METHODES

DEMARCHE DE CONCEPTION
D'UN TABLEAU DE BORD QUALITE
APPLIQUE A LA SECURITE

"Je crois qu'on ne peut mieux vivre qu'en cherchant à devenir meilleur, ni plus agréablement qu'en ayant pleine conscience de son amélioration".

Socrate

Juin 1997

Commission Méthodes

CLUB DE LA SECURITE DES SYSTEMES D'INFORMATION FRANÇAIS
30, Rue Pierre Sémard – 75009 Paris
Mail : clusif@clusif.asso.fr Web : http://www.clusif.asso.fr

REMERCIEMENTS

Le CLUSIF tient à mettre ici à l'honneur les personnes qui ont rendu possible la réalisation de cette méthode et de ce document, tout particulièrement :

BERTIN	*Michel*	**ATHESA**
BOSTFFOCHER	*Catherine*	**GROUPE MALAKOFF**
COURBIS	*Marie-Hélène*	**ABYSS ENGINEERING**
DUPONT	*Annie*	**Jacques Anis et Associés**
GANDOIS	*Jean-Claude*	**LEGRAND**
LAUTIER	*Patrick*	**COMPAGNIE GENERALE DES EAUX**
VALENTIN	*Bernard*	**CBV2A / SYSIACOM**

TABLE DES MATIERES

0. PREAMBULE

La complexité croissante des systèmes d'information et des moyens de communication de l'entreprise impose une très lourde responsabilité aux acteurs liés aux services de sécurité, quelque soit le niveau de la fonction qu'ils intègrent.

Dans cette optique, la mesure est devenue nécessaire et, à cet égard, un tableau de bord précis et bien adapté à chaque fonction est un atout certain pour optimiser la qualité des services de sécurité.

Ce système de mesure doit s'appuyer sur une organisation au sein de laquelle chacun doit avoir des responsabilités.

1. GENERALITES

Le tableau de bord est un outil de synthèse et de visualisation de situations décrites et de constats effectués par les indicateurs.

1.1. Objectifs

Les objectifs du système "tableau de bord" sont :

- suivre la qualité de la politique de sécurité établie,
- suivre la qualité des services de sécurité,
- remonter les alertes afin de prévenir les dysfonctionnements,
- permettre une synthèse rapide des actions en cours.
- fournir un outil d'aide au système d'assurance et de gestion de la sécurité.

1.2. Contraintes

Le tableau de bord :

- Nécessite un pilote.
- Doit véhiculer seulement les informations pertinentes.
- Doit comporter un nombre très limité d'indicateurs.
- Nécessite une sensibilisation et une formation des pilotes et responsables de la collecte d'information.
- Nécessite une vérification de la pertinence des éléments ou événements à mesurer.
- Nécessite de déterminer les valeurs cibles à atteindre ainsi que leur seuil de tolérance.
- Nécessite une fréquence adaptée à une exploitation attentive.

2. PHILOSOPHIE ET ARCHITECTURE

"Je crois qu'on ne peut mieux vivre qu'en cherchant à devenir meilleur, ni plus agréablement qu'en ayant pleine conscience de son amélioration".

Cette citation de SOCRATE résume la philosophie d'un tableau de bord construit consciencieusement.

2.1. Eléments

L'analyse de la qualité se fonde sur la mise en évidence d'un ensemble de facteurs qui correspondent aux thèmes spécifiques de qualification - ce document traite seulement le facteur sécurité.

Pour apprécier ce facteur, on lui associe les trois critères "disponibilité, intégrité et confidentialité" que l'on doit respecter.

L'adéquation à chaque critère est évaluée par un ensemble de métriques appelés indicateurs de mesure.

Les critères et les indicateurs de mesure, selon leur importance, sont pondérés en vue d'établir un diagnostic à l'issue de l'application du tableau de bord.

Il existe deux types d'indicateurs de mesure ; indicateur simple et indicateur composé.

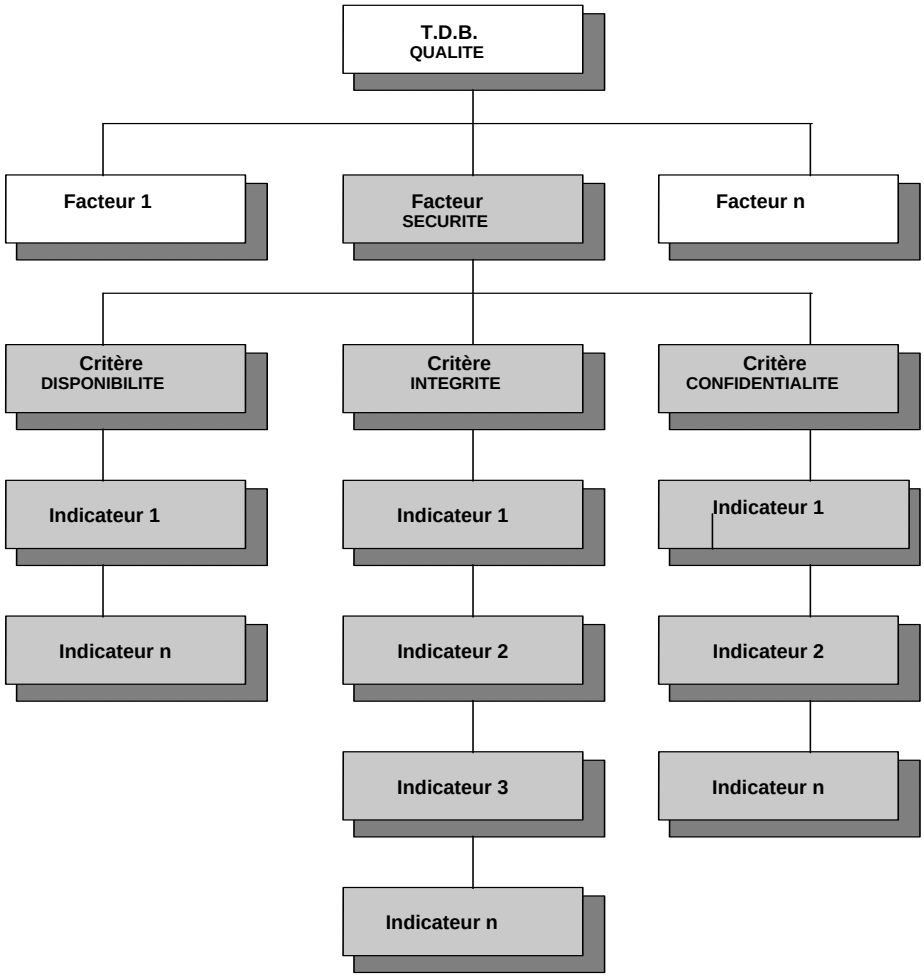
Un indicateur de mesure simple comporte :

