LES DOSSIERS TECHNIQUES

Le tableau de bord de la sécurité, élément clé du dialogue RSSI/Directions

Octobre 2018

CLUB DE LA SECURITE DE L'INFORMATION FRANÇAIS

11 rue de Mogador - 75009 Paris

Tél. : +33 1 53 25 08 80 – Fax : +33 1 53 25 08 88

clusif@clusif.fr – www.clusif.fr

La loi du 11 mars 1957 n'autorisant, aux termes des alinéas 2 et 3 de l'article 41, d'une part, que les « copies ou reproductions strictement réservées à l'usage privé du copiste et non destinées à une utilisation collective » et, d'autre part, que les analyses et les courtes citations dans un but d'exemple et d'illustration, « toute représentation ou reproduction intégrale, ou partielle, faite sans le consentement de l'auteur ou de ayants droit ou ayants cause est illicite » (alinéa 1er de l'article 40)

Cette représentation ou reproduction, par quelque procédé que ce soit, constituerait donc une contrefaçon sanctionnée par les articles 425 et suivants du Code Pénal.

Table des matières

Remerciements

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

Le responsable du groupe de travail :

Frédéric	**MALMARTEL**	*ACOSS*

Le représentant du CDSE (Club des directeurs de sécurité et de sûreté des entreprises) :

Alain	**JEANDAT**	*EDF D.S.P.*

Les contributeurs :

Grégory	**ADROT**	*ARMAND THIERY SAS*
Thibault	**BASSET**	*MINISTERE DES ARMEES*
William	**BOURGEOIS**	*IN EXTENSO OPERATIONNEL*
Xavier	**CHAPELLE**	*TOTAL*
Frédérique	**DRON PARDO**	*POLE EMPLOI*
Emmanuel	**GARNIER**	*GIE AG2R REUNICA*
Cédric	**GASPARD**	*SYNETIS SAS*
Fabrice	**IDIER**	*CONSEIL DEPARTEMENTAL DE LA SEINE-SAINT-DENIS*
Guillaume	**KERMARREC**	*VEOLIA ENVIRONNEMENT*
Thomas	**LE GALLAIS**	*CDC CAISSE DES DEPOTS ET CONSIGNATIONS*
Alain	**MELAMED**	*CYBERSEL S.R.L.*
Hélène	**SAUVANT**	*IDNA*
Hervé	**SCHAUER**	*HS2 – HERVE SCHAUER SECURITE*
Dominique	**SOULIER**	*AGENCE DE LA BIOMEDECINE*

Le **CLUSIF** remercie également les adhérents ayant participé à la relecture.

I. Introduction

La gouvernance de la sécurité des systèmes d'information (SSI) doit permettre de maîtriser et, le cas échéant, réduire les risques dans une approche technique comme dans une stratégie globale. Elle doit tenir compte de la menace cyber, i.e. menace sur les réseaux et les systèmes informatiques, et aussi de toutes les contraintes existantes : obligations légales et réglementaires, besoins des métiers et évolutions technologiques notamment.

Elle justifie et maîtrise ses coûts.

Elle s'appuie sur les tableaux de bord de la SSI pour disposer d'une vision globale, stratégique et dynamique de la sécurité atteinte en regard de celle exigible. Ainsi sera-t-elle à même de remplir au mieux sa tâche en effectuant les meilleurs choix.

Le présent document propose un guide d'aide à la création de tableaux de bord de la SSI, destiné au lecteur désireux de la mettre en œuvre en s'appuyant sur eux.

Il décrit les bonnes pratiques en la matière. Il identifie les utilisateurs et les utilisations possibles des tableaux de bord ainsi que les principaux écueils à éviter. Il illustre ses propos par l'exemple. Des compléments sont donnés en annexe. Les exemples donnés ne prétendent pas à l'exhaustivité.

I.1. Définitions

I.1.1. Tableau de bord

Le tableau de bord est un ensemble structuré d'indicateurs objectifs et factuels, ce qui n'interdit pas d'être qualitatif. Il décrit, avec des éléments mesurables ou appréciables une situation et son évolution. Il se doit d'être synthétique pour être pertinent. Fonction de sa typologie, ses principaux objectifs sont de présenter :

- Une vision claire du niveau de sécurité et de conformité à des réglementations, des normes ou par rapport à une politique interne. L'efficacité des mesures de sécurisation des SI
- Les risques auxquels est exposée l'entité
- L'évolution de la sécurisation
- Le suivi et le contrôle des dépenses liées à la sécurité

Il concerne tous les publics. Il doit permettre : gain de temps, ergonomie dans le travail, efficacité, disponibilité, confidentialité des données personnelles et professionnelles… tant aux niveaux direction et cadres, qu'employés. Il aide à la prise de décision.

Il implique tous les acteurs principaux de la sécurité : Direction Générale, Responsable de la sécurité du système d'information (RSSI), opérationnels de la direction des systèmes d'information (DSI), services juridiques, services achats…

I.1.2. Indicateur

Un indicateur est une information quantitative ou qualitative obtenue à partir d'une mesure permettant de donner une idée raisonnable sur une thématique particulière de la SSI. Il doit être reproductible. Il permet d'identifier les actions à mener, communication comprise.

I.1.3. Typologie

Il existe trois niveaux de tableaux de bord : stratégique, de coordination et opérationnel. Ils sont décrits dans le chapitre suivant.

I.1.4. Normes et méthodologies existantes

Les normes et documents ci-dessous ont servi à bâtir le document :

- ISO 27004:2016 – *Management de la sécurité de l'information - Surveillance, mesurage, analyse et évaluation*.
- Cigref : 2007 – *Guide pratique pour un tableau de bord sécurité stratégique et opérationnel.*
- ANSSI : 2004 – *Elaboration de tableaux de bord SSI.*
- CLUSIF : 2001 – *Indicateurs de sécurité.*
- CLUSIF : 2008 – *Les métriques dans le cadre de la série 27000.*
- Swedish Civil Contingencies Agency : 2011 – *Information Security Metrics.*
- NIST SP 800-55.

II. Objectifs des tableaux de bord

Les tableaux de bord sont des outils de pilotage qui répondent à des objectifs différents selon leur typologie.

2 typologies d'indicateurs ont été identifiées :

- La catégorie « **Scorecard** » dans laquelle on trouve le tableau de bord de niveau **stratégique**.

- La catégorie « **Dashboard** » dans laquelle on trouve généralement 2 niveaux : le tableau de bord de **coordination** et le tableau de bord **opérationnel**.

Il existe également une notion de tableau de bord éphémère, qui peut être construit pour réaliser un suivi d'activité en rapport avec l'actualité.

Par exemple, dans le cadre d'une faille de sécurité annoncée, il permettra de faire un point de situation en regard de l'exposition de l'organisation à cette faille, d'identifier les actions de maîtrise à définir, et informer sur le suivi de ces actions.

Une fois la faille pleinement maîtrisée, ce tableau de bord éphémère ne sera pas reconduit. Il dispose ainsi d'une durée de vie limitée. Il est important que la **filière sécurité SI (ou filière SSI)** partage l'ensemble des informations de ces tableaux de bord (toutes typologies et niveaux confondus). Par filière SSI, nous entendons l'ensemble des acteurs contribuant au travers de leurs missions quotidiennes à la sécurité des systèmes d'information (on parle également de « chaîne fonctionnelle de la sécurité des SI »)

II.1. Le niveau Stratégique

Ce niveau correspond au niveau de suivi le plus élevé. Il permet de consolider une vision des risques SSI au niveau de l'organisation.

Les indicateurs permettent de fixer des orientations à court, moyen et long terme, de mesurer la performance de la sécurité et de donner un éclairage sur la connaissance des risques pour les directions, les autorités de tutelle, les partenaires, etc.

Ils peuvent également être utiles pour obtenir des financements compte tenu des risques à traiter.

Aussi, ils peuvent être utilisés par l'entité qui a en charge la communication.

Quelques exemples de thèmes couverts :

- Cartographie des risques (évolution, nombre de risques majeurs, …)
- Plans d'action : mise en œuvre de la politique de sécurité, de correctifs, …
- Dépenses liées à la sécurité (formation, sensibilisation, investissements, …)

II.2. Le niveau Coordination

Ce niveau correspond au niveau de suivi intermédiaire et permet de fournir une vision consolidée des risques SSI pour chaque thématique.

Les indicateurs donnent un éclairage sur la connaissance des risques et leur maîtrise, ils servent également aux autres directions de l'organisation (métier ou support), aux autorités de tutelle, si elles existent, ainsi qu'à des partenaires.

Quelques exemples de thèmes couverts :

- Nombre de sessions de sensibilisation à la sécurité ;
- Suivi des participations à ces formations ;
- Identification et suivi des publics les plus sensibles ;
- Etc.

II.3. Le niveau Opérationnel

Ce niveau correspond au niveau le plus granulaire et le plus proche du « terrain ».

Ces indicateurs sont utiles pour les opérationnels en usage interne, ils peuvent également donner de la visibilité à l'ensemble des acteurs de la sécurité de l'information (la filière SSI) et à la DSI ou une autre entité, garante du niveau opérationnel de sécurité.

Quelques exemples de thèmes couverts :

- Nombre de failles logicielles / applicatives ;
- Suivi des mises à jour logicielles, progicielles et des systèmes d'exploitation ;
- Bilan des alertes et incidents survenus (*) ;
- Bilan des audits et des tests de vulnérabilité éventuels (*) ;
- Nombre de personnes habilitées en fonction des différents niveaux d'authentification ;
- Fréquence des mises à jour des actifs (postes de travail, pare-feux, routeurs, anti-virus, systèmes…) et des alertes ;
- Suivi du déploiement de ces mises à jour ;
- Nombre d'équipements par version d'OS déployée ;
- …

Il est possible d'aborder les indicateurs de la sécurité de l'information par thématique, en faisant le rapprochement avec celles de la norme ISO27002-2013 (cf. exemple en annexe).

(*) Si non reportés au niveau des autres reportings.

Le tableau ci-dessous récapitule les usages des tableaux de bord en fonction de leur nature :

	Usage interne	**Filières SSI**	**DSI** **(ou toute entité de l'entreprise responsable d'outils informatiques (IT classique, SCADA…)**	**Directions, autorités de tutelle, partenaires**
Stratégique	Alimenter une communication	Fixer des orientations	Obtenir des financements	Connaître les risques et leur gravité
Coordination		Disposer de reporting		Connaître les plans d'action de maîtrise des risques et leur avancement
Opérationnel	Aider les opérationnels	Donner de la visibilité opérationnelle	Suivre les actions « terrain »	

Les autorités de tutelle peuvent imposer des obligations, qui se traduisent par des indicateurs types afin de montrer la bonne conformité, notamment dans les contextes d'Opérateur d'Importance Vitale (OIV) et d'Opérateur de Service Essentiel (OSE).

III. Comment procéder, quelle granularité ?

III.1. Les acteurs

Pour concevoir correctement un tableau, il est essentiel d'identifier l'ensemble des acteurs de la chaîne de la plus haute instance dirigeante jusqu'au responsable de la mise en œuvre du système d'information. Il est impératif que chaque acteur de la filière SSI soit impliqué au juste niveau.

Parmi les acteurs du tableau de bord, nous distinguerons deux catégories : les clients et les fournisseurs. La même entité peut être client ou fournisseur, suivant les circonstances. Nous retrouvons dans ces deux catégories les trois niveaux (stratégique, coordination et opérationnel).

Il sera essentiel d'adapter le contenu des tableaux de bord au niveau de maturité du client ou du fournisseur.

La confidentialité doit être préservée.

Clients[1] :

- **Stratégique** : Le comité exécutif, le comité directeur, le haut fonctionnaire de défense et sécurité, la fonction SSI, etc. ;
- **Coordination** : La direction des systèmes d'information, le bureau « gouvernance », la direction des risques, etc. ;
- **Opérationnel** : Le COS[2], la division opérations, etc.

Fournisseurs[3] :

- **Stratégique** : La direction des systèmes d'information, le RSSI, le DPO[4], la direction des risques, etc. ;
- **Coordination** : Le COS, le service clients, etc. ;
- **Opérationnel** : Le COS, les équipes techniques et sous-traitants, etc.

Il est impératif d'impliquer chaque fournisseur de manière durable en lui présentant la finalité de son travail. Remplir des tableaux et des indicateurs sans objectif concret peut rapidement s'avérer fastidieux et lassant. En partageant les objectifs et finalités supérieures avec les fournisseurs, l'implication de chaque acteur s'inscrit dans la durée.

[1] Les destinataires du tableau de bord
[2] COS : Centre Opérationnel de Sécurité
[3] Fournisseurs : Les contributeurs et responsables de la fourniture des indicateurs
[4] Data Protection Officer ou Délégué à la protection des données (DPD)

Le service communication de l'entreprise est également un acteur essentiel dans la mise en forme du tableau, il permettra de :

- Gagner en lisibilité ;
- Répondre aux objectifs de visibilité du tableau ;
- Atteindre la cible efficacement.

III.2. La construction

L'élément clé de la construction d'un tableau de bord commence par la conception des indicateurs et les différents niveaux de vues du tableau de bord. Plusieurs perspectives seront alors nécessaires afin d'avoir un impact adéquat sur chaque niveau de clients.

La détermination des éléments primordiaux à présenter, en fonction de la vue souhaitée, sera à déterminer par le responsable du tableau de bord stratégique au sein de l'organisme. Il connaît les Indicateurs Clés de Performances (ICP/KPI) qui relèvent du niveau stratégique. Il sera en général intéressé par le niveau de vulnérabilité des systèmes d'information aux menaces à forte médiatisation (par exemple en 2017 : Wannacry et NotPetya), le niveau de conformité aux normes et règlements impactant son activité, etc.

En ce qui concerne la collecte des informations, il est préférable de récupérer et de traiter l'ensemble des indicateurs de manière automatisée (exemple : collecteurs de données installés sur les équipements).

Dans l'idéal, un tableau de bord doit se mettre à jour automatiquement. L'utilisation d'une base de données ainsi qu'un outil de visualisation est incontournable. Il permet d'avoir un rendu clair et reproductible.

III.3. Bonnes pratiques

Nous identifions quelques points importants lors de la construction d'un tableau de bord. Ces éléments sont donnés à titre indicatif. Ils peuvent varier en fonction des organismes, de leur taille et de leur secteur d'activité :

- Pour une communication efficace, les points critiques devront être immédiatement lisibles grâce à des chiffres clairs et des couleurs savamment choisies (si possible dans la charte graphique de l'organisme)
- Le tableau de bord doit être en corrélation avec l'actualité de l'organisme
    - Incident informatique récent au sein de l'entreprise
    - Période critique pour l'entreprise (exemple : clôture des comptes)
- Le tableau de bord doit répondre aux objectifs de l'organisme (exemple : transformation numérique) ou encore aux demandes particulières des instances dirigeantes
- Il est important de mettre en avant la couverture sécurité apportée par les équipes

afin de prouver la valeur apportée à l'organisme par ces dernières. La sécurité informatique est souvent vue comme un coût et non un gain

- Le tableau de bord peut être dissocié en deux parties, une avec les indicateurs courants et une autre sur l'évolution de la sécurité sur l'année
- Toutes les données du tableau de bord doivent pouvoir être expliquées par le présentateur (exemple : baisse du niveau de correctifs, augmentation du nombre d'ordinateurs détectés, etc.)
- Proposer un tableau de bord récapitulant l'état du parc (Système d'Exploitation utilisé), tant pour les ordinateurs que pour les smartphones. Des prévisions pourront ainsi être réalisées depuis le tableau de bord
- Identifier les éléments pouvant faire fluctuer les indicateurs (exemple : niveau de déploiement des correctifs et attaques de logiciels malfaisants)
- Le tableau de bord est itératif, il évoluera grâce au gain en pertinence de ces indicateurs et à la plus grande précision de ces derniers. Il restera toutefois limité, pour se concentrer sur l'essentiel

III.4. La granularité

Quel que soit le niveau de tableau de bord (stratégique, de coordination ou opérationnel), éphémère ou non, le niveau de granularité doit être celui attendu par le client. Il dépend de l'organisation et des objectifs définis par les instances dirigeantes. Les données doivent être mesurées et présentées selon une approche basée sur l'analyse des risques pour l'organisme.

Le type et le détail des indicateurs sont liés au niveau de maturité de l'organisme en matière de SSI.

Identifier et mettre en place un système de mesure avec le bon niveau de détails nécessite un processus itératif et une amélioration continue du dispositif. Le niveau de détails choisi doit permettre de visualiser les tendances sur plusieurs exercices tout en garantissant une flexibilité pour améliorer le tableau de bord en particulier en fonction de la menace cyber en forte évolution.

La bonne granularité s'apprécie via la pérennité du tableau de bord. Elle ne doit pas être modifiée à chaque changement d'acteur.

La concaténation d'indicateurs opérationnels peut déboucher sur des indicateurs stratégiques. Ce modèle d'indicateurs ascendants, bien que très utile, peut s'avérer difficile à construire.

III.5. Tableau de bord stratégique

Le niveau d'information doit être le plus synthétique possible et répondre à la question principale des plus hautes instances de l'organisme : quel est le niveau d'exposition aux risques pour les métiers et la continuité de l'activité ?

Pour répondre à cette question centrale, les éléments suivants doivent être présentés ou rappelés avant tout indicateur cybersécurité propre à l'entreprise :

- La description générale du SI de l'entreprise et les zones de risque cybersécurité
- L'état de la menace cyber globale et les conséquences possibles pour l'entreprise
- La stratégie DSI et son volet cybersécurité intégré

Le tableau de bord peut alors présenter les indicateurs pertinents des contrôles opérationnels, des analyses de risques ou des audits.

Sur le volet opérationnel et toujours de manière la plus concise, les indicateurs ci-dessous peuvent être proposés :

- Taux d'applications configurées de manière non sécurisée ;
- Taux de projets menés selon les règles de la politique de sécurité SI ;
- Nombre d'exceptions à la PSSI ;
- Taux d'accès privilégiés non en règle ;
- Nombre d'incidents de sécurité SI significatifs et d'événements ;
- Nombre de violations de données à caractère personnel (art. 33 du RGPD) ;
- Taux de postes de travail et de serveurs à jour des correctifs de sécurité (en cas de crise) ;
- Taux de postes de travail et de serveurs protégés par un dispositif antiviral à jour ;
- Taux de collaborateurs sensibilisés à la cybersécurité.

Concernant le volet des analyses de risques et des audits, les indicateurs suivants sont pertinents :

- Nombre d'analyses de risques nouvelles ou mises à jour ;
- Nombre de risques critiques couverts / non couverts ;
- Nombre de risques critiques réduits ;
- Nombre et type de nouveaux risques.

Un indicateur présentant le niveau de gestion de risque cybersécurité de l'organisme par rapport à ses pairs est une information stratégique intéressante. La notation cyber peut ainsi être présentée comme un bon complément par cette vision extérieure proposée par les agences cyber. Si l'auditeur a accès aux données internes de l'organisme, alors la notation pourra être considérée de meilleure qualité car plus complète.

La précision du tableau de bord stratégique tient d'abord dans celle des messages qui supportent ou accompagnent les indicateurs. C'est l'élément idéal pour communiquer aux instances dirigeantes de l'organisme.

III.6. Tableau de bord de coordination

Le tableau de bord de coordination est une synthèse du tableau de bord opérationnel. A ce titre, le niveau d'information doit correspondre à un résumé des indicateurs opérationnels, se concentrant sur les priorités des instances de coordination.

Le tableau de bord de coordination doit présenter des indicateurs plus détaillés et plus techniques que ceux du tableau de bord stratégique. Il peut présenter les conséquences des manques constatés. Cela permet aux responsables de ce niveau une prise de décision avec des impacts dans la gestion du risque et en lien avec les responsables métiers.

Les indicateurs peuvent se répartir comme suit selon les principes clés :

Organisation / Prévention cybersécurité

- Etat du cadre normatif (ex : date dernière mise à jour de la politique SSI). Allocation des ressources (ex : nombre de fonctions allouées par rapport aux besoins)
- Compétences : nombre et types de compétences assurées / Nombre et type de compétences nécessaires
- Nombre d'actions de sensibilisation et résultats obtenus
- Nombre d'actions de formation

Dispositif technique

- Nombre d'incidents avérés ou d'incidents frôlés (classés selon une échelle d'impact)
- Nombre d'alertes

Etat du parc applicatif

- Nombre d'applications configurées de manière sécurisée (revue de code, correctifs, SSO)
- Taux de revue des accès logiques (standards et privilégiés)
- Estimation du shadow IT

Etat de l'infrastructure

- Taux de postes de travail et serveurs disposant des derniers correctifs
- Taux de postes de travail et serveurs disposant d'un logiciel antiviral à jour
- Taux de revue des règles pare-feux

Dispositif d'analyse de risques

- Nombre d'audits réalisés et classés par résultats
- Nombre d'analyses de risques effectuées et classées par résultats
- Suivi des plans d'actions : indicateur sur les actions en cours

III.7. Tableau de bord opérationnel

Le tableau de bord opérationnel est l'outil de pilotage pour les responsables cybersécurité et techniques. Les informations collectées et traitées peuvent ainsi avoir un niveau de détail très important toujours en fonction des besoins de l'entreprise. Aussi, sans pouvoir en faire une liste exhaustive, ces indicateurs peuvent être les suivants :

Politique de sécurité

- Mise à jour de la charte informatique ;
- Mise à jour de la politique de sécurité des SI ;
- Nombre de dispenses au référentiel par règles, thématiques et répartis par activités métiers.

Etat du parc applicatif – Informations détaillés par applications disponibles

- Nombre d'applications ayant fait l'objet d'un audit
- Nombre d'applications ayant fait l'objet d'un test d'intrusion
- Taux d'accès standard recertifiés
- Taux d'accès privilégiés recertifiés
- Niveau d'authentification approprié
- Besoins de continuité d'activité exprimés par le métier
- Réalisation et résultats de tests de reprise d'activité
- Taux d'installation des correctifs de sécurité par application
- Nombre de vulnérabilités en fonction d'une échelle de criticité
- Estimation chiffrée et type de shadow IT

Etat de l'infrastructure

- Taux de postes de travail (par environnement) avec les derniers correctifs de sécurité ;
- Taux de serveurs (par environnement) avec les derniers correctifs de sécurité
- Taux de postes de travail (par environnement) avec un logiciel antiviral à jour
- Taux de serveurs (par environnement) avec un logiciel antiviral à jour
- Taux de règles pare-feux revues selon une fréquence donnée
- Taux de règles pare-feux non conformes
- Taux d'accès utilisateurs revus et approuvés
- Taux d'accès privilégiés revus et approuvés
- Niveau d'expression de besoins en continuité / reprise d'activité
- Nombre et résultats des tests de continuité / reprise d'activité

III.8. Tableau de bord « éphémère »

Le tableau de bord éphémère se construira souvent dans l'urgence de situations exceptionnelles. Cependant dans certains cas il s'inscrira dans le temps et pourra parfois

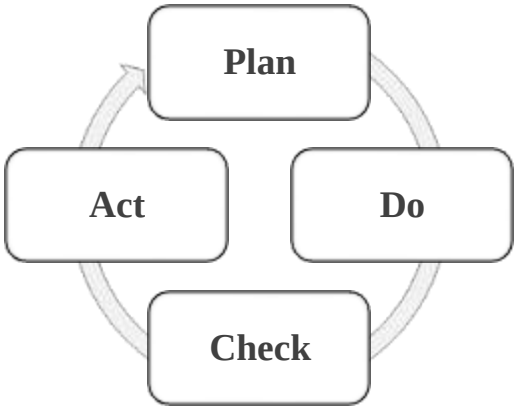
intégrer les tableaux de bord standards. Il doit présenter des indicateurs permettant de gérer et de comprendre une situation d'exception, avec des incidents avérés ou potentiels. Il doit permettre à chaque niveau d'avoir une visualisation rapide sur les conséquences de la situation. Les indicateurs doivent être précis et mis à jour le plus fréquemment possible. Dans cette optique, les indicateurs ci-dessous semblent pertinents vis à vis de la menace cybersécurité connue en 2018 :

- Nombre et type de vulnérabilités critiques existantes (en précisant le nombre et le type de systèmes concernés) ;
- Taux de postes de travail et serveurs disposant d'un correctif de sécurité identifié ;
- Taux de postes de travail et serveurs disposant d'une signature antivirale identifiée.

Il faut également savoir relativiser et pondérer les risques au vu des mesures organisationnelles ou techniques présentes sur les systèmes d'information.

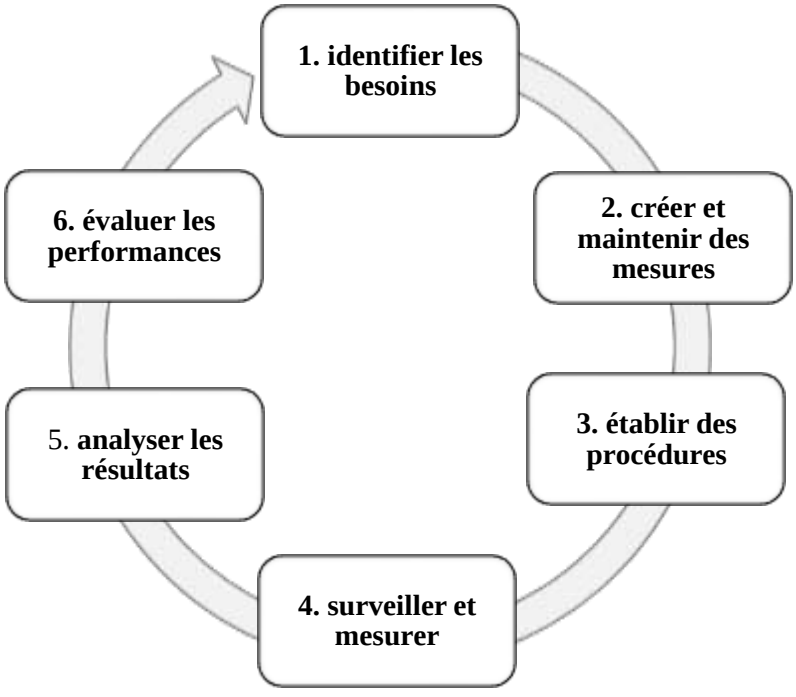
IV. Cycle et dynamique de vie des tableaux de bord.

Comme pour tout élément évolutif, le principe de Deming s'applique également au tableau de bord dans son amélioration continue. Toutefois, il est important de ne pas confondre le principe d'amélioration continue qui s'applique à la création et à l'évolution du tableau de bord avec les processus de mesure et d'évaluation d'un indicateur qui sont des valeurs inhérentes à la norme ISO 27004.



Le tableau de bord de la sécurité des systèmes d'information en s'inscrivant dans une démarche d'amélioration continue, s'appuie alors sur des processus de surveillance, de mesure, d'analyse et d'évaluation que l'on peut décomposer, en reprenant le découpage proposé par la norme ISO/IEC 27004 :2016, de la façon suivante :

1. Identifier les besoins d'information
2. Créer et maintenir des mesures
3. Établir des procédures
4. Surveiller et mesurer
5. Analyser les résultats
6. Évaluer les performances de sécurité de l'information et l'efficacité du système de gestion de la sécurité de l'information (SMSI)



IV.1. PLAN : Identifier les besoins d'information

Les indicateurs créés ou revus répondent à des besoins d'information. L'identification de ces besoins doit être menée tout au long de la vie des tableaux de bord car ils évoluent avec le temps.

La démarche d'identification des besoins d'information doit rester pragmatique en s'appuyant sur les indicateurs à disposition et en interrogeant les différents acteurs ou décideurs.

Les commentaires lors des présentations des tableaux de bord doivent être pris en compte pour bien comprendre les demandes et les besoins d'information.

Des documents de référence peuvent être utilisés, tel que :

- Les attentes spécifiques de la direction ;
- La stratégie de l'organisation ;
- La politique de sécurité des systèmes d'information ;
- La cartographie des risques.

L'identification des indicateurs pertinents peut s'appuyer sur une démarche rationnelle :

- Examiner le SMSI, ses processus et d'autres éléments tels que :
  1. Les recommandations, politique de sécurité, plan de sécurisation
  2. Les exigences légales, réglementaires, contractuelles et organisationnelles pour la sécurité de l'information
  3. Les résultats du processus de gestion des risques liés à la sécurité de l'information

- Prioriser les besoins d'information identifiés en fonction de critères, tels que :
  1. Les urgences de traitement des risques
  2. Les capacités et les ressources de l'organisation
  3. Les besoins des parties intéressées
  4. La politique de sécurité du système d'information et les objectifs de contrôle
  5. L'information requise pour respecter l'obligation organisationnelle, juridique, réglementaire et contractuelle
  6. La valeur de l'information par rapport au coût de la mesure et difficultés d'obtention

- Sélectionner un sous-ensemble restreint des besoins d'information à partir de la liste des indicateurs possibles
- Documenter et communiquer les besoins d'information sélectionnés à toutes les parties intéressées

Dans la pratique, il est parfois nécessaire de produire plusieurs versions du tableau de bord. En utilisant les premières remontées, les commentaires, il est alors possible de faire évoluer le tableau de bord qui gagne progressivement en maturité.

Les indicateurs sont ainsi utilisés avec pertinence et discernement selon la maturité : on peut imaginer une phase de démarrage, de croissance et de maturité. A chaque étape, les indicateurs pourront être différents et permettre le cas échéant d'initier des actions correctrices et de progresser de manière pragmatique tout en permettant de mesurer l'agissement suivi par la partie intéressée. A chaque indicateur, une valeur cible et un responsable de collecte doivent être définis en concertation avec les secteurs d'activités concernés.

IV.2. DO : Création et maintien des indicateurs

Les indicateurs sont d'abord créés puis révisés et mis à jour systématiquement selon des intervalles planifiés préétablis.

En cas de changements substantiels sur le SMSI, le tableau de bord bien évidemment évolue (par exemple dans le cas de modification des objectifs SMSI, modification de l'organigramme ou de la structure de l'organisation, modification des responsabilités, rôles des parties intéressées, modification des objectifs commerciaux, nouvelles exigences légales ou réglementaires…).

La création ou la mise à jour des indicateurs inclut les étapes suivantes :

1. Identifier les pratiques de sécurité actuelles pouvant répondre aux besoins d'information
2. Développer ou mettre à jour des indicateurs
3. Documenter les mesures et définir la priorité de mise en œuvre
4. Tenir la direction informée et engagée

La mise à jour des indicateurs prend moins de temps et d'effort que la création initiale.

a) Identifier les pratiques de sécurité actuelles pouvant répondre aux besoins d'information

Une fois qu'un besoin d'information est identifié, il convient de répertorier les pratiques de mesure et de sécurité existantes (par exemple cartographie des risques, gestion de projet, rapports de conformité, politique de sécurité).

Une démarche pragmatique consistera à commencer avec des indicateurs à disposition.

b) Développer ou mettre à jour des indicateurs

Les mesures doivent répondre au besoin d'information. Elles peuvent s'appuyer sur les pratiques actuelles ou nouvelles. Les mesures nouvellement identifiées peuvent également impliquer une adaptation des mesures et des processus existants. Dans tous les cas, les indicateurs identifiés sont définis de manière suffisamment détaillée pour permettre la mise en œuvre des mesures correspondantes aux attentes.

Exemples de données pouvant être collectées :

1. Sortie de divers journaux et analyses
2. Statistiques sur la formation et d'autres activités liées aux ressources humaines
3. Enquêtes et questionnaires pertinents
4. Statistiques d'incidents
5. Résultats des audits internes et des tests d'intrusions
6. Résultats des exercices des plans de continuité des activités et/ou de reprise après sinistre
7. Rapports des revues de direction

Ces sources de données potentielles d'origine interne ou externe sont examinées pour déterminer les données disponibles.

Les indicateurs sélectionnés correspondent aux priorités définies en prenant en compte les critères suivants :

- Facilité de la collecte de données
- Disponibilité des ressources humaines pour collecter et gérer les données
- Disponibilité d'outils logiciels appropriés
- Facilité d'interprétation
- Nombre d'utilisateurs des résultats
- Preuves démontrant l'adéquation de la mesure à l'objectif ou au besoin d'information
- Coûts de collecte, de gestion et d'analyse des données

Il faut savoir également retirer des indicateurs pour gagner en lisibilité sur le tableau de bord global et s'assurer que les indicateurs exploités restent pertinents.

L'historisation des indicateurs « éliminés » et des tableaux de bord « éphémères » est organisée.

c) Documenter les mesures et définir la priorité de mise en œuvre

Les indicateurs sont documentés. La mise en œuvre des indicateurs est fonction de la priorité de chaque besoin d'information et de la faisabilité de l'obtention des données.

Les mesures de performance doivent d'abord être implémentées pour s'assurer de la mise en œuvre des processus et contrôles du SMSI. Les mesures d'efficacité sont ensuite mises en œuvre.

d) Tenir la direction informée et engagée

Les différents niveaux organisationnels sont impliqués dans l'élaboration et la mise en œuvre des mesures, afin qu'elles reflètent les besoins de la direction.

La direction reçoit les mises à jour régulières dans des formats et des styles appropriés, afin de s'assurer qu'elle reste informée des activités tout au long du cycle de vie des tableaux de bord.

IV.3. DO : Établir des procédures

Pour mettre en œuvre des indicateurs définis et hiérarchisés, les mesures suivantes doivent être prises :

- Les parties intéressées sont informées de la mise en œuvre ou de l'évolution d'un tableau de bord de suivi et de la justification ;
- Les outils de collecte et d'analyse de données sont identifiés et, si nécessaire, modifiés, afin de recueillir des mesures de manière efficace et efficiente.

Des procédures sont alors établies pour la collecte de données, l'analyse et la notification des mesures. Les procédures doivent définir les méthodes de collecte, de stockage, d'intégrité et quelles informations contextuelles sont nécessaires pour un traitement ultérieur. Par exemple, la vérification des données s'effectue en s'assurant que la valeur :

- Se situe dans une étendue acceptable ;
- Est conforme à l'intervalle attendu ;
- Que l'horodatage de collecte soit correct.

Les procédures spécifient aussi les techniques d'analyse des données et la fréquence de notification des mesures résultantes.

Enfin, la norme ISO 27004 indique que les méthodes et les formats de rapport doivent inclure :

- un tableau de bord fournissant des informations stratégiques et intégrant des indicateurs de performance de haut niveau ;
- des tableaux de bord exécutifs et opérationnels axés sur des objectifs stratégiques plutôt que sur des contrôles et des processus spécifiques ;
- des formats de rapport aux styles simples et statiques ;
    - par exemple : une liste de mesures pour une période donnée ;
- des rapports de références croisées plus sophistiqués avec des regroupements imbriqués et des analyses dynamiques ;
    - par exemple : des jauges pour représenter les valeurs et les alertes.

On pourra s'appuyer sur un RACI pour définir les rôles et responsabilités dans la construction des indicateurs et tableaux de bord.

IV.4. CHECK : Surveiller et mesurer

Les procédures de surveillance et de mesures effectuées, de stockage et de vérification (par des moyens manuels ou automatisés) sont définies initialement et peuvent être revues en cas de difficultés constatées et justifiées.

La vérification des données s'effectue en qualifiant les données recueillies par rapport à une liste de contrôle (adéquation des valeurs dans des limites reconnues). Aux fins de l'analyse,

des données suffisantes devraient être recueillies pour s'assurer que les résultats de l'analyse sont fiables.

L'analyse s'appuie sur le recueil de données suffisamment légitimes et fiables sur une périodicité établie.

En fonction des contraintes, il peut être envisagé de mettre à jour ces processus de surveillance, de mesure, d'analyse et d'évaluation.

Certaines données relatives à la sécurité des informations peuvent être confidentielles. Aussi, avant de publier des informations dans des rapports, des tableaux de bord, etc., l'organisation doit déterminer comment les données et les résultats collectés peuvent être partagés et avec qui.

De plus, il y a avantage à avoir une méthode pour vérifier et évaluer le processus de collecte afin de confirmer que de bonnes mesures sont recueillies et qu'elles sont répétables, précises et cohérentes.

IV.5. ACT : Analyser les résultats

Les données collectées sont analysées par rapport à la cible ou l'objectif. Des conseils pour effectuer des analyses statistiques peuvent être trouvés dans ISO / TR 10017:2003.

Les résultats de l'analyse des données doivent être interprétés. La personne analysant les résultats doit être capable de tirer les premières conclusions à confirmer avec les pilotes des activités concernées. Toutes les interprétations doivent tenir compte du contexte des mesures.

L'analyse des données doit identifier les écarts entre les résultats de mesure attendus et réels (cf. SMSI). Les lacunes identifiées peuvent indiquer la nécessité d'améliorer le SMSI mis en œuvre, y compris ses politiques, ses objectifs, ses contrôles, ses processus et ses procédures.

IV.6. ACT : Évaluer les performances de sécurité de l'information et l'efficacité du SMSI

Comme pour le SMSI, le tableau de bord doit être efficace et efficient sur le long terme, il doit donc s'adapter aux changements qui ont lieu dans l'environnement interne et externe.

Le tableau de bord, en tant qu'outil de pilotage, permet de s'assurer du parfait fonctionnement de son système de gestion de la sécurité et doit donc signaler les écarts et les dysfonctionnements constatés sur les mesures de sécurité décidées et validées avec la direction. Il devient alors une véritable tour de contrôle qui fournit des indicateurs pertinents et met en évidence les points les plus vulnérables du système d'information.

Si durant les revues du tableau de bord, il est constaté que les écarts sont réguliers ou deviennent permanents, il permet alors de s'interroger sur les moyens matériels, financiers et humains mis en œuvre pour atteindre les objectifs fixés. C'est pourquoi, pour chaque mesure mise en œuvre, un indicateur doit permettre de quantifier son efficacité et contrôler l'état global d'avancement du déploiement des politiques de sécurité.

Le tableau de bord général indiquera l'efficacité globale du SMSI. Le RSSI sera alors en mesure de justifier l'efficacité des choix techniques et organisationnels mis en place pour protéger les biens essentiels et le cas échéant, justifier des projets, des évolutions de l'existant et des budgets complémentaires visant à couvrir le risque résiduel. Le bien essentiel pouvant lui-même faire l'objet d'un indicateur plus spécifique à destination des métiers.

La norme ISO 27001:2013 précise les questions à se poser. Quoi surveiller et mesurer ? Quel point à surveiller et à mesurer ? Quand les résultats doivent être analysés et évalués ? Qui doit surveiller et mesurer ? Qui doit analyser et évaluer les résultats ?

Dans ce cadre, les organisations doivent exprimer leurs besoins d'information concernant la performance et l'efficacité du SMSI et préciser leurs indicateurs souhaités en fonction de ces besoins d'information.

L'analyse des résultats doit fournir des données pouvant être utilisées pour satisfaire les besoins d'information. L'évaluation est le processus d'interprétation de ces données pour répondre à la performance de SSI de l'organisation et aux questions d'efficacité du SMSI.

IV.7. ACT : Examiner et améliorer les processus de surveillance, de mesure, d'analyse et d'évaluation

Les processus de contrôle, de mesure, d'analyse et d'évaluation devraient continuellement s'améliorer avec les besoins du SMSI. Les activités d'amélioration continue peuvent inclure, entre autres :

a) la sollicitation des commentaires des parties intéressées

b) la révision des techniques de collecte et d'analyse, sur la base des enseignements tirés

c) la révision des procédures de mise en œuvre

d) la vérification des données d'étalonnage

IV.8. ACT : Conserver et communiquer des informations documentées

Conformément aux exigences de la norme ISO 27001:2013, il est nécessaire de conserver les mesures des indicateurs comme preuve du suivi. Les organisations sont libres de décider ce qui est approprié. Elles peuvent, par exemple, documenter le processus et les méthodes utilisées pour analyser et évaluer les résultats.

Les résultats de l'analyse des données doivent être documentés. Les rapports communiqués aux parties prenantes sont réalisés avec des formats appropriés et adaptés. Les conclusions de l'analyse doivent être examinées par les parties prenantes afin de garantir une interprétation correcte des données.

Comme indiqué par la norme ISO 27004, l'analyste doit déterminer comment communiquer les résultats des mesures en se posant les questions suivantes :

a) quels sont les résultats qui doivent être communiqués à l'interne et à l'externe ;

b) quelle est la liste des mesures pour chaque partie prenante ;

c) quelle est la fourniture des résultats spécifiques et le type de présentation adapté aux besoins de chaque groupe ;

d) quels sont les moyens permettant d'obtenir des commentaires des parties prenantes.

Ces commentaires seront utilisés pour évaluer l'utilité des résultats et l'efficacité de la mesure.

IV.9. Prise en compte de l'environnement interne et externe

Une fois construit, le tableau de bord évoluera tout au long de son usage en fonction des besoins de l'organisme et des mesures de sécurité prises pour protéger le patrimoine de l'entreprise. Cette métamorphose continue de l'information mise à disposition des équipes techniques, des métiers et des dirigeants, devra tenir compte des contraintes, nombreuses, que rencontrera l'organisme. En effet, ce dernier évolue de manière permanente pour s'adapter aux besoins de son secteur. Il est alors impératif de veiller à s'assurer que les indicateurs et les tableaux de bord accompagnent cette évolution.

Il est important de distinguer deux types de contraintes :

- ✓ Celles internes, qui concernent les restructurations techniques et organisationnelles, l'évolution du système d'information ou les exercices budgétaires ;
- ✓ Celles externes, liées à l'actualité politique, commerciale ou réglementaire, aux opportunités diverses ainsi qu'aux clients, fournisseurs et partenaires.

IV.9.1. Environnement Interne

Pour maintenir un tableau de bord en phase avec les besoins définis lors de la construction, il sera nécessaire de toujours disposer des ressources, à la fois matérielles, qui alimentent les indicateurs en données techniques, mais aussi humaines, qui assurent la cohérence et la mise en forme.

Dans la rupture de génération de tableaux de bord il y a d'abord le cas de ce qui n'a pas été automatisé : les gens ne répondent plus ou de manière inexacte, etc…

A chaque gestion du changement la donnée qui sert à documenter un indicateur peut être absente.

Une rupture dans la génération des tableaux de bord peut aussi être provoquée par des changements majeurs :

- refonte profonde de l'architecture du SI ;
- modification de stockage des données susceptible de perturber l'approvisionnement des indicateurs ;
- réorganisation des ressources en charge de leur mise en forme.

Afin de se prémunir du risque d'interruption, il est impératif de lister/cartographier les besoins vitaux.

Ressources matérielles

Lorsque les mesures d'un indicateur se basent sur un ou plusieurs biens, il est impératif de veiller à ce que ces derniers soient toujours disponibles et qu'un changement ou une suppression de solution soit suivi par une mise à jour de son indicateur. Par exemple, pour un indicateur mesurant le taux d'utilisation d'une passerelle VPN, si la solution d'accès distant change, elle provoquera une rupture dans l'alimentation en données si l'équipe en charge de la conception des indicateurs n'a pas été mise au courant de la modification.

Les indicateurs techniques sont alimentés à partir de sources d'information des actifs, souvent les fichiers journaux, jugées fiables par les équipes techniques et donc à même de fournir des données pertinentes. Il convient alors de s'assurer que les actifs produisant les événements sont en mesure de les exporter et les plateformes chargées de les collecter et de les traiter soient capables de les recevoir. Cela implique alors pour les uns et les autres qu'ils disposent de suffisamment de ressources :

- ✓ Temps processeur et mémoire vive pour générer traiter les événements ;
- ✓ Espace de stockage suffisant pour écrire et stoker les fichiers journaux ;
- ✓ Infrastructure réseau fiable pour le transfert des journaux ;
- ✓ …

Il est donc pertinent de mettre en œuvre une supervision fine des biens et services nécessaires à l'alimentation des indicateurs. Cette supervision fera alors elle aussi l'objet d'indicateurs et d'un tableau de bord permettant d'en mesurer l'efficacité.

La temporalité étant un élément important dans la comparaison des indicateurs, il est impératif de s'assurer de leur horodatage. Une datation erronée des événements induira des indicateurs non pertinents et donc inutilisables. Il faudra alors s'assurer que chaque actif dispose d'une source fiable et commune de temps.

Ressources humaines

Les ressources humaines interviennent à la fois dans l'alimentation des indicateurs en données non informatisées ou dans la pondération des données techniques existantes du fait de leur connaissance du système d'information. Une absence ou un départ ne doit pas impacter la cohérence et la pertinence des données. Il convient alors de s'assurer que, au sein d'une équipe, le niveau de connaissance et de compréhension des méthodes et des procédures soit le même pour tous. Les transferts de compétences doivent être assurés de manière continue afin de se prémunir de l'absence d'une ressource. De plus, lorsque les intervenants sont externes, il sera nécessaire de contractualiser une continuité de service sans perte d'information.

Ressources budgétaires

Les ressources matérielles utilisées dans l'alimentation et la construction des tableaux de bord sont soumises aux aléas techniques et sont donc susceptibles de rencontrer des défaillances matérielles ou logicielles. Ces points de rupture sont à surveiller et doivent donc être couverts en cas d'incident. Pour cela, le responsable en charge des indicateurs et des tableaux de bord doit s'assurer de disposer d'un budget ou doit vérifier que les services en charge de l'infrastructure disposent d'une enveloppe de maintenance suffisante pour couvrir d'éventuelles pannes.

Les besoins budgétaires ne sont pas exclusivement matériels. Dans le cas d'une prestation externe, le responsable en charge des indicateurs et des tableaux de bord devra valider que les budgets liés aux prestations de développement, d'intégration et d'analyse sont bien reconduits d'année en année.

IV.9.2. Environnement Externe

Dans le cadre de son cycle de vie, le fond et la forme du tableau de bord seront soumis à toutes sortes de contraintes externes ; l'actualité de l'établissement, de ses clients ou fournisseurs, l'évolution réglementaire et les opportunités d'un secteur.

Un organisme, qui, dans le cadre d'une expansion, rachète ou fusionne avec un concurrent, déclenchera une réflexion sur les évolutions à apporter à un tableau de bord pour que ce dernier continue à fournir des informations pertinentes et en adéquation avec les objectifs initiaux.

Un fournisseur, qui, dans le cadre de sa prestation, assure la gestion d'indicateurs, voit sa structure évoluer (rachat, fusion ou liquidation), représentera alors un risque de rupture pour le tableau de bord. En fonction du rôle du fournisseur dans la production du tableau de bord, ce dernier ne sera peut-être plus en mesure d'assurer une alimentation en données et/ou une construction des indicateurs dont il a la charge.

L'évolution des réglementations constitue une contrainte supplémentaire apportant une charge complémentaire plus ou moins importante en fonction du secteur. En Europe, l'adoption par la Commission européenne du Règlement général sur la protection des données (RGPD) a obligé les organismes, qu'ils soient publics ou privés, à réfléchir à de nouveaux indicateurs prenant en compte le suivi de la mise en conformité, de la gestion des demandes ou encore des violations de données.

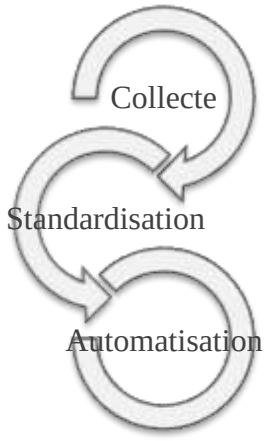
IV.9.3. Fréquence de rafraîchissement

Les contraintes internes et externes influeront sur la fréquence de rafraîchissement des indicateurs. En fonction de la contrainte, le tableau de bord devra être mis à jour sur des périodes plus ou moins courtes.

Dans le cadre d'une attaque virale à grande échelle, l'indicateur de conformité d'un parc vis-à-vis du déploiement d'un correctif verra sa fréquence de rafraîchissement augmenter pour fournir une information plus précise de l'état de la menace pesant sur le système d'information. A l'opposé, un indicateur de perte ou de vol de matériel peut voir sa fréquence limitée à l'année et ainsi mesurer uniquement la perte financière engendrée par le remplacement des actifs manquants. Néanmoins, cette évolution ne doit pas exclure la définition d'invariants d'une année sur l'autre afin de pouvoir comparer des périodes.

La fréquence de rafraîchissement doit faire l'objet d'une concertation avec le besoin du client et ce dernier doit être parfaitement conscient des contraintes et risques liés à une fréquence trop courte (performance nécessaire dans le traitement des données, absence de pondération, etc.) ou trop élevée (risque de passer à côté d'informations importantes).

IV.9.4. Industrialiser au maximum la collecte des indicateurs



La collecte des informations doit se faire par le biais d'outils, qu'ils soient gratuits ou payants, dont la fonction première est d'assurer une mise à disposition des données. Cette collecte doit au maximum être réalisée de manière automatisée afin de limiter le besoin en ressource humaine. En effet, en fonction de leur disponibilité, l'opérateur en charge de la collecte pourrait omettre des données avec pour conséquence un indicateur non pertinent. De plus, même si la ressource humaine dédiée à la collecte est disponible, la quantité de données à traiter peut être importante et dépasser la capacité d'action de l'opérateur.

Aujourd'hui, la standardisation des fichiers journaux rend l'automatisation de leur collecte facile et efficace.

De nombreuses solutions logicielles qu'elles soient gratuites ou commerciales, facilitent leur collecte. De plus, de nombreux développeurs proposent des éléments prêts à l'emploi.

En fonction du tableau de bord, la mise en forme peut devenir chronophage, il est donc important de limiter les actions « humaines » durant cette phase. L'automatisation peut être réalisée au travers d'outils, toujours gratuits ou payants. L'utilisation d'une fonction « macro », sous conditions qu'elle soit activée dans le respect des règles de sécurité de l'organisme, permet de mettre en forme des données depuis n'importe quel tableur du marché.

Des procédures seront établies pour organiser le recueil des indicateurs. Chaque indicateur fera l'objet d'une fiche de description comprenant à minima :

- Le libellé
- Le calcul
- La source de la collecte
- La périodicité
- L'objet de la mesure
- La valeur cible
- Le responsable de la collecte

La mise en forme du tableau de bord est importante pour qu'il soit facilement compréhensible par les décideurs. Il est l'image rendue de l'activité de la sécurité. Des commentaires doivent permettre de compléter et conforter la lisibilité du tableau de bord stratégique. Il ne faut pas oublier que le tableau de bord est un outil d'aide à la décision.

V. Des Tableaux de bord, sous quelle forme ?

V.1. La forme doit servir l'objectif

La forme et le visuel du tableau de bord doivent être pris en considération dès sa constitution car ils participent fortement à la bonne compréhension des informations présentées. Une représentation adaptée aux objectifs recherchés permettra de faciliter une lecture rapide des résultats présentés. Une bonne représentation des indicateurs d'un tableau de bord apportera une vision claire d'un état de situation qui permet une prise de décision (ce qui reste l'objectif principal d'un tableau de bord qu'il soit stratégique, de pilotage ou opérationnel).

Il n'existe pas, à ce jour, de format universel ou normé de représentation des tableaux de bord. L'ISO 27004 fait référence au format de reporting de l'indicateur qui indique comment la mesure doit être collectée et reportée (en mode texte, alphanumérique ou graphique) et donne quelques exemples (camembert, graphiques en barre, histogramme…). L'ANSSI s'inscrit dans la même démarche dans son recueil de recommandations TDBSSI. Ainsi, plusieurs représentations possibles des mêmes indicateurs s'offrent au RSSI.

V.2. Les différents visuels des indicateurs :

- *Visualiser l'atteinte d'un objectif*

Plusieurs formes graphiques simples et visuelles, non spécifiques aux problématiques de sécurité, permettent de visualiser l'atteinte d'un objectif. Vous trouverez ci-dessous quelques exemples parmi les plus classiques, dont les formats dits « météo » :

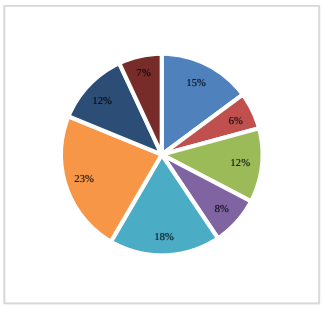
Météo **Barres de seuil** **Feux**

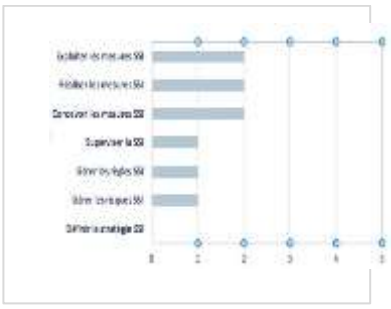
Un graphisme parlant (soleil, nuage, pluie) ou associé à des couleurs représentatives (vert, orange, rouge) permet instantanément de connaître le niveau général d'atteinte de l'indicateur à un instant « t ».

- *Valider une conformité ou un résultat d'audit*

D'autres formats disponibles (araignée, camembert, …) permettent d'avoir une vision plus précise et/ou détaillée d'un ensemble ou sous-ensemble d'indicateurs. Ils peuvent s'avérer utiles pour valider une conformité à une norme ou à une politique SSI.

Araignée **Camembert** **Barres**

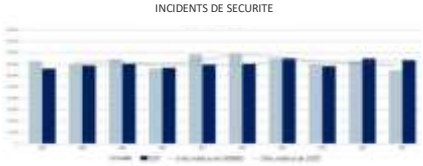




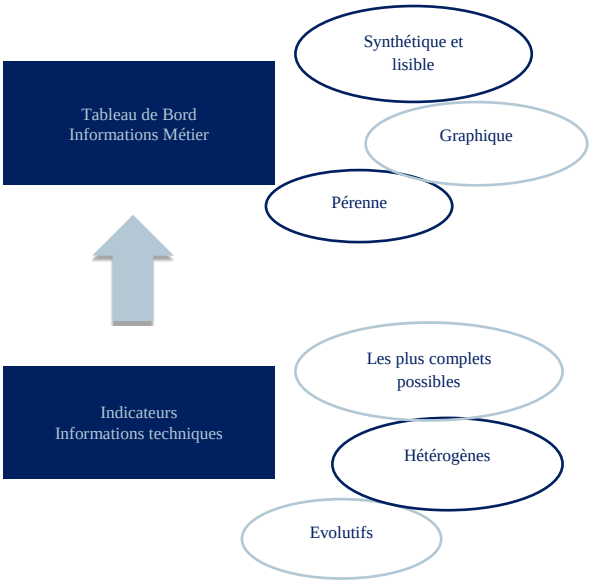
- *S'inscrire dans une tendance*

Au-delà de la valorisation de l'atteinte d'un objectif à un instant « t », il est important de pouvoir l'inscrire dans une dynamique temporelle et de montrer la progression ou l'évolution. Cela permet de définir une tendance qui peut s'avérer nécessaire à la bonne interprétation du résultat pour une meilleure anticipation des risques ou des efforts réalisés.

Barres **Courbes** **Flèches**



Pour constituer un tableau de bord, les indicateurs doivent former un tout cohérent et dynamique qui rend compte de l'ensemble.



Un bon format sera fonction de la nature du tableau de bord (stratégique, pilotage, opérationnel) et en liaison avec les habitudes, et la culture des destinataires et/ou de l'entreprise.

V.3. Tableau de bord stratégique

Un tableau de bord stratégique s'adresse à la direction de l'entreprise et doit lui permettre d'avoir une vision claire de sa situation/niveau de risque SSI et de pouvoir prendre des décisions.

Pour ce faire, le tableau de bord stratégique doit avoir une représentation :

- Simple
- Synthétique (moins d'une dizaine d'information clés)
- Lisible
- Visuelle
- Pérenne et inscrite dans une tendance

Dans la mesure du possible, la représentation des indicateurs de sécurité doit correspondre au format des tableaux de bord stratégiques déjà utilisés au sein de l'entreprise. Ce qui permettra d'offrir une continuité visuelle facilitant la bonne compréhension par la direction des informations portées à sa connaissance.

Un exemple (non exhaustif) de tableau de bord stratégique mensuel est présenté ci-dessous. Dans cet exemple, chaque indicateur clé est associé à une icône pour créer une représentation visuelle symbolique de l'indicateur. L'atteinte ou non de l'objectif est indiquée par une météo. Les éléments clés de chaque indicateur stratégique sont redonnés succinctement (les valeurs cibles, le rappel de l'objectif, la tendance / mois précédent). Les principaux risques et projets de sécurité sont listés avec leur état et les dates clés d'avancement. L'objectif est ici de porter à la connaissance de la direction des risques de sécurité identifiés et comment ils sont traités.

A noter :

- Un espace est dédié pour les commentaires « à retenir » relatifs à chaque indicateur
- Les alertes sont marquées visuellement sur le tableau de bord. Ce qui permet d'attirer l'attention sur les points de vigilance
- Une demande de décision de la part de la direction peut également être mise en exergue par un visuel spécifique (ici, « Go / No Go ? »)

V.4. Tableau de bord de Pilotage

Un tableau de bord de pilotage s'adresse à la direction projet et doit lui permettre d'avoir une vision claire de l'état d'avancement et de pouvoir décider rapidement des actions à mener.

La représentation doit être simple et les points d'alerte mis en avant. L'exemple donné ci-dessous présente de façon synthétique un état de chaque projet ou chantier identifié, en rappelant :

- La désignation du projet
- L'état d'avancement / la phase dans lequel il se trouve (étude, mise en service, recette/clôture)
- Une appréciation de l'état d'avancement par rapport aux objectifs fixés au travers d'une météo
- La tendance par rapport au mois précédent (ici, en gardant le même visuel)
- Le principal jalon suivant

Dans cet exemple, les éléments à retenir concernant le projet (ainsi que les dates clés) sont indiqués dans les commentaires.

CHANTIER	AVANCEMENT	ETAT DU PROJET 30/03/2018	ETAT DU PROJET 27/06/2018	JALONS	DATE	COMMENTAIRES
Processus de gestion de crise	Mise en service			Simulation de crise	S37	- Kit de e-learning déployé le 17/04 - Formations réalisées les 23/24 Juin - Simulation de crise planifiée le 14/09
Sensibilisation utilisateur	Clôture			Chantier finalisé	S25	- Dernière vague de sensibilisation 2018 réalisée S25
Scan applicatifs Web	Mise en service			Validation pilote	S30	- Contrat signé - Lotissement finalisé pour le déploiement des scans - Pilote en cours
Refonte sécurité périmétrique	Etude			Validation projet	S40	- Phase d'étude toujours en cours (priorité best effort) : 1,5 mois de retard

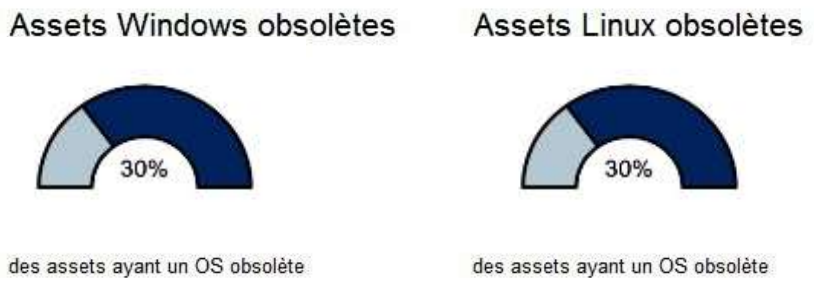
V.5. Tableau de bord opérationnel

Le tableau de bord opérationnel doit permettre d'identifier les actions prioritaires en matière d'exploitation (amélioration et fiabilisation des processus SSI et offrir la possibilité d'une vision sur la conformité, les incidents, les anomalies, etc.).

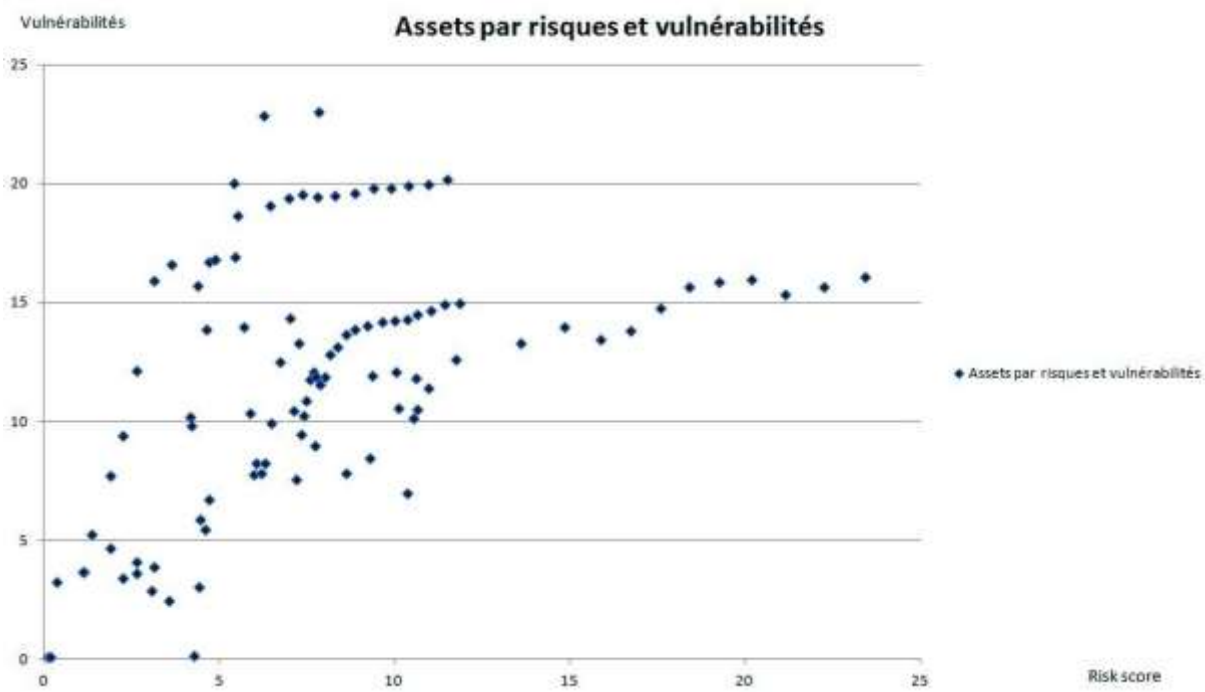
Ils doivent permettre de :

- Garantir la sécurité du système d'information
- Donner une vision opérationnelle
- Mesurer la performance
- Mesurer l'efficacité

Exemple de graphiques en anneaux



Exemple de graphique en nuage de points



V.6. Tableau de bord « flash » éphémère

Les tableaux de bord éphémères répondent au besoin :

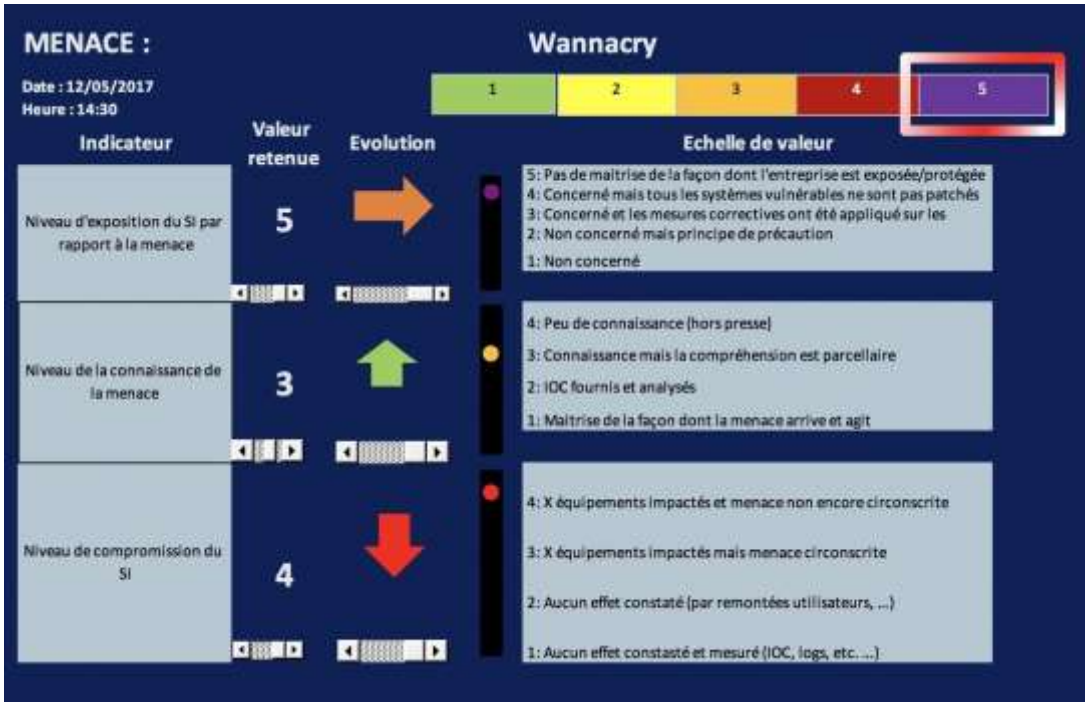
- D'apporter de la visibilité à la direction et/ou aux équipes face à une menace spécifique et critique pour l'entreprise, comme par exemple :
  - des attaques massives mondiales telles que Wannacry en 2017
  - une attaque DDOS
  - une fuite massive de données
- De mesurer son évolution dans un laps de temps court (voire en quasi temps réel)
- Mesurer l'impact des actions de remédiation

Le tableau de bord éphémère est constitué d'un certain nombre d'indicateurs s'appuyant sur des formats conformes à ceux déjà utilisés pour la gestion des risques classique (estimation du niveau de risque, évolution…).

Certains points plus spécifiques peuvent, par exemple, être indiqués :

- L'horodatage du tableau de bord. La durée de vie du tableau de bord étant relativement courte (quelques jours ou semaines), la fréquence de mise à jour sera plus importante qu'un tableau de bord opérationnel ou de pilotage et peut potentiellement aller jusqu'à l'heure en situation exceptionnelle
- Le niveau de connaissance de la menace
- Le niveau de compromission du SI si le risque est déclaré

Le tableau de bord suivant illustre ces éléments et donne un exemple possible de tableau de bord éphémère.



V.7. Outillage

Plusieurs types d'outils peuvent aider à la construction des formats des tableaux de bord :

- Tableurs
- BD
- Outil HTML coconstruits
- Outils du marché (dédiés à la sécurité ou non)

Les outils du marché permettent de consolider automatiquement des indicateurs sous forme de tableaux de bord opérationnels graphiques, soit :

- à partir de données collectées directement par l'outil (par exemple : les outils de scan de vulnérabilités proposent nativement les tableaux de bord opérationnels associés)
- en important et consolidant des données d'autres provenances

Les principaux avantages de l'utilisation d'outils automatisés pour la construction de tableaux de bord sont de pouvoir fournir une vision temps réel et de disposer d'une ou plusieurs représentations graphiques des mêmes indicateurs, dans des formats généralement plus esthétiques et plus facilement obtenus que par l'usage de simples tableurs.

Les recommandations sur les choix d'outillage dépendent de l'organisation de l'entreprise et de son niveau de maturité SSI, et se fondent sur les principales attentes du RSSI et de l'outillage existant au sein de son entreprise.

Pour les organisations matures en termes de méthodologie et de processus, utilisant déjà en interne des outils pour leur management (Qualité, SI, en sécurité ou autre), il est recommandé d'y intégrer la gestion des tableaux de bord SSI. En effet, certains outils initialement prévus pour d'autres périmètres comme des outils « Système de Management » (SM), souvent issus du monde de la Qualité, ou de gestion de risques de l'entreprise « Gouvernance, Risques, Conformité » (GRC) peuvent répondre à de nombreuses attentes liées au reporting sécurité : gestion des risques, suivi de la conformité, suivi de plan d'actions... Ainsi, si les attentes fonctionnelles sont similaires à celles d'autres services, il sera certainement intéressant de mutualiser un même outil pour diminuer les coûts et harmoniser le format des tableaux de bord au sein de l'organisation.

Certaines organisations peuvent avoir mis en œuvre des processus et appliquer une méthodologie SSI sans avoir pour autant investi dans un outillage en particulier. Le besoin d'outillage pour la fourniture des tableaux de bord peut alors s'inscrire dans le choix d'un outil plus large permettant la gestion du SMSI. Dans ce cas, il est recommandé de chercher un outil souple qui puisse s'adapter aux pratiques existantes.

Les points importants à valider dans le choix de l'outil :

- La capacité de l'outil pour répondre aux fonctionnalités attendues (outil complet contenant toutes les fonctionnalités, versus outil simple aux fonctionnalités limitées mais facile à mettre en œuvre). Les besoins de l'organisation doivent avoir préalablement été définis ;
- Le choix de l'installation sur site ou hébergée ;
- Une estimation complète des coûts de la mise en œuvre :
    - Le mode d'acquisition de la solution (investissement/abonnement/options payantes) pour anticiper les coûts cachés et/ou les besoins futurs ;
    - Les coûts d'accompagnement à la mise en œuvre et au paramétrage ainsi que les formations nécessaires à la prise en main de l'outil ;
    - Valider les coûts et processus de maintenance de l'application : associés au support du logiciel mais également en ressource interne pour maintenir la solution en conditions opérationnelles et la faire évoluer.
- Au démarrage, des outils légers et simples d'utilisation (tableurs, outils gratuits, open source…) doivent permettre, avec un investissement financier limité, de répondre aux principaux besoins fonctionnels. Attention néanmoins au temps « caché » à consacrer pour personnaliser les outils gratuits ou libres. Fonction des objectifs poursuivis, leur utilisation peut s'avérer gourmande en temps de développement.

VI. Annexe : Thématiques où créer des indicateurs sécurité de l'information

Thématique SSI	Chapitres norme ISO 27001-2013 et Annexes
Gouvernance	**A 5** : Politiques de sécurité de l'information **A 6.1** : Organisation de la sécurité de l'information / Organisation interne
Sensