responsable systèmes et d'exploitation,
  - responsable des serveurs,
  - responsable réseaux,
  - maîtrise d'ouvrage,
  - chef de projet Tableaux de bord SSI.

Enfin, un planning initial pour le projet a été élaboré (l'assistance d'un prestataire externe est un facteur de diminution des durées) :

Planning initial							
Phase du projet	Intitulé	Date de début	Date de fin	Avancement	Documents résultats		
					Intitulé	Référence	Emplacement
E1-T1 à T8	Vérification des pré-requis	J	J+2 semaines	100%	Synthèse des prérequis	SYSTÈME-PREREQUIS v1.0	Ressource partagée
E2-T1 et T2	Mise en place du projet Tableau de bord SSI	J+1 semaine	J+3 semaines	100%	Note de cadrage	SYSTÈME-LANCEMENT v1.0	Ressource partagée

Planning initial							
Phase du projet	Intitulé	Date de début	Date de fin	Avancement	Documents résultats		
					Intitulé	Référence	Emplacement
E3-T1	Formalisation des objectifs mesurables	J+3 semaines	J+4 semaines	0%	Synthèse des objectifs mesurables	SYSTÈME-OBJECTIFS v1.0	Ressource partagée
E3-T2	Sélection des éléments de mesure	J+4 semaines	J+5 semaines	0%	Synthèse des éléments de mesure	SYSTÈME-SOURCES v1.0	Ressource partagée
E3-T3	Élaboration des indicateurs	J+5 semaines	J+7 semaines	0%	Synthèse des indicateurs	SYSTÈME-INDICATEURS v1.0	Ressource partagée
E3-T4	Constitution des tableaux de bord SSI	J+7 semaines	J+10 semaines	0%	Synthèse des tableaux de bord SSI	SYSTÈME-TDB v1.0	Ressource partagée
E3-T5	Élaboration des procédures d'alimentation	J+10 semaines	J+11 semaines	0%	Synthèse des procédures d'alimentation	SYSTÈME-ALIM v1.0	Ressource partagée
E3-T6	Validation des tableaux de bord SSI	J+11 semaines	J+13 semaines	0%	Note de validation	SYSTÈME-VALID v1.0	Ressource partagée

→ La validation de l'étape est assurée par les personnes en charge de la préparation du projet de tableaux de bord SSI.

→ À l'issue de la seconde étape, une **note de cadrage** est rédigée. Celle-ci formalise l'ensemble des éléments des 2 tâches de l'étape.

Étape 3 – Élaboration des tableaux de bord

Tâche 1 - Formalisation des objectifs mesurables

Les objectifs de sécurité utilisés sont constitués de l'ensemble des actions préconisées à la suite de l'étude SSI. Les actions sont réparties en domaines et ne sont pas forcément homogènes en termes de précision et d'interprétation. La transcription de ces actions en objectifs exploitables pour un tableau de bord nécessite donc de lever les ambiguïtés en affinant les actions, en les rendant mesurables et en privilégiant l'aspect représentatif du phénomène que l'on souhaite observer.

Le tableau des pages suivantes présente la formalisation des objectifs mesurables.

Remarques :

- les objectifs et actions de sécurité sont issus du plan d'action et de la charte de sécurité, ils reposent sur la même numérotation dans ce document ;

- le plan d'action proposé par le prestataire ayant effectué l'étude de sécurité n'ayant pas encore donné lieu à un plan d'action détaillé (ordonnancement, ressources allouées…) validé par la hiérarchie du ministère, les valeurs ciblées correspondent majoritairement à la fin des actions et ne comportent pas d'indications de durée ; en effet, il est important de considérer deux projets distincts ; dans le projet Tableaux de bord SSI, les groupes de travail ne peuvent pas prendre de décision relatives aux actions SSI ;

- certains objectifs ou actions de sécurité ne peuvent se décliner sous la forme d'objectifs mesurables ; généralement, un audit permet de vérifier que les actions correspondantes sont bien mises en œuvre ;

- certains objectifs ou actions de sécurité sont volontairement écartés de l'étude ; en effet, il peut avoir été décidé qu'un objectif de sécurité ne serait pas traité, les solutions choisies pour couvrir l'objectif de sécurité ou les entités concernées (matériels, logiciels, réseaux…) par l'objectif de sécurité peuvent avoir évolué, ce qui rend l'objectif obsolète…

Formalisation des objectifs mesurables			
N°	Objectifs ou actions de sécurité	Objectifs mesurables	Valeurs seuils et cibles
1	Politique de sécurité – Formaliser et valider une politique de sécurité des applications	- Pas d'objectif mesurable -	
2	Politique de sécurité – Définir les règles de protection des mots de passe pour les différents systèmes	- Pas d'objectif mesurable -	
3	Politique de sécurité – Définir et mettre en œuvre des règles sur le firewall régissant tout accès au réseau depuis l'extérieur et restreindre les connexions depuis le réseau local par les commutateurs en fonction des besoins de l'utilisateur principal du poste de travail	Le nombre d'incidents que le firewall doit couvrir (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 Le nombre d'incidents que les commutateurs doivent couvrir (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	0 0
4	Politique de sécurité – Formaliser et valider une politique d'audit SSI : responsabilités liées aux audits de sécurité et règles générales de production et d'analyse des traces	- Pas d'objectif mesurable -	
5	Politique de sécurité – Formaliser et valider une politique d'audit SSI : champ des audits de la sécurité des applications	- Pas d'objectif mesurable -	
6	Politique de sécurité – Formaliser et valider une politique d'audit SSI : champ des audits des accès réseaux depuis l'extérieur	- Pas d'objectif mesurable -	
7	Politique de sécurité – Mettre en place un suivi régulier des activités de contrôle des traces et des incidents détectés sous la forme de bilans diffusés aux responsables de l'audit	Les traces doivent être contrôlées régulièrement Les incidents doivent être contrôlés régulièrement	100% 100%
8	Politique de sécurité – Élaborer un plan de sensibilisation / formation à la sécurité : formation approfondie du personnel technique et des équipes d'exploitation de la maîtrise d'œuvre	Les personnels techniques doivent être formés Les personnels techniques doivent être régulièrement sensibilisés / informés	100% Pas de valeur ciblée
9	Politique de sécurité – Élaborer un plan de sensibilisation / formation à la sécurité : sensibilisation des utilisateurs	Les utilisateurs doivent être sensibilisés régulièrement (politique de sécurité)	Pas de valeur ciblée

Formalisation des objectifs mesurables			
N°	Objectifs ou actions de sécurité	Objectifs mesurables	Valeurs seuils et cibles
10	Protection des informations – Définir une classification des informations et les règles de stockage et de diffusion associées, former les gestionnaires à l'application des règles associées à la classification et assister les propriétaires dans le classement des informations, identifier les fichiers stockés sur les serveurs contenant des informations sensibles au sens de la classification définie et vérifier les habilitations définies sur ces fichiers et attribuées aux utilisateurs, identifier les propriétaires des fichiers et informer l'équipe système des besoins de protection des fichiers identifiés comme sensibles et du respect des règles de sécurité	- Objectif écarté (non traité) -	
11	Protection des informations – Élaborer les règles et une procédure complète de gestion et de protection des supports d'information : protection des supports papier	- Pas d'objectif mesurable -	
12	Protection des informations – Élaborer les règles et une procédure complète de gestion et de protection des supports d'information : protection des éditions papier	Les utilisateurs doivent être sensibilisés régulièrement (protection des informations)	Pas de valeur ciblée
13	Protection des informations – Élaborer les règles et une procédure complète de gestion et de protection des supports d'information : gestion et protection des supports magnétiques	Le nombre d'incidents liés à la gestion et protection des supports magnétiques doit diminuer	0
14	Sécurité des applications – LIQUID : rédiger une procédure permettant le contrôle de la saisie des paramètres de la réglementation à partir des mises à jour fournies par la paierie	- Objectif écarté (évolution du contexte) -	
16	Sécurité des applications – CONCOURS : vérifier que les fichiers des notes ne sont pas accessibles par les utilisateurs via DXE et mettre en place une procédure de contrôle de l'intégrité des fichiers téléchargés avant leur intégration dans l'application	- Objectif écarté (évolution du contexte) -	
18	Sécurité des applications – CONCOURS : mettre en place une procédure de téléchargement FTP garantissant que le téléchargement d'un fichier ne peut pas écraser un ancien fichier	- Objectif écarté (évolution du contexte) -	
19	Sécurité des applications – PERSONNEL : modifier l'application pour prendre en compte la chronologie des informations échangées et éviter des erreurs de mises à jour provenant de l'importation de deux fichiers d'un même service déconcentré	Le nombre d'erreurs de mises à jour provenant de l'importation de deux fichiers d'un même service déconcentré doit diminuer	Pas de valeur ciblée

Formalisation des objectifs mesurables			
N°	Objectifs ou actions de sécurité	Objectifs mesurables	Valeurs seuils et cibles
20	Sécurité des applications – PERSONNEL : définir des moyens d'analyse des délais d'échange et suivre la progression des périodes d'échanges afin d'anticiper un dysfonctionnement du processus	Les délais d'échanges doivent être suivis afin de prévenir les saturations	Pas de valeur ciblée
21	Sécurité des applications – PERSONNEL : formaliser une procédure dégradée des échanges entre PERSONNEL et le système de gestion des bases lors du rechargement de l'une des bases à partir d'une sauvegarde de la veille	- Pas d'objectif mesurable -	
22	Sécurité des applications – PERSONNEL : formaliser une procédure dégradée de mise à jour des informations (pour lesquelles les accusés réceptions n'ont pas été reçus)	- Pas d'objectif mesurable -	
23	Sécurité des applications – PERSONNEL : vérifier que le réseau RSX garantit une indisponibilité des échanges inférieure à 24 heures	L'indisponibilité des échanges du réseau du sous-système PERSONNEL ne doit pas être supérieure à 24h L'intervention des prestataires de maintenance du réseau du sous-système PERSONNEL doit être effectuée sous 4h	24h max 4h max
24	Sécurité des applications – Procédure de reprise : formaliser une procédure pour chaque application permettant la reconstruction des données de la veille en cas de reprise du serveur DPS à partir d'une sauvegarde	- Pas d'objectif mesurable -	
25	Sécurité des postes de travail et du réseau local – Formaliser des règles de protection des accès aux postes de travail et de l'environnement Bureautique sur le serveur du réseau local	- Pas d'objectif mesurable -	
26	Sécurité des postes de travail et du réseau local – Formaliser des règles d'utilisation des postes de travail et sensibiliser les utilisateurs au respect des règles d'utilisation des postes de travail	Les utilisateurs doivent être sensibilisés régulièrement (respect des règles d'utilisation des postes de travail)	Pas de valeur ciblée
27	Sécurité des postes de travail et du réseau local – Inventorier les postes de travail équipés de modem et vérifier que la configuration du micro-ordinateur ne permet pas d'utiliser le modem en réception	- Objectif écarté (évolution du contexte) -	

Formalisation des objectifs mesurables			
N°	Objectifs ou actions de sécurité	Objectifs mesurables	Valeurs seuils et cibles
28	Sécurité des postes de travail et du réseau local – Organiser un suivi des nouvelles failles connues des systèmes UNIX et Windows NT et identifier leurs impacts ; relever les risques pertinents et mettre en œuvre les mesures de sécurité recommandées	La quantité de failles traitées doit être suivie par système et source d'information	Pas de valeur ciblée
29	Sécurité des postes de travail et du réseau local – Formaliser et contrôler les règles de sécurité mises en œuvre sur le firewall	- Pas d'objectif mesurable -	
30	Sécurité des postes de travail et du réseau local – Appliquer une procédure de contrôle et d'audit régulier de la configuration du firewall ; définir les règles et les moyens de journalisation et d'analyse des traces sur le firewall	Les contrôles et audits sur le firewall doivent être réguliers Les traces doivent être analysées Les incidents de sécurité dont des traces apparaissent dans la journalisation doivent être détectés dans l'analyse des traces	Pas de valeur ciblée Pas de valeur ciblée 0%
31	Sécurité du serveur DPS et réseau – Formaliser les procédures de gestion des comptes utilisateurs	Il ne doit pas exister de compte inutilisé	0
32	Sécurité du serveur DPS et réseau – Contrôler que l'utilisation des privilèges du compte ROOT est nécessaire pour réaliser les tâches d'administration courantes et attribuer un compte personnel à chaque administrateur. Les privilèges de ces comptes seront attribués selon les besoins de chaque administrateur pour l'exécution de sa tâche	La proportion des tâches d'administration réalisées sous le compte ROOT doit être suivie	Pas de valeur ciblée
33	Sécurité du serveur DPS et réseau – Appliquer les règles de gestion des accès définies dans la Politique de Sécurité	- Pas d'objectif mesurable -	
34	Sécurité du serveur DPS et réseau – Définition d'une solution technique pour empêcher la réattribution d'une adresse sur la passerelle	- Pas d'objectif mesurable -	
35	Sécurité du serveur DPS et réseau – Formaliser et mettre en œuvre un suivi et les mécanismes de protection des accès de télémaintenance	Les accès de télémaintenance doivent faire l'objet de mécanismes de protection	100%
36	Sécurité du serveur DPS et réseau – Définir des consignes de sécurité pour les interventions de télémaintenance afin de réaliser une reprise du serveur en cas d'anomalie se produisant pendant l'intervention	- Objectif écarté (évolution du contexte) -	

Formalisation des objectifs mesurables			
N°	Objectifs ou actions de sécurité	Objectifs mesurables	Valeurs seuils et cibles
37	Sécurité du serveur DPS et réseau – Le serveur SERV doit être intégré au plan de secours ; les procédures de secours devront être testées notamment pour le SERV afin de s'assurer que le rechargement d'une sauvegarde sur une machine différente (serveur disponible dans le plan de secours) permet la reprise de l'activité	Le nombre d'échecs de basculement du serveur sur le serveur de secours doit être minimal	Pas de valeur ciblée
38	Sécurité du serveur DPS et réseau – Formaliser les actions à entreprendre en cas d'anomalie détectée sur une sauvegarde	Les anomalies sur les sauvegardes doivent être suivies	Pas de valeur ciblée
39	Sécurité physique – Formaliser une procédure à appliquer lors du départ d'un agent permettant de désactiver ses accès physiques (badge d'accès au bâtiment et aux locaux informatiques) et ses accès logiques (suppression des comptes lui appartenant sur les différents systèmes, la messagerie et réseau local) ; désigner un responsable de la gestion de ces accès, centraliser l'attribution des habilitations d'accès aux locaux informatiques et aux salles hébergeant les serveurs, informer le service de sécurité du Ministère de la mise en place de cette procédure et réaliser des inventaires réguliers des autorisations attribuées pour accéder aux locaux hébergeant les serveurs ; prévoir une procédure d'alerte du responsable de la sécurité des locaux hébergeant les serveurs en cas de détection de toute alarme	Les agents ayant quitté l'établissement doivent rendre leur badge d'accès et voir leur compte utilisateur supprimé Les habilitations d'accès aux locaux informatiques et aux salles hébergeant les serveurs doivent être valides	0% 0%
40	Sécurité physique – Formaliser et appliquer des consignes de protection des matériels en cas d'intervention de personnel extérieur	- Pas d'objectif mesurable -	
41	Sécurité physique – Modifier l'emplacement de la porte d'accès de la salle hébergeant les serveurs de manière à ce que les pupitreurs puissent surveiller les personnes accédant à cette salle	- Pas d'objectif mesurable -	
42	Sécurité physique – Protection Incendie dans la salle hébergeant les serveurs	- Objectif écarté (prise en charge indépendante par les pompiers et services logistiques) -	

Formalisation des objectifs mesurables			
N°	Objectifs ou actions de sécurité	Objectifs mesurables	Valeurs seuils et cibles
43	Sécurité physique – Vérifier que des gouttières sont installées sous toutes les canalisations présentes dans les faux plafonds de la salle hébergeant les serveurs et l'existence de détecteur de présence d'eau sous les climatiseurs, dans les gouttières sous les canalisations des faux plafonds ; mettre en place une procédure périodique de test des détecteurs de présence d'eau (une fois par an)	- Objectif écarté (prise en charge indépendante par les pompiers et services logistiques) -	
44	Sécurité physique – Formaliser des consignes de protection contre les dégâts des eaux et sensibiliser les agents aux consignes de protection contre les dégâts des eaux	Les agents doivent être sensibilisés régulièrement (consignes de protection contre les dégâts des eaux)	Pas de valeur ciblée

→ La validation de la tâche est assurée par les groupes de travail "utilisation" et "technique".

→ À l'issue de cette tâche, une **synthèse des objectifs mesurables** est rédigée.

Tâche 2 - Sélection des éléments de mesure

Le tableau suivant complète les objectifs mesurables par la sélection des éléments de mesure

Remarques :

- la première colonne indique le numéro de l'objectif mesurable ;
- afin de simplifier l'étude de cas, **seule une partie des objectifs mesurables est développée**.

Sélection des éléments de mesure					
N°	Objectifs mesurables	Valeurs seuils et cibles	Points-clés et paramètres	Données et sources des données	Objectifs ou actions de sécurité
1	Les traces doivent être contrôlées régulièrement	100%	Contrôle des traces	Journaux systèmes, du firewall…	7
2	Les personnels techniques doivent être formés	100%	Formation des personnels techniques	Activité des personnels techniques	8
3	Les personnels techniques doivent être régulièrement sensibilisés / informés	Pas de valeur ciblée	Régularité des sensibilisations / informations des personnels techniques	Activité des personnels techniques	8
4	Les utilisateurs doivent être sensibilisés régulièrement (politique de sécurité)	Pas de valeur ciblée	Sensibilisation des utilisateurs (politique de sécurité) Régularité des sensibilisations / informations (politique de sécurité)	Activité des utilisateurs	9
5	Les utilisateurs doivent être sensibilisés régulièrement (protection des informations)	Pas de valeur ciblée	Sensibilisation des utilisateurs (protection des informations) Régularité des sensibilisations / informations (protection des informations)	Activité des utilisateurs	12
6	L'indisponibilité des échanges du réseau du sous-système PERSONNEL ne doit pas être supérieure à 24h	24h max	Durée d'indisponibilité des échanges du réseau du sous-système PERSONNEL	Rapports d'intervention	23
7	L'intervention des prestataires de maintenance du réseau du sous-système PERSONNEL doit être effectuée sous 4h	4h max	Délai d'intervention des prestataires de maintenance du réseau du sous-système PERSONNEL	Rapports d'intervention	23

Sélection des éléments de mesure					
N°	Objectifs mesurables	Valeurs seuils et cibles	Points-clés et paramètres	Données et sources des données	Objectifs ou actions de sécurité
8	Les utilisateurs doivent être sensibilisés régulièrement (respect des règles d'utilisation des postes de travail)	Pas de valeur ciblée	Sensibilisation des utilisateurs (respect des règles d'utilisation des postes de travail) Régularité des sensibilisations / informations (respect des règles d'utilisation des postes de travail)	Activité des utilisateurs	26
9	Il ne doit pas exister de compte inutilisé	0	Comptes inutilisés	Fichiers système	31
10	Les agents doivent être sensibilisés régulièrement (consignes de protection contre les dégâts des eaux)	Pas de valeur ciblée	Sensibilisation des utilisateurs (consignes de protection contre les dégâts des eaux) Régularité des sensibilisations / informations (consignes de protection contre les dégâts des eaux)	Activité des utilisateurs	44
…	…	…	…	…	…

→ La validation de la tâche est assurée par le groupe de travail "technique".

→ À l'issue de cette tâche, une **synthèse des éléments de mesure** est rédigée.

Tâche 3 - Élaboration des indicateurs

Chaque indicateur est décrit dans les tableaux suivants. Cette première description permet de préciser le fond (calcul des données, valeurs seuils et cibles, plage de tolérance) et la forme (échelle choisie, représentations graphiques proposées) des indicateurs. Elle permet aussi de prévoir l'utilisation des indicateurs dans des tableaux de bord SSI (périodicité du calcul, tableaux de bord SSI). Le premier tableau présente les indicateurs de base, c'est-à-dire ceux qui sont directement issus des points-clés de la tâche précédente. Le second tableau présente les indicateurs construits à partir des indicateurs de base pour répondre au besoin de remontée d'informations des niveaux opérationnel et de pilotage au niveau stratégique.

Remarques :

- la première colonne indique le numéro de l'indicateur ;
- les indicateurs sont majoritairement issus des points-clés du tableau précédent, mais certains doivent être crées afin de répondre aux besoins des différents destinataires (par exemple, des synthèses d'indicateurs sur un même thème doivent être réalisées) ;
- les valeurs issues du tableau précédent peuvent être différentes (notamment pour les valeurs seuils et cibles) du fait de l'avancement des réflexions sur les indicateurs ;
- les informations relatives aux indicateurs restent prévisionnelles, il s'agit de premières propositions qui pourront être adaptées dans la suite de l'étude, mais il convient de les garder telles quelles afin de disposer d'une traçabilité des réflexions.

Élaboration des indicateurs de base								
N°	Indicateurs	Calcul des données	Valeurs seuils et cibles	Plage de tolérance choisie	Échelle choisie	Représentations graphiques proposées	Périodicité du calcul	Objectifs mesurables
1	Proportion de traces contrôlées	Volume des traces contrôlées x 100 / volume des traces	Cible : 100%	Aucune	De 0 à 100%	Répartition sectorielle (traces contrôlées, traces non contrôlées) Historique : courbe d'évolution quantitative (proportion de traces contrôlées)	1 mois	1
2	Indisponibilité des échanges du réseau du sous-système PERSONNEL	Somme des durées d'indisponibilité des échanges du réseau du sous-système PERSONNEL / nombre d'indisponibilités	Seuil : 24h	Aucune	Selon les valeurs de l'historique	Historique : courbe d'évolution quantitative (moyenne des durées d'indisponibilité)	1 mois	6
3	Évolution du délai d'intervention des prestataires de maintenance du réseau du sous-système PERSONNEL	Somme des délais d'intervention des prestataires de maintenance du réseau du sous-système PERSONNEL / nombre d'interventions	Seuil : 4h	24h	Selon les valeurs de l'historique	Historique : courbe d'évolution quantitative (moyenne des délais d'intervention)	1 mois	7
4	Évolution du nombre de comptes inutilisés	Nombre de comptes inutilisés	Cible : 0	Aucune	Selon les valeurs de l'historique	Historique : courbe d'évolution quantitative (nombre de comptes inutilisés)	1 semaine	9
5	Proportion de personnels techniques formés	Nombre de personnels techniques formés x 100 / nombre de personnels techniques	Cible : 100%	Aucune	De 0 à 100%	Répartition sectorielle (personnels techniques formés, personnels techniques non formés) Historique : courbe d'évolution quantitative (proportion de personnels techniques formés)	6 mois	2

Élaboration des indicateurs de base								
N°	Indicateurs	Calcul des données	Valeurs seuils et cibles	Plage de tolérance choisie	Échelle choisie	Représentations graphiques proposées	Périodicité du calcul	Objectifs mesurables
6	Renouvellement des sensibilisations et informations des personnels techniques	Somme des délais écoulés depuis la dernière sensibilisation ou information de chaque personnel technique / nombre de personnels techniques	Seuil : délai moyen maximal à fixer	Aucune	Selon les valeurs de l'historique	Historique : courbe d'évolution quantitative (moyenne des délais écoulés depuis la dernière sensibilisation ou formation des personnels techniques)	6 mois	3
7	Renouvellement des sensibilisations des utilisateurs (politique de sécurité)	Somme des délais écoulés depuis la dernière sensibilisation (politique de sécurité) de chaque utilisateur / nombre d'utilisateurs	Seuil : délai moyen maximal à fixer	Aucune	Selon les valeurs de l'historique	Historique : courbe d'évolution quantitative (moyenne des délais écoulés depuis la dernière sensibilisation des utilisateurs)	6 mois	4
8	Renouvellement des sensibilisations des utilisateurs (protection des informations)	Somme des délais écoulés depuis la dernière sensibilisation (protection des informations) de chaque utilisateur / nombre d'utilisateurs	Seuil : délai moyen maximal à fixer	Aucune	Selon les valeurs de l'historique	Historique : courbe d'évolution quantitative (moyenne des délais écoulés depuis la dernière sensibilisation des utilisateurs)	6 mois	5
9	Renouvellement des sensibilisations des utilisateurs (respect des règles d'utilisation des postes de travail)	Somme des délais écoulés depuis la dernière sensibilisation (respect des règles d'utilisation des postes de travail) de chaque utilisateur / nombre d'utilisateurs	Seuil : délai moyen maximal à fixer	Aucune	Selon les valeurs de l'historique	Historique : courbe d'évolution quantitative (moyenne des délais écoulés depuis la dernière sensibilisation des utilisateurs)	6 mois	8
10	Renouvellement des sensibilisations des agents (consignes de	Somme des délais écoulés depuis la dernière sensibilisation (consignes de protection contre les dégâts des eaux) de chaque agent /	Seuil : délai moyen maximal à fixer	Aucune	Selon les valeurs de l'historique	Historique : courbe d'évolution quantitative (moyenne des délais écoulés depuis la dernière sensibilisation des agents)	6 mois	10

Élaboration des indicateurs de base								
N°	Indicateurs	Calcul des données	Valeurs seuils et cibles	Plage de tolérance choisie	Échelle choisie	Représentations graphiques proposées	Périodicité du calcul	Objectifs mesurables
	protection contre les dégâts des eaux)	nombre d'agents						
11	Proportion d'utilisateurs sensibilisés (politique de sécurité)	Nombre d'utilisateurs sensibilisés (politique de sécurité) x 100 / nombre d'utilisateurs	Cible : 100%	Aucune	De 0 à 100%	Répartition sectorielle (utilisateurs sensibilisés, utilisateurs non sensibilisés) Historique : courbe d'évolution quantitative (proportion d'utilisateurs sensibilisés)	6 mois	4
12	Proportion d'utilisateurs sensibilisés (protection des informations)	Nombre d'utilisateurs sensibilisés (protection des informations) x 100 / nombre d'utilisateurs	Cible : 100%	Aucune	De 0 à 100%	Répartition sectorielle (utilisateurs sensibilisés, utilisateurs non sensibilisés) Historique : courbe d'évolution quantitative (proportion d'utilisateurs sensibilisés)	6 mois	5
13	Proportion d'utilisateurs sensibilisés (respect des règles d'utilisation des postes de travail)	Nombre d'utilisateurs sensibilisés (respect des règles d'utilisation des postes de travail) x 100 / nombre d'utilisateurs	Cible : 100%	Aucune	De 0 à 100%	Répartition sectorielle (utilisateurs sensibilisés, utilisateurs non sensibilisés) Historique : courbe d'évolution quantitative (proportion d'utilisateurs sensibilisés)	6 mois	8
14	Proportion d'utilisateurs sensibilisés (consignes de protection contre les dégâts des eaux)	Nombre d'utilisateurs sensibilisés (consignes de protection contre les dégâts des eaux) x 100 / nombre d'utilisateurs	Cible : 100%	Aucune	De 0 à 100%	Répartition sectorielle (utilisateurs sensibilisés, utilisateurs non sensibilisés) Historique : courbe d'évolution quantitative (proportion d'utilisateurs sensibilisés)	6 mois	10

Élaboration des indicateurs de base								
N°	Indicateurs	Calcul des données	Valeurs seuils et cibles	Plage de tolérance choisie	Échelle choisie	Représentations graphiques proposées	Périodicité du calcul	Objectifs mesurables
…	…	…	…	…	…	…	…	…

Élaboration des indicateurs complémentaires								
N°	Indicateurs	Calcul des données	Valeurs seuils et cibles	Plage de tolérance choisie	Échelle choisie	Représentations graphiques proposées	Périodicité du calcul	Objectifs mesurables
15	Application de la politique de sécurité	Bilan des tableaux de bord (opérationnels et de pilotage) relatifs à la politique de sécurité (ex. : contrôle des traces)	Cible : OK	Aucune	De "mauvais" à "bon"	Feu tricolore	1 an	1
16	Sécurité des applications	Bilan des tableaux de bord (opérationnels et de pilotage) relatifs à la sécurité des applications (ex. : maintenance PERSONNEL)	Cible : OK	Aucune	De "mauvais" à "bon"	Feu tricolore	1 an	6-7
17	Sécurité du serveur DPS et réseaux	Bilan des tableaux de bord (opérationnels et de pilotage) relatifs à la sécurité du serveur DPS et réseaux (ex. : comptes inutilisés)	Cible : OK	Aucune	De "mauvais" à "bon"	Feu tricolore	1 an	9
18	Sensibilisation et formation	Bilan des tableaux de bord (opérationnels et de pilotage) relatifs à la sensibilisation et formation (ex. : formation des personnels techniques, sensibilisation des utilisateurs)	Cible : OK	Aucune	De "mauvais" à "bon"	Feu tricolore	1 an	2-5, 8, 10
…	…	…	…	…	…	…	…	…

→ La validation de la tâche est assurée par les groupes de travail "technique", "exploitation" et "utilisation".

→ À l'issue de cette tâche, une **synthèse des indicateurs** est rédigée.

Tâche 4 - Constitution des tableaux de bord SSI

La tâche précédente a permis d'identifier différents tableaux de bord SSI.

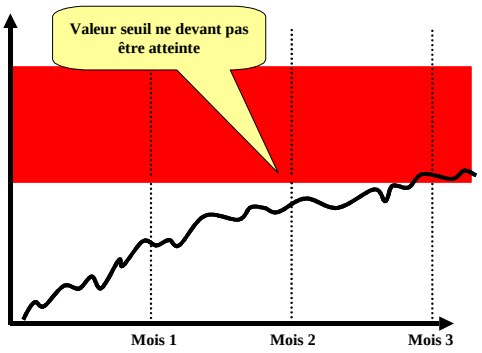
En premier lieu, cette tâche consiste à **revoir les regroupements d'indicateurs afin de créer des tableaux de bord SSI cohérents** en fonction des destinataires et de la périodicité. Nous obtenons les tableaux de bord SSI suivants.

Constitution des tableaux de bord SSI			
Tableaux de bord SSI	Indicateurs	Destinataires	Périodicité
Atteinte des objectifs (stratégique)	15 - Application de la politique de sécurité 16 - Sécurité des applications 17 - Sécurité du serveur DPS et réseaux 18 - Sensibilisation et formation …	- Haut fonctionnaire de défense et Fonctionnaire de sécurité des systèmes d'information - Autorité qualifiée responsable de la maîtrise d'ouvrage - Autorité qualifiée responsable de la maîtrise d'œuvre	1 an
Formation des personnels techniques (pilotage)	5 - Proportion de personnels techniques formés 6 - Renouvellement des sensibilisations et informations des personnels techniques …	- Autorité qualifiée responsable de la maîtrise d'ouvrage - Autorité qualifiée responsable de la maîtrise d'œuvre	6 mois
Contrôle des traces (pilotage)	1 - Proportion de traces contrôlées …	- Autorité qualifiée responsable de la maîtrise d'œuvre - Responsable de la maîtrise d'ouvrage du sous-système PERSONNEL - Responsable de la maîtrise d'ouvrage du sous-système CONCOURS - Responsable de la maîtrise d'ouvrage du sous-système LIQUID	1 mois

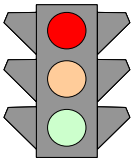
Constitution des tableaux de bord SSI			
Tableaux de bord SSI	Indicateurs	Destinataires	Périodicité
Maintenance PERSONNEL (pilotage)	2 - Indisponibilité des échanges du réseau du sous-système PERSONNEL 3 - Évolution du délai d'intervention des prestataires de maintenance du réseau du sous-système PERSONNEL …	- Autorité qualifiée responsable de la maîtrise d'œuvre - Responsable de la maîtrise d'ouvrage du sous-système PERSONNEL	1 mois
Sensibilisation des utilisateurs (pilotage)	7 - Renouvellement des sensibilisations des utilisateurs (politique de sécurité) 8 - Renouvellement des sensibilisations des utilisateurs (protection des informations) 9 - Renouvellement des sensibilisations des utilisateurs (respect des règles d'utilisation des postes de travail) 10 - Renouvellement des sensibilisations des agents (consignes de protection contre les dégâts des eaux) 11 - Proportion d'utilisateurs sensibilisés (politique de sécurité) 12 - Proportion d'utilisateurs sensibilisés (protection des informations) 13 - Proportion d'utilisateurs sensibilisés (respect des règles d'utilisation des postes de travail) 14 - Proportion d'utilisateurs sensibilisés (consignes de protection contre les dégâts des eaux) …	- Autorité qualifiée responsable de la maîtrise d'ouvrage - Autorité qualifiée responsable de la maîtrise d'œuvre	6 mois

Constitution des tableaux de bord SSI			
Tableaux de bord SSI	Indicateurs	Destinataires	Périodicité
Comptes inutilisés (opérationnel)	4 - Évolution du nombre de comptes inutilisés …	- Responsable de la maîtrise d'œuvre du système SYSTÈME - Responsable de la maîtrise d'œuvre du domaine des systèmes - Responsable du domaine des réseaux - Responsable du domaine de la logistique	1 semaine
…	…	…	…

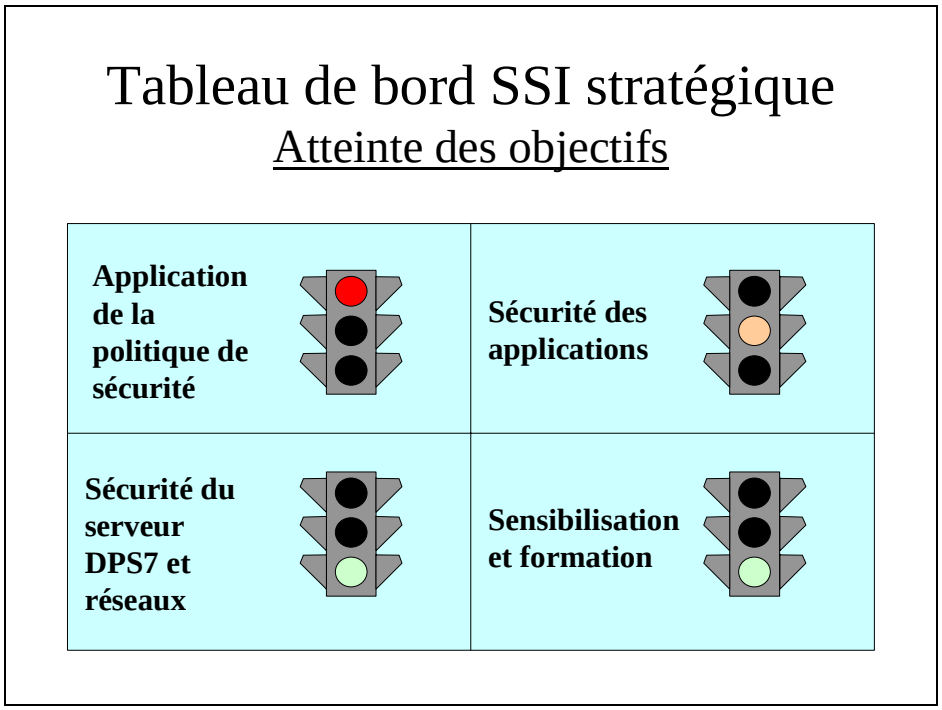
Ensuite, la **description des indicateurs est affinée sous la forme de fiches descriptives**. Deux exemples sont proposés ici.

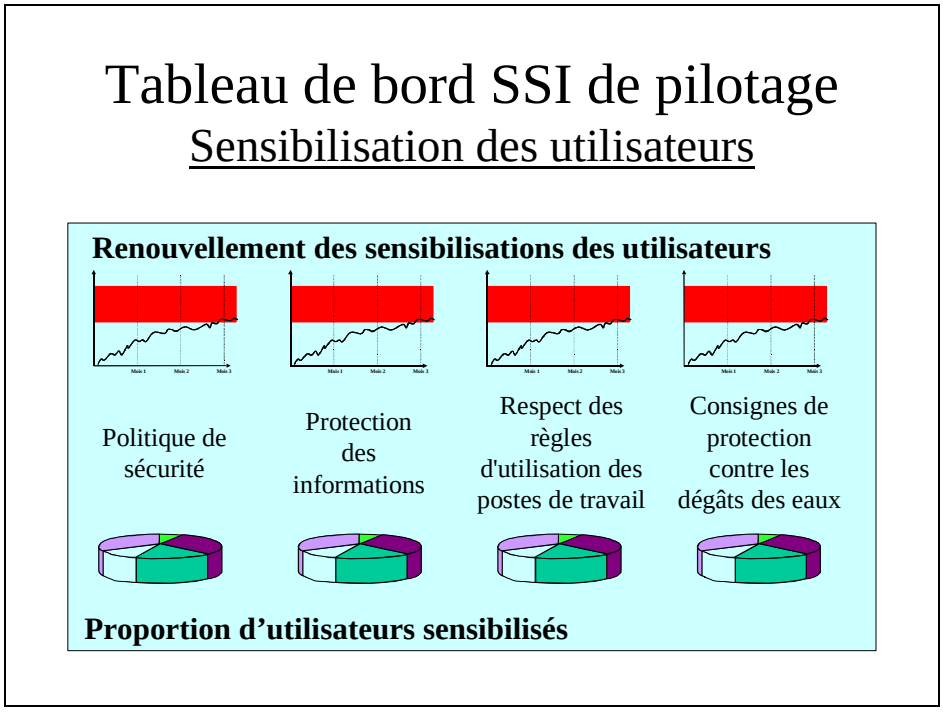
Fiche descriptive d'indicateur	
Libellé	**7 – Renouvellement des sensibilisations des utilisateurs (politique de sécurité)**
Niveau	Pilotage
Objectif(s) mesurable(s)	Les utilisateurs doivent être sensibilisés régulièrement (politique de sécurité)
Valeur(s) significative(s)	Seuil : délai moyen maximal à fixer
Description	L'indicateur permet de mesurer les délais de renouvellement des sensibilisations (politique de sécurité)
Représentation graphique	Courbe d'évolution quantitative (moyenne des délais écoulés depuis la dernière sensibilisation des utilisateurs) Échelle : selon les valeurs de l'historique
Forme	
Responsable	Chef de projet maîtrise d'ouvrage, Monsieur A
Données et sources de données	Délais écoulés depuis la dernière sensibilisation (politique de sécurité) de chaque utilisateur Nombre d'utilisateurs
Calcul des données	Somme des délais écoulés depuis la dernière sensibilisation (politique de sécurité) de chaque utilisateur / nombre d'utilisateurs
Périodicité de calcul	Mensuelle
Interprétation	Si la courbe est en dessous du seuil, cela signifie que les sensibilisations sont renouvelées suffisamment. Si la courbe est au-dessus du seuil, cela signifie que la fréquence des sensibilisations est insuffisante.

Fiche descriptive d'indicateur

Fiche descriptive d'indicateur	
Libellé	**16 – Sécurité des applications**
Niveau	Stratégique
Objectif(s) mesurable(s)	L'indisponibilité des échanges du réseau du sous-système PERSONNEL ne doit pas être supérieure à 24h L'intervention des prestataires de maintenance du réseau du sous-système PERSONNEL doit être effectuée sous 4h …
Valeur(s) significative(s)	Cible : OK
Description	L'indicateur permet d'alerter le niveau stratégique en cas de problèmes relatifs à la sécurité des applications
Représentation graphique	Feu tricolore rouge, orange et vert Échelle : de "mauvais" à "bon"
Forme	
Responsable	Monsieur B.
Données et sources de données	Indicateurs (opérationnels et de pilotage) relatifs à la sécurité des applications (ex. : 2 - Indisponibilité des échanges du réseau du sous-système PERSONNEL)
Calcul des données	Bilan des indicateurs (opérationnels et de pilotage) relatifs à la sécurité des applications (ex. : 2 - Indisponibilité des échanges du réseau du sous-système PERSONNEL)
Périodicité de calcul	Annuelle
Interprétation	Si le feu est vert, cela signifie que la sécurité des applications est gérée conformément à la politique de sécurité. Si le feu est orange, cela signifie que la sécurité des applications n'est pas complètement gérée conformément à la politique de sécurité. Si le feu est rouge, cela signifie que la sécurité des applications n'est absolument pas gérée conformément à la politique de sécurité.

Enfin, l'**agencement pertinent des différents indicateurs** composant chaque tableau de bord SSI est étudié afin d'élaborer une maquette. Deux exemples sont proposés ici.





→ La validation de la tâche est assurée par les groupes de travail "technique", "exploitation" et "utilisation".

→ À l'issue de cette tâche, une **synthèse des tableaux de bord SSI** est rédigée.

Tâche 5 - Élaboration des procédures d'alimentation

Pour chaque indicateur composant un tableau de bord SSI, la procédure d'alimentation est formalisée de façon détaillée. Deux exemples sont proposés ici.

Procédure d'alimentation d'indicateur						
Libellé			**7 – Renouvellement des sensibilisations des utilisateurs (politique de sécurité)**			
Niveau			Pilotage			
Données et sources de données						
Libellé	Description et unité	Source	Mode de production	Responsable de production	Périodicité de production	Mode de collecte
Délais écoulés depuis la dernière sensibilisation (politique de sécurité) de chaque utilisateur	Délais (en mois)	Activité des utilisateurs	Saisie	Mademoiselle M.	Chaque fin de mois	Saisie
Nombre d'utilisateurs	Nombre d'utilisateurs qui doivent être sensibilisés	Activité des utilisateurs	Saisie	Monsieur N.	Chaque fin de mois	Saisie
Élaboration de l'indicateur						
Formule			Commentaires		Unité choisie	
Somme des délais écoulés depuis la dernière sensibilisation (politique de sécurité) de chaque utilisateur / nombre d'utilisateurs			Aucun		Mois	
Gestion de l'indicateur						
Périodicité de production	Responsable de la production	Procédure d'historisation	Consolidation	Mode de diffusion pour consolidation		
Chaque fin de mois	Monsieur A.	Archivage dans le répertoire relatif au tableau de bord "Sensibilisation des utilisateurs"	18 - Sensibilisation et formation	Courrier électronique		
Automatisation des procédures						
Tableur et logiciel de présentation.						

Procédure d'alimentation d'indicateur	
Libellé	**16 – Sécurité des applications**
Niveau	Pilotage

Données et sources de données

Libellé	Description et unité	Source	Mode de production	Responsable de production	Périodicité de production	Mode de collecte
Indicateur 2 - Indisponibilité des échanges du réseau du sous-système PERSONNEL	Courbe d'évolution quantitative	Indicateur N°2	Élaboration d'indicateur	Monsieur K.	Chaque fin de mois	Saisie
Indicateur 3 - Évolution du délai d'intervention des prestataires de maintenance du réseau du sous-système PERSONNEL	Courbe d'évolution quantitative	Indicateur N°3	Élaboration d'indicateur	Madame L.	Chaque fin de mois	Saisie
…	…	…	…	…	…	…

Élaboration de l'indicateur

Formule	Commentaires	Unité choisie
Bilan des indicateurs (opérationnels et de pilotage) relatifs à la sécurité des applications	Ce bilan est pour l'instant laissé à l'appréciation du responsable de l'indicateur. Une objectivation reste à déterminer.	Mois

Gestion de l'indicateur

Périodicité de production	Responsable de la production	Procédure d'historisation	Consolidation	Mode de diffusion pour consolidation
Chaque fin de mois	Monsieur B.	Archivage dans le répertoire relatif au tableau de bord "Sécurité des applications"	Aucune	Aucun

Automatisation des procédures

Tableur et logiciel de présentation.

Chaque tableau de bord SSI doit aussi disposer d'une procédure d'alimentation. Un exemple suit.

Procédure d'alimentation de tableau de bord SSI				
Libellé	**Sensibilisations des utilisateurs**			
Niveau	Pilotage			
Indicateurs composant le tableau de bord SSI				
Indicateur	Responsable de production	Mode de collecte		
7 - Renouvellement des sensibilisations des utilisateurs (politique de sécurité)	Monsieur A.	Courrier électronique		
8 - Renouvellement des sensibilisations des utilisateurs (protection des informations)	Madame C.	Courrier électronique		
9 - Renouvellement des sensibilisations des utilisateurs (respect des règles d'utilisation des postes de travail)	Mademoiselle D.	Courrier électronique		
10 - Renouvellement des sensibilisations des agents (consignes de protection contre les dégâts des eaux)	Monsieur E.	Courrier électronique		
11 - Proportion d'utilisateurs sensibilisés (politique de sécurité)	Madame F.	Courrier électronique		
12 - Proportion d'utilisateurs sensibilisés (protection des informations)	Mademoiselle G.	Courrier électronique		
13 - Proportion d'utilisateurs sensibilisés (respect des règles d'utilisation des postes de travail)	Monsieur H.	Courrier électronique		
14 - Proportion d'utilisateurs sensibilisés (consignes de protection contre les dégâts des eaux)	Madame I.	Courrier électronique		
Gestion du tableau de bord SSI				
Périodicité de production	Responsable de la production	Procédure d'historisation	Destinataires	Mode de diffusion aux destinataires
Chaque fin de semestre	Mademoiselle J.	Archivage dans le répertoire relatif au tableau de bord "Sensibilisation des utilisateurs"	- Autorité qualifiée responsable de la maîtrise d'ouvrage - Autorité qualifiée responsable de la maîtrise d'œuvre	Courrier électronique
Automatisation des procédures				
Logiciel de présentation.				

Enfin les **charges de travail et coûts récurrents** induits pour l'édition des tableaux de bord SSI doivent être calculés. Quelques exemples sont proposés ici.

Charges de travail et coûts récurrents			
Tableaux de bord SSI	Indicateurs	Détail des coûts	TOTAL
Atteinte des objectifs (stratégique)	15 - Application de la politique de sécurité 16 - Sécurité des applications 17 - Sécurité du serveur DPS et réseaux 18 - Sensibilisation et formation …	Collecte et analyse : 1h * N indicateurs Mise en forme : 1h	Environ 1 J*H une fois par an
Formation des personnels techniques (pilotage)	5 - Proportion de personnels techniques formés 6 - Renouvellement des sensibilisations et informations des personnels techniques …	Collecte : 0.5 J * N indicateurs Analyse : 30min * N indicateurs Mise en forme : 1h	Environ 1.5 J*H une fois par mois
…	…	…	…

→ La validation de la tâche est assurée par les groupes de travail "technique" et "exploitation".

→ À l'issue de cette tâche, une **synthèse des procédures d'alimentation** est rédigée.

Tâche 6 - Validation des tableaux de bord SSI

Cette tâche consiste à valider l'applicabilité des tableaux de bord SSI. En effet, la démarche prévoit des validations successives tout au long de l'étude, qui permettent de ne pas revenir sur des points formalisés précédemment.

Les tableaux de bord SSI sont édités une première fois en utilisant les procédures d'alimentation définies.

Ensuite, les groupes de travail valident le processus après avoir réalisé quelques ajustements en vue de cette première expérience.

Les modifications éventuellement apportées doivent être intégrées au niveau du projet (mise à jour de la documentation, modification des procédures…).

Par exemple, il a été décidé de renforcer la procédure d'alimentation de l'indicateur "1 – Renouvellement des sensibilisations des utilisateurs (politique de sécurité)" afin que les données (Délais écoulés depuis la dernière sensibilisation de chaque utilisateur et nombre d'utilisateurs) soient renseignées par les responsables des données dans des fichiers appropriés.

→ La validation de la tâche est assurée par les groupes de travail "exploitation", "pilotage" et "utilisation".

→ À l'issue de cette tâche, une **note de validation** est rédigée.

Étape 4 – Exploitation des tableaux de bord SSI

Tâche 1 – Mise en œuvre des tableaux de bord SSI

Les tableaux de bord SSI sont édités en utilisant les procédures d'alimentation définies. Les dates de disponibilités des données sont consignées, ainsi que la durée d'élaboration des indicateurs et tableaux de bord. Les données constitutives sont conservées dans des répertoires adéquats.

Une fois les tableaux de bord SSI édités, ceux-ci sont délivrés à leurs destinataires afin de prendre place dans le processus de décision.

→ La validation de la tâche est assurée par le groupe de travail "exploitation".

Étape 5 – Évolution des tableaux de bord SSI

Tâche 1 - Suivi des tableaux de bord SSI

La tâche de suivi consiste à :

- vérifier la qualité des indicateurs et tableaux de bord SSI (ergonomie, cohérence...) ;
- vérifier la pertinence des indicateurs et des valeurs ;
- vérifier l'adéquation des indicateurs et tableaux de bord SSI par rapport aux évolutions des objectifs de sécurité ;
- vérifier le besoin de mise à jour des tableaux de bord SSI ;
- vérifier que des compléments d'information ne sont pas nécessaires pour certains indicateurs.

Lors des premières itérations, des améliorations possibles sont identifiées quant à la qualité des indicateurs et aux informations les accompagnant.

Les indicateurs et valeurs collectées ont fait l'objet de vérifications qui ont confirmé leur pertinence.

Au bout de plusieurs itérations, l'évolution des objectifs de sécurité à été identifiée. Les objectifs de sécurité pour lesquels aucun objectif mesurable n'a pu être identifié pour cause d'évolution du contexte sont principalement concernés.

→ La validation de la tâche est assurée par les groupes de travail "exploitation", "pilotage", "technique" et "utilisation".

Tâche 2 - Suivi des modifications du contexte ou des objectifs

Dans le cas de l'intervention d'un élément nouveau, celui-ci doit être étudié afin d'envisager une mise à jour des indicateurs et tableaux de bord SSI. Il peut s'agir d'un changement concernant les objectifs de sécurité, les destinataires des tableaux de bord SSI, ou encore d'une révision souhaitée (périodiquement ou sur demande).

Les modifications éventuellement apportées doivent être intégrées au niveau du projet (mise à jour de la documentation, modification des procédures…).

Suite aux premières éditions de tableaux de bord SSI, il a été possible d'affiner les plages de tolérance, les échelles choisies, les valeurs seuils et cibles…

Les éditions suivantes ont permis de réajuster les indicateurs, notamment en termes description, d'interprétation des résultats et de périodicité. De plus, les efforts entrepris pour produire et éditer les tableaux de bord ont été capitalisés afin d'améliorer les procédures de production et la collecte de certaines données a pu être automatisée. De ce fait, les coûts associés à la production des indicateurs et tableaux de bord SSI ont diminué.

Il est maintenant envisagé de mettre à jour les objectifs de sécurité afin de prendre en compte les évolutions relatives au contexte (changement d'entités telles que matériels et réseaux, réorganisations internes). Par ailleurs, il est aussi envisagé d'étendre le périmètre du projet. Par conséquent, les groupes de travail doivent reprendre la démarche en amont afin d'ajuster chaque étape à ces évolutions.

→ La validation de la tâche est assurée par les groupes de travail "exploitation", "pilotage", "technique" et "utilisation".

Conclusion

Le projet Tableaux de bord SSI est un projet stratégique qui demande l'implication de nombreux personnels. Cet investissement est surtout significatif au lancement du projet et dans la phase de conception. Par la suite, le retour sur investissement prend la forme de plusieurs bénéfices :

- le tableau de bord SSI devient un véritable outil :
  - de décision (pour le niveau stratégique),
  - de suivi des travaux (pour le niveau pilotage),
  - d'auto-évaluation (pour le niveau opérationnel) ;

- les procédures de collecte et de production d'indicateurs sont peu à peu optimisées de telle sorte que leur coût s'amoindrisse (pérennité des procédures) ;

- le projet génère une synergie autour de la SSI et permet de sensibiliser tous les acteurs impliqués ;

- le projet peut s'étendre à d'autres systèmes en profitant de l'expérience du projet pilote (pérennité du projet).

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