- une question, une pondération, un ensemble de valeurs de référence et une procédure.

Un indicateur de mesure composé comporte :

- en plus des éléments de l'indicateur simple, un indicateur de comparaison et un opérateur.

2.2. Schéma de l'architectue d'un tableau de bord système d'information



COMPOSITION D'UN INDICATEUR

QUESTION
PONDERATION
VALEURS DE REFERENCE
PROCEDURE ASSOCIEE
MESURE DE L'INDICATEUR DE COMPARAISON
OPERATEUR

2.3. Classification des tableaux de bord

On peut classer les TDB en trois niveaux selon la nature des indicateurs. On distingue ainsi :

- niveau stratégique
- niveau fonctionnel
- niveau opérationnel

T.D.B. STRATEGIQUE

Les indicateurs appartenant à ce type de T.D.B. sont intimement liés à la politique et à l'image de marque de l'entreprise. Ils sont généralement à caractère générique et on les appelle indicateurs de stratégie ou indicateurs de résultat.

On peut définir un indicateur de stratégie comme celui qui décrit des résultats, obtenus du point de vue qualitatif, par rapport aux objectifs fixes par la politique de l'entreprise.

EXEMPLE :

UNE CIBLE D'EVALUATION : Image de marque de l'entreprise.

UN FACTEUR A EVALUER : Sécurité du système d'information.

LES CRITERES A RESPECTER : Disponibilité de l'information,

Intégrité de l'information,

Confidentialité de l'information.

On va donner à chacun de ces critères une pondération qui sera intimement liée à l'image, que l'entreprise désire donner à ses clients et partenaires. Suite à cette pondération, la direction va s'intéresser au suivi des indicateurs attachés au(x) critère(s) de plus haute pondération car il(s) sera(seront) considéré(s) comme étant le(s) plus représentatif(s) de l'image de marque.

Ainsi, s'il s'agit d'une entreprise de vente par correspondance, on va s'intéresser aux critères : disponibilité de l'information et intégrité de l'information.

On peut constater que dans ce type d'entreprise :

a) L'indisponibilité de l'information peut se traduire par une perte d'activité.

b) Si l'information est disponible mais l'intégrité n'est pas assurée, ceci peut se traduire par des dysfonctionnements organisationnels et / ou la perte du client.

Les indicateurs seront alimentés par consolidation des indicateurs du niveau fonctionnel correspondant.

T.D.B. FONCTIONNEL

Les indicateurs appartenant à ce type de T.D.B. sont de deux natures : indicateurs d'efficacité et indicateurs de satisfaction.

Un indicateur fonctionnel décrit des résultats atteints en termes de qualité avec un double point de vue qui comporte à la fois la vision d'efficacité du fournisseur du service et la vision de satisfaction du client ou utilisateur du service.

La collecte se fait avec les deux types de population et il y aura un T.D.B. par application concerné.

EXEMPLE :

UNE CIBLE D'EVALUATION : Application Informatique

UN FACTEUR A EVALUER : Sécurité du système d'information.

LES CRITERES A RESPECTER : Disponibilité de l'information,

Intégrité de l'information,

Confidentialité de l'information.

S'il s'agit d'une entreprise de vente par correspondance, la consolidation de certains indicateurs attachés aux critères de disponibilité et intégrité va permettre d'alimenter les indicateurs de niveau stratégique, les autres seront traités au niveau fonctionnel.

Au niveau fonctionnel, on traite les indicateurs de satisfaction dédiés aux clients (utilisateurs des applications informatiques) ainsi que les indicateurs d'efficacité des fournisseurs (services informatiques). On peut élaborer certains indicateurs d'efficacité par consolidation des indicateurs opérationnels collectés directement de l'ordinateur.

C'est au niveau fonctionnel que l'élaboration des indicateurs est la plus complexe, mais c'est aussi à ce niveau qu'on peut déceler la plupart des menaces et prendre les principales mesures de sécurité, car on peut agir rapidement par démultiplication.

T.D.B. OPERATIONNEL

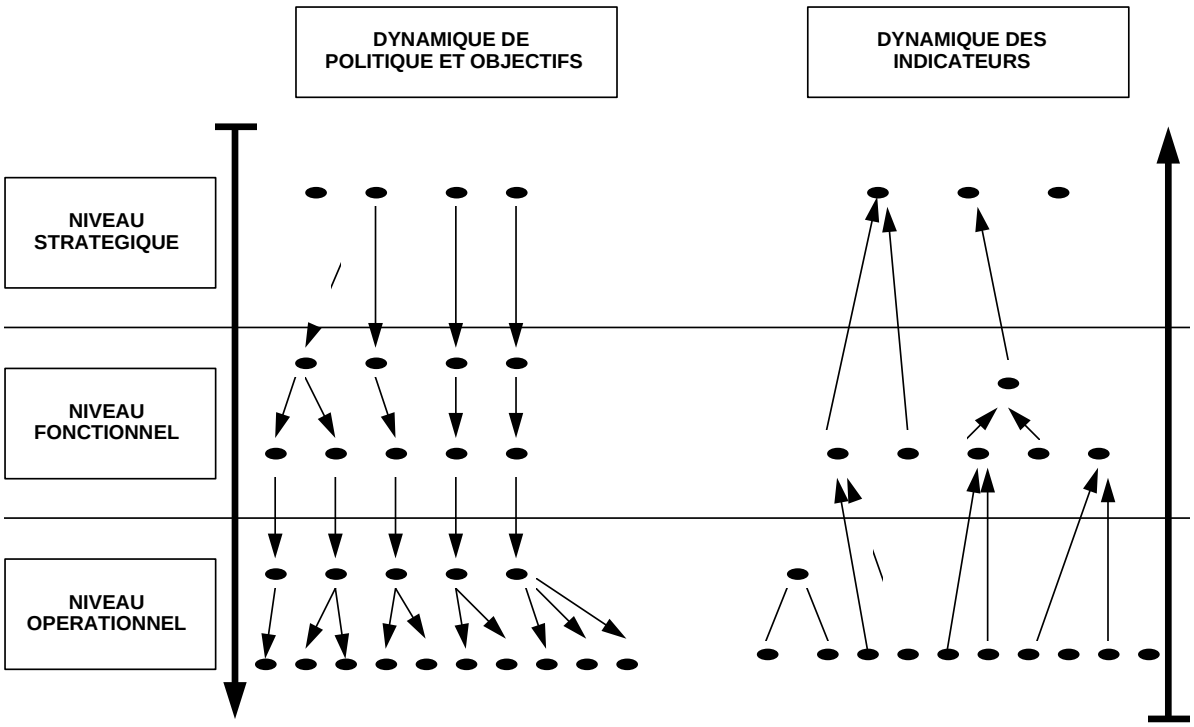
Les indicateurs de ce type de T.D.B. vont décrire une situation du point de vue quantitatif pour constater des résultats qualitatifs par rapport à des valeurs de référence établis.

La collecte de l'information peut se faire par simple mesure et / ou comptage (voir quelques exemples d'indicateurs opérationnels en chapitre 4).

2.4. Dynamique de la politique de l'entreprise et des indicateurs

On peut distinguer trois niveaux au sein de l'organisation de l'entreprise :

- niveau stratégique
- niveau fonctionnel
- niveau opérationnel



Tandis que la politique est communiquée de haut en bas, les indicateurs sont communiqués du bas vers le haut.

DYNAMIQUE DES INDICATEURS :

- INDIC. STRATEGIQUES : Plusieurs indic.stratégiques peuvent alimenter un indic. Stratégique
  Un indic.stratégique peut être indépendant.

- INDIC. FONCTIONNELS : Plusieurs indic.fonctionnels peuvent alimenter un indic. stratégique
  Plusieurs indic.fonctionnels peuvent alimenter un indic. fonctionnel
  Un indic.fonctionnel peut être indépendant.

- INDIC. OPERATIONNELS : Plusieurs indic.opérationnels peuvent alimenter un indic. opérationnel
  Plusieurs indic.opérationnels peuvent alimenter un indic. fonctionnel
  Un indic.opérationnel peut être indépendant.

2.5. Exemple de l'approche par niveaux

2.5.1. Etablissement des indicateurs

Exemple : cas de la Disponibilité

Pour certaines entreprises, la disponibilité est très importante, exemple : la Bourse, la vente par correspondance,...

Il faut :

- analyser l'entreprise avec une approche systémique : rechercher les différents sous-systèmes qui constituent le système de l'entreprise.
- suivre la dynamique de l'entreprise (de haut en bas) pour identifier les indicateurs (de bas en haut) au moyen de cartographies.

Niveau et nature des cartographies :

NIVEAU	NATURE
Stratégique	Activités
Fonctionnel	Applications
Opérationnel	Traitement

Au niveau stratégique :

Les activités majeures de l'entreprise qui influent sur l'image de l'entreprise.

Au niveau fonctionnel :

Pour chaque activité selectionnée, on peut trouver n applications informatique ; on va selectionner la(les) application(s) concernée(s) par la disponibilité.

Au niveau opérationnel :

Pour chaque application selectionnée, on peut trouver n traitements : Tr1, Tr2, Tr3, ...

On commence par l'application la plus représentative de l'activité concernée. On cherche l'importance relative des traitements par rapport à la disponibilité, par exemple :

TRAITEMENT	PONDERATION	INDICATEUR
Tr1	1	Indicateur Tr1
Tr2	4	Indicateur Tr2
Tr3	3	Indicateur Tr3
…	…	…

Pour chaque traitement, il faut un indicateur pour la disponibilité que l'on peut pondérer par le poids du traitement correspondant.

Ces indicateurs peuvent servir :

- par eux-mêmes au niveau traitement pour chaque traitement,
- à constituer des indicateurs de niveaux supérieurs en fonction de leur poids, par exemple les indicateurs de traitement de poids 4 peuvent remonter au niveau stratégique.

2.5.2. Exemple de découpage schématique de l'entreprise pour une étude de tableaux de bord

Selon les entreprises, le découpage et les besoins en indicateurs peuvent être :

- **Au niveau stratégique**

La disponibilité étant l'un des principaux critères de l'image de marque de l'entreprise, la Direction détermine, parmi les activités existantes, celle qui a le plus de liens directs (la plus représentative) avec la disponibilité de l'information.

- **Au niveau fonctionnel**

Au sein de l'activité retenue, on détermine la ou les applications les plus liées à la disponibilité de l'information.

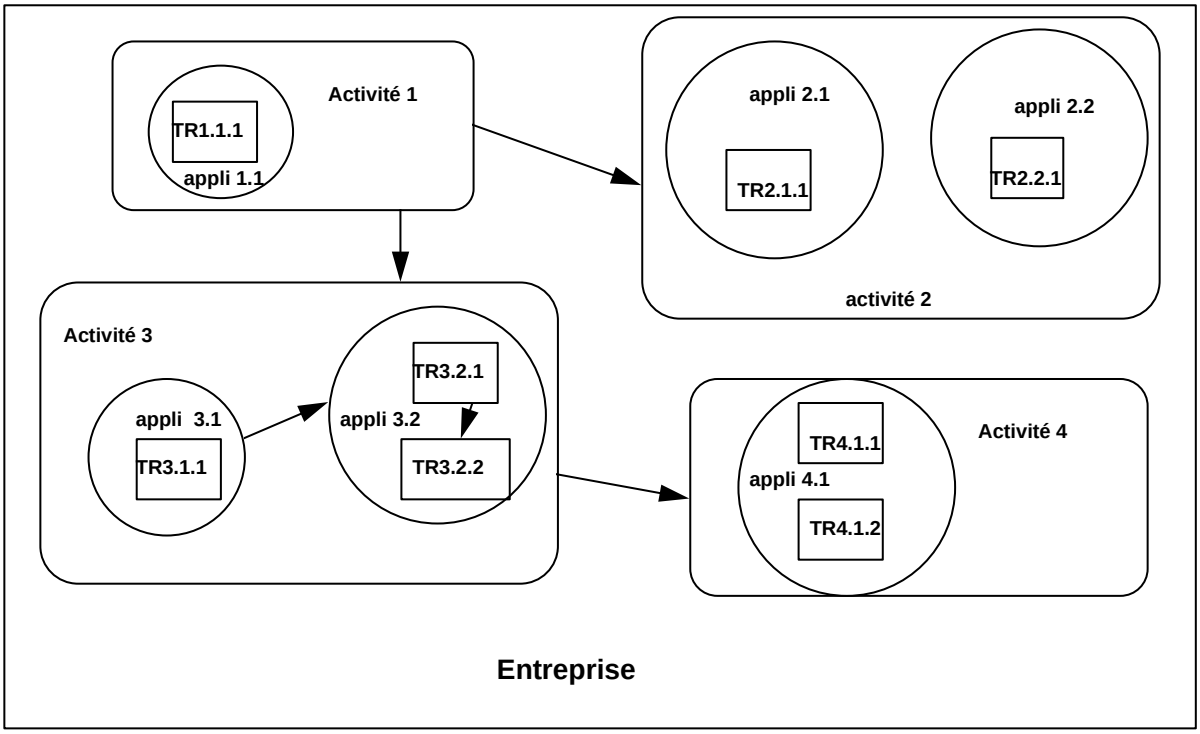
- **Au niveau opérationnel**

Pour chaque application sélectionnée, on pondère les traitements par rapport à la disponibilité puis on selectionne ceux qui sont pondérés au niveau critique et au niveau stratégique.

Pour chaque traitement retenu, on détermine les indicateurs de disponibilité à suivre, pondérés en fonction de leur importance.

Les indicateurs opérationnels de forte pondération peuvent être remontés dans les TDB fonctionnels, voire stratégiques.

Vision Schématique de l'Entreprise



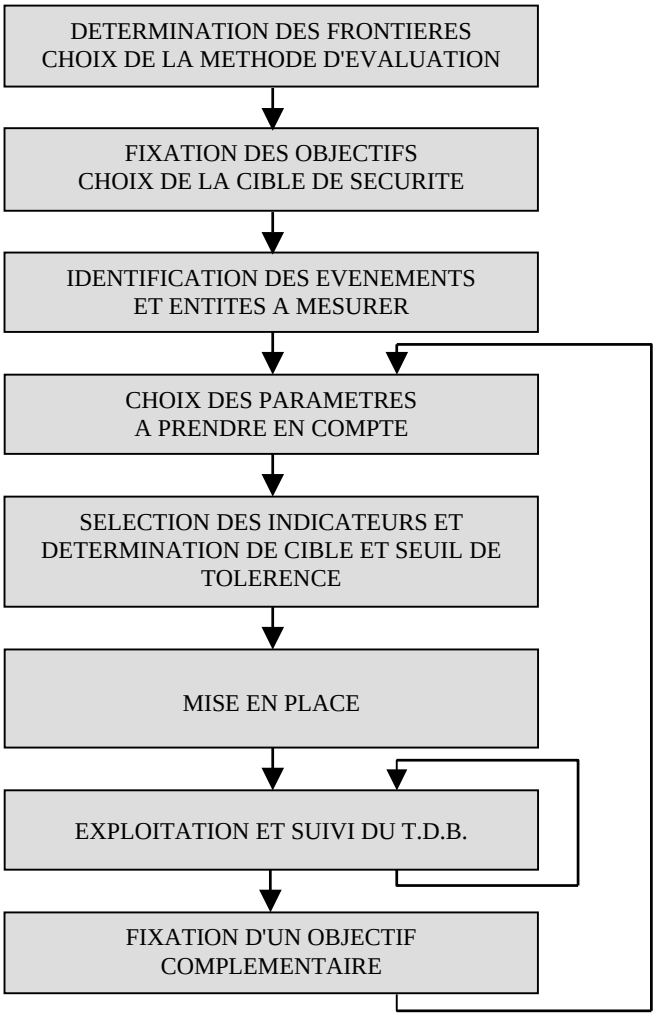
3. METHODE

3.1. Introduction

Le tableau de bord est un support de communication opérationnel très puissant s'il comporte des informations dont on peut prouver l'utilité, la pertinence, la fiabilité et s'il offre une accessibilité adéquate.

C'est pourquoi l'élaboration d'un tableau de bord nécessite une méthode à suivre et une démarche adéquate pour mettre en œuvre la méthode.

3.2. Schéma de la démarche



3.3. Etapes de la méthode

3.3.1. Détermination des frontières du domaine ou cible d'évaluation

La détermination des frontières du domaine couvert par le T.D.B. consiste à déterminer une cible d'évaluation. La cible d'évaluation se matérialise par une fonction ou service de sécurité.

Principes directeurs.

- Etablir le lien entre les objectifs stratégiques de l'organisation et ses besoins en information.
- Définir les domaines ainsi que leur architecture pour comprendre ce qu'ils sont, ce qu'ils font et comment ils sont articulés.
- Connaître la population à prendre en compte et les responsables concernés.

Pratiques et outils.

- Elaboration des cartographies de l'entreprise (activités, applications, traitements).
- Modélisation des processus concurrentiels.

3.3.2. Fixation des objectifs ou cible de sécurité.

- Déterminer le champ d'action et les responsabilités du pilote en vue de déceler les objectifs à atteindre.

Pour déterminer la cible de sécurité, il est nécessaire :

- d'identifier les menaces relatives à la cible d'évaluation, domaine qui sera couvert par le tableau de bord.
- de déterminer une politique de sécurité contenant les mesures à prendre et les procédures à suivre pour réduire les risques et pour minimiser l'impact en cas d'agression.

Exemples de Menaces :

- sabotage d'équipements.
- vol d'équipements stratégiques.
- modification malveillante du matériel ou du logiciel par un tiers non autorisé.
- effacement malveillant d'un support magnétique amovible.
- substitution des supports par une personne autorisée ou un tiers non autorisé.
- manipulation d'un équipement de réseau par une personne autorisée en vue de divulguer des données.
- écoute sur le réseau.

Exemple de Mesures :

Mesures structurelles destinées à l'organisation des ressources humaines.

- Formaliser une procédure de contrôle des droits d'accès.
- Informer et former le personnel sur les différents systèmes de détection et de contrôle d'accès installés.

- Informer et former le personnel sur les procédures établies.
- Elaborer les questionnaires destinés à auditer les procédures.
- Elaborer les questionnaires d'audit de l'application de chaque procédure, audits qui seront réalisés selon une fréquence déterminée.
- Identifier les indicateurs de mesure à suivre dans le(s) tableau(x) de bord.

Les procédures formalisées jouent un rôle de formation et d'information des acteurs.

Organisation des procédures

Les procédures doivent être organisées par fonction et par tâche en vue de transmettre le savoir et savoir-faire. Elles seront regroupées dans un ou plusieurs manuels afin de décrire l'ensemble des actions à mener et leur séquencement. L'organisation des procédures s'apparente à l'organisation des ressources humaines.

3.3.3. Identification des événements et entités à mesurer

Le Tableau de Bord a pour objectif de mesurer l'efficacité de la politique sécurité établie pour contrer les menaces. C'est-à-dire de suivre les progrès réalisés et d'être une aide à la décision pour orienter des nouveaux objectifs.

Pour apprécier l'efficacité, il faut trouver les indicateurs de mesure adéquats parmi les éléments recueillis, les pondérer selon leur importance et déterminer la valeur cible et le seuil de tolérance.

- Lister les événements déclencheurs du processus concerné et les événements résultats en sortie.
- Mettre en évidence les entités mesurables.
- Sélectionner les événements et entités à mesurer.

3.3.4. Choix des paramètres à prendre en compte

- Pour chaque événement et/ou entité sélectionné, identifier les paramètres qui permettront de faire le point par rapport aux objectifs.
- Déterminer les indicateurs de mesure.

3.3.5. Sélection des indicateurs et détermination de : Cible et Seuil de Tolérance

- Sélectionner les indicateurs pertinents pour le pilote.
- Etablir des valeurs de référence en vue de déterminer la cible (pour chaque indicateur).
- Déterminer le seuil de tolérance.

3.3.6. Mise en place

- Etablir la procédure à suivre pour la collecte de données de chaque indicateur,
- Etablir la procédure d'alerte à suivre pour chaque indicateur,
- Etablir une procédure de contrôle des procédures.

3.3.7. Exploitation et suivi

- Révision des valeurs de référence (spécialement valeur cible et seuil de tolérance),
- Modification ou ajout des procédures liées à chaque indicateur,
- Création des indicateurs génériques servant à remonter l'information.

3.3.8. Réactualisation

- Suppression de certains indicateurs,
- Création des nouveaux indicateurs,
- Modification de la cible.

4. EXEMPLES

4.1. Tableau de bord 330 (MEHARI)

4.1.1. Détermination des frontières du domaine.

A l'intérieur du domaine 300 "sécurité anti-intrusion", on va choisir le système de protection contre l'intrusion dans les locaux. Ce système est étroitement lié à l'image de l'entreprise, car une entreprise bien protégée donne confiance à ses clients et à son personnel.

La cible d'évaluation se matérialise par le service 330 "se protéger de l'intrusion dans les locaux" qui comporte 4 sous-services chargés :

- du contrôle d'accès aux locaux
- de la surveillance des locaux
- du contrôle des passages adjacents aux locaux
- des automatismes de détection d'intrusion

4.1.2. Fixation des objectifs ou cible de sécurité

Pour déterminer la cible de sécurité, il est nécessaire :

- d'identifier les menaces relatives à la cible d'évaluation (service 330), domaine qui sera couvert par le tableau de bord.
- de déterminer une politique de sécurité contenant les mesures à prendre et les procédures à suivre pour réduire les risques et pour minimiser l'impact en cas d'agression.

Menaces :

- petit vandalisme sur les équipements soit par des personnes autorisées à pénétrer dans les locaux, soit par des tiers non autorisés.
- sabotage d'équipements, par des casseurs, entraînant leur destruction partielle ou totale.
- vol d'équipements stratégiques.
- modification malveillante du matériel ou du logiciel par un tiers non autorisé entraînant une dégradation des performances.
- effacement malveillant d'un support magnétique amovible entraînant la destruction des logiciels.
- substitution des supports par une personne autorisée ou un tiers non autorisé en vue de frauder ou causer des torts à l'entreprise.
- manipulation d'un équipement de réseau par une personne autorisée en vue de divulguer des données.

Les mesures

Mesures structurelles destinées à l'organisation des ressources humaines.

- Formaliser une procédure stricte de la gestion des clés, des badges ou des cartes magnétiques ou à mémoire.
- Formaliser la procédure à suivre en cas de perte ou de vol des clés, des badges ou des cartes magnétiques ou à mémoire.
- Formaliser les procédures de gestion de surveillance des locaux.
- Formaliser une procédure de contrôle des droits d'accès hiérarchisés (par profil et par local).
- Informer et former le personnel sur les différents systèmes de détection et de contrôle d'accès installés.
- Informer et former le personnel sur les procédures établies.
- Elaborer les questionnaires destinés à auditer les procédures.
- Elaborer les questionnaires d'audit de l'application de chaque procédure, audits qui seront réalisés selon une fréquence déterminée.
- Identifier les indicateurs de mesure à suivre dans le(s) tableau(x) de bord.

Mesures de dissuasion pour éviter la concrétisation de la menace.

- Utilisation d'un système de vidéo-surveillance.
- Identifier les indicateurs de mesure à suivre dans le(s) tableau(x) de bord.

Mesures préventives pour empêcher l'aboutissement de l'agression.

- Utilisation d'un dispositif d'habilitation (digicode) couplé à la clé, au badge ou à la carte magnétique ou à mémoire.
- Un organisme spécialisé doit être chargé de la vérification et de l'entretien périodique de l'ensemble des installations de contrôle d'accès.
- la résistance à l'effraction des portes doit être certifiée suite à une certification APSAD.
- Identifier les indicateurs de mesure à suivre dans le(s) tableau(x) de bord.

Les mesures de sécurité destinées à minimiser l'impact du disfonctionnement

Mesures de protection pour limiter l'ampleur de la détérioration.

- Installer un ou des sas asservis avec temporisation ne permettant l'accès qu'à une seule personne à la fois.
- Installer un système de détection d'intrusion fonctionnant en dehors des heures de travail.
- Identifier les indicateurs de mesure à suivre dans le(s) tableau(x) de bord.

Mesures palliatives pour réparer et atténuer les dégâts.

- On doit avoir étudié les situations d'indisponibilité grave dues à la malveillance et défini au moins un plan de secours comportant :

  - Moyens de secours.

  - Procédure de mise en œuvre du secours.

4.1.3. Identification des évènements et entités à qualifier

Dans le cas présent, on va s'intéresser à :

- L'utilisation du lecteur de cartes.
- La qualité technique de fonctionnement du lecteur de cartes.
- Le flux du personnel autorisé à circuler dans les locaux.

Eléments quantifiables

Nombre total de cartes en circulation

Nombre total de personnes autorisées à circuler en salle machine

Nombre total de personnes autorisées à circuler dans le local d'archives

Nombre d'utilisation du lecteur de cartes d'accès à l'entreprise par période (semaine, mois, trimestre...)

Nombre d'utilisation du lecteur de cartes d'accès au local d'archives par période (semaine, mois, trimestre...)

Nombre d'utilisation du lecteur de cartes d'accès à la salle machine par période (semaine, mois, trimestre...)

Nombre de rejets de cartes de lecteur de cartes d'accès à l'entreprise par période (semaine, mois, trimestre...)

Nombre de rejets de cartes de lecteur de cartes d'accès à la salle machine par période (semaine, mois, trimestre...)

Nombre de rejets de cartes de lecteur de cartes d'accès au local d'archives par période (semaine, mois, trimestre...)

Nombre de pannes du lecteur de cartes d'accès à l'entreprise par période (semaine, mois, trimestre...)

Nombre de pannes du lecteur de cartes d'accès à la salle machine par période (semaine, mois, trimestre...)

Nombre de pannes du lecteur de cartes d'accès au local d'archives par période (semaine, mois, trimestre...)

Nombre d'interventions du service de maintenance sur le lecteur de cartes d'accès à l'entreprise par période (semaine, mois, trimestre...)

Nombre d'interventions du service de maintenance sur le lecteur de cartes d'accès à la salle machine par période (semaine, mois, trimestre...)

Nombre d'interventions du service de maintenance sur le lecteur de cartes d'accès au local d'archives par période (semaine, mois, trimestre...)

Nombre total de cartes perdues ou volées par période (semaine, mois, trimestre...)

Effectif total du département informatique

Turnover (Nombre d'entrées / sorties du personnel d'exploitation par période (mois, trimestre...)

Taux de participation aux formations sur les différents systèmes de détection et de contrôle d'accès installés

Taux de participation aux informations sur les différents systèmes de détection et de contrôle d'accès installés

Nombre total des prestataires du mois

Nombre de tentatives d'intrusion enregistrées par l'appareil de détection par période (semaine, mois, trimestre...)

Nombre d'agressions détectées par période (semaine, mois, trimestre...)

4.1.4. Exemple de construction d'indicateurs de mesure

A. Effectif total du département informatique

B. Nombre total de personnes autorisées à circuler en salle machine

C. Nombre d'utilisation du lecteur de cartes d'accès à la salle machine par période (semaine, mois, trimestre...)

D. Nombre de rejets de cartes du lecteur de cartes d'accès à la salle machine par période (semaine, mois, trimestre...)

E. Nombre de pannes du lecteur de cartes d'accès à la salle machine par période (semaine, mois, trimestre...)

F. Nombre d'interventions du service de maintenance sur le lecteur de cartes d'accès à la salle machine par période (semaine, mois, trimestre...)

G. Turnover (Nombre d'entrées / sorties du personnel d'exploitation par période

Indicateur A

Cet indicateur n'a ni valeur cible ni seuil de tolérance car il sert de base au calcul d'autres indicateurs.

Pondération : selon la sensibilité, choisir entre, 0 = neutre, 1 = faible, 2 = sensible, 3 = critique,

4 = stratégique.

Indicateur B

Cet indicateur sera utilisé avec l'indicateur "A" comme indicateur de comparaison pour établir le ratio "B/A".

Pondération : selon la sensibilité, choisir entre, 0 = neutre, 1 = faible, 2 = sensible, 3 = critique,

4 = stratégique.

Indicateur C

Scénario pour établir les valeurs de référence : si chaque personne autorisée à circuler dans le local utilise en moyenne X fois par jour l'appareil de contrôle d'accès pendant Y jours par mois, la base pour établir les valeurs de référence sera : B x X x Y. Parmi les valeurs de référence ainsi établies, on désigne la valeur cible et le seuil de tolérance.

Pondération : choisir entre, 0 = neutre, 1 = faible, 2 = sensible, 3 = critique, 4 = stratégique.

Indicateur D

Les valeurs de référence qui vont permettre d'établir la valeur cible et les seuils de tolérance vont dépendre du quotient : mesure indicateur D / mesure indicateur C

Valeurs de référence :

$$\frac{D}{C} = 0 \rightarrow \text{très bon} = 5 \quad \text{(BLEU)}$$

$$\frac{D}{C} \leq 0{,}02 \rightarrow \text{bon} = 4 \quad \text{(VERT)}$$

$$0{,}02 < \frac{D}{C} < 0{,}05 \rightarrow \text{moyen} = 3 \quad \text{(JAUNE)}$$

$$0{,}05 < \frac{D}{C} < 0{,}08 \rightarrow \text{médiocre} = 2 \quad \text{(ORANGE)}$$

$$0{,}08 \leq \frac{D}{C} \rightarrow \text{mauvais} = 1 \quad \text{(ROUGE)}$$

Valeur cible = 0 Seuil de tolérance = 0,05

Pondération : selon la sensibilité du local, choisir entre,

0 = neutre, 1 = faible, 2 = sensible, 3 = critique, 4 = stratégique.

TABLEAU DE BORD SECURITE

INDICATEUR	CIBLE SECURITE	PONDERATION	SEUIL DE TOLERANCE	MESURE	STATUS *

*** Très bon = 5 (Bleu), Bon = 4 (Vert), Moyen = 3 (Jaune**), **Médiocre = 2 (Orange), Mauvais = 1 (Rouge)**

4.2. Tableau de bord suivi du contrat de service

Ce Tableau de Bord Sécurité d'Exploitation permet de suivre l'adéquation du service fourni par l'exploitation aux utilisateurs en termes d'objectifs fixés par un "contrat de service", qui est l'expression formelle de la "relation de type Client-Fournisseur, pour une application donnée.

4.2.1. Définitions

- on y appelle "Client" l'acteur qui demande la fourniture d'un bien ou d'un service, soit ici précisément un résultat d'étape matérialisé notamment par des documents;
- on y appelle "Fournisseur" l'acteur qui délivre cette fourniture;
- la relation Client-Fournisseur est initialisée lorsque ces deux acteurs ont formalisé leur accord réciproque concernant :
    - la consistance de la fourniture attendue,
    - les règles qui permettront d'évaluer si la fourniture délivrée est conforme à la fourniture attendue,
    - le délai au terme duquel le fournisseur s'engage à avoir délivré la fourniture;
    - la valorisation des moyens que mettra en œuvre le fournisseur pour s'acquitter de la fourniture.

Le contrat de service négocié entre l'informatique et ses utilisateurs :

- formalise les relations de type client-fournisseur entre les deux parties

- définit les prestations de service

- sert de référence à la relation régulière dans la fourniture du service informatique

Le client :

Le client dans le monde utilisateur est responsable de la validité des données fournies, de leur volume et des processus de gestion. Il est co-signataire du contrat de service.

Le fournisseur :

L'informatique est responsable de l'intégrité et de la validité des moyens. Le choix des moyens informatiques (technologie, architecture, outils, logiciels) lui appartient tout en offrant le service au meilleur ratio coût/performance. Il est co-signataire du contrat de service.

4.2.2. Prestations.

Plage de fonctionnement : c'est la durée durant laquelle les prestations sont garanties.

Temps de réponse : c'est le délai entre la transmission et la réponse au terminal de l'utilisateur. Il ne doit pas être supérieur à un certain seuil déterminé.

Le temps de réponse des traitements, défini directement par l'utilisateur, est fonction de leur complexité.

Ces mesures seront effectuées par la production informatique sur demande du client.

Prise en compte et résolution des problèmes : c'est le pourcentage d'incidents résolus dans les délais prévus, les incidents ont une évaluation de 1 à 4 donnée par le client pour la prise en compte et la résolution des incidents par la production informatique pour l'application.

Tout problème ayant potentiellement ou non un impact sur une prestation d'un contrat est considéré comme incident.

Le temps fixé pour la résolution des incidents, s'applique à partir du moment de la notification de l'incident par l'une des deux parties et est dépendant de leur niveau de sévérité.

sévérité 4 : "stratégique"

sévérité 3 : "critique"

sévérité 2 : "sensible"

sévérité 1 : "faible"

Ce niveau de sévérité est défini par le client en fonction de l'importance de l'application.

4.2.3. Valeurs contractuelles

Pour chacune des prestations mesurables, une valeur sera affectée, négociée entre les deux parties, déterminant le seuil.

Les valeurs contractuelles des prestations sont garanties dans les limites des volumes définis par le client.

Manuel de procédures : Un manuel de procédures destiné à l'exploitation du tableau de bord s'avère nécessaire.

exemple :

Une application dont les traitements sont classés stratégiques, qui a subi un incident de production pouvant avoir un impact sur le niveau de service - tel que défini dans le contrat de service - doit être munie d'une procédure qui indique la méthode à suivre pour porter l'incident à la connaissance de l'utilisateur à qui il appartiendra de prendre les mesures prévues.

EXEMPLE DE TABLEAU DE BORD SECURITE

INDICATEUR	CIBLE SECURITE	PONDERATION	SEUIL DE TOLERANCE	MESURE	STATUS *
Plage de fonctionnement					
Nombre d'arrêt hebdo Nombre d'utilisation					
Nombre d'accès rejetés Nombre total d'accès					
Nombre d'incidents					
Volume traité					
Fraîcheur des données					

*** Très bon = 5 (Bleu), Bon = 4 (Vert), Moyen = 3 (Jaune), Médiocre = 2 (Orange), Mauvais = 1 (Rouge)**

5. GLOSSAIRE

ACTION OU TACHE A REALISER

Description de l'action ou de la tâche à réaliser.

CIBLE :

Valeur à atteindre (valeur optimale affectée à un indicateur, cette valeur fait partie des valeurs de référence).

CIBLE D'EVALUATION :

Dans ce document, la Cible d'évaluation est matérialisée par une fonction (service) de sécurité.

CIRCUITS ASSOCIES

Indique quels sont les circuits suivis par la procédure ou par les documents élaborés lors de l'application de la procédure.

DOCUMENTS EN SORTIE ET DESTINATAIRES

Noms et structure des documents en sortie élaborés lors de l'application de la procédure et liste des destinataires.

DOMAINE :

Etendue de la Cible d'évaluation

ENTREES

Noms des documents en entrée et/ou événements déclencheurs de l'action ou tâche à réaliser.

FREQUENCE ET/OU CALENDRIER D'APPLICATION

Indique la fréquence d'application de la procédure et/ou les dates.

INDICATEUR DE COMPARAISON :

L'indicateur de comparaison sert au calcul d'un autre indicateur au moyen d'un opérateur (ex : pour établir des ratios).

INDICATEUR DE MESURE :

Un indicateur est une donnée objective qui décrit une situation du strict point de vue qualitatif, qui constate un résultat.

INTERVENANT RESPONSABLE :

Acteur chargé de l'alimentation du tableau de bord.

OPERATEUR :

Opération élémentaire effectuée entre la mesure de l'indicateur composé et la mesure de l'indicateur de comparaison.

/ = Division

+ = Addition

- = Soustraction

x = Multiplication

PILOTE :

Responsable qui suit le tableau de bord, directement impliqué dans le processus de prise de décision en cas de dysfonctionnement et dans la fixation des nouveaux objectifs.

PONDERATION :

Elle hiérarchise l'indicateur (la pondération représente le degré d'importance attribué à un indicateur).

0	=	NEUTRE	è	Aucune importance
1	=	FAIBLE	è	Faible importance
2	=	SENSIBLE	è	Importance non négligeable
3	=	CRITIQUE	è	Importance déterminante
4	=	STRATEGIQUE	è	Importance capitale.

PROCEDURE :

Dans le cadre d'une politique qualité, la procédure écrite est la base de la formalisation du système qualité. Pour faciliter le management, l'exploitation et la capitalisation des procédures, nous proposons un modèle - la métaprocédure - qui tient compte de tous les éléments (hommes, activités, documents) qui ont une incidence ou qui sont affectés par les procédures.

Une procédure garantit l'exécution d'une tâche et assure qu'une même tâche est toujours réalisée de manière identique et surtout de la façon la plus adéquate. Elle permet également d'informer et de former les acteurs dans le but de minimiser les pertes relatives à la non qualité du processus.

La métaprocédure est le canevas de rédaction d'une procédure.

COMPOSITION DE LA METAPROCEDURE :

Domaine d'application ou activité
Service Responsable de la rédaction de la procédure
Service responsable de l'exécution de la procédure
Profil des acteurs
Action ou tâche à réaliser

Entrées
Documents en sortie et destinataires
Fréquence et / ou calendrier d'application
Circuits associés
Tableaux de bord associés
Règles à respecter

DOMAINE D'APPLICATION

Nom du domaine ou activité

Le domaine d'application : permet de regrouper les procédures par activité, peut être utilisé pour élaborer un manuel, peut servir d'index à l'intérieur d'un manuel.

SERVICE RESPONSABLE DE LA REDACTION DE LA PROCEDURE

Comporte :

Nom du service

Date de création de la procédure.

Date de validation de la procédure

Date de mise à jour de la procédure.

SERVICE RESPONSABLE DE L'EXECUTION DE LA PROCEDURE

Comporte :

Nom du service

Date de mise en application de la procédure

PROFIL DES ACTEURS

Permet de formaliser le profil :

Du responsable de la rédaction

Du responsable de la validation

Du responsable de la mise en application

Des exécutants

Du responsable de M.A.J.

REGLES

Indique les règles à respecter

SEUIL DE TOLERANCE :

Valeur à ne pas franchir et considérée comme limite acceptable (cette valeur fait partie des valeurs de référence).

STATUS :

Etat de la qualité de service constaté par un indicateur de mesure :

TRES BON = BLEU / BON = VERTE / MOYEN = JAUNE / MEDIOCRE = ORANGE /

MAUVAIS = ROUGE.

TABLEAU DE BORD (T.D.B.) :

Le T.D.B. est un outil de synthèse et de visualisation des situations décrites et des constats effectués par les indicateurs.

TABLEAU DE BORD

Indique le tableau de bord utilisateur de la procédure

TENDANCE D'UN INDICATEUR

Il y a trois types de tendances par indicateur :

AMELIORATION ↗ STATIONNAIRE ➔ DETERIORATION ↘

La tendance d'un indicateur se calcule sur la mesure d'une période "P" par rapport à la période

"P-1". Son interprétation exige leur rapprochement avec le statuS de l'indicateur.

VALEURS DE REFERENCE :

Ensemble de valeurs affectées à un indicateur servant de base pour qualifier et donner un status à la mesure faite. Parmi les valeurs de référence, on trouve la valeur cible à atteindre et la valeur fixée comme seuil de tolérance. Les valeurs de référence vont établir le modèle pour mesurer. On peut établir cinq valeurs de référence, chacune liée à un status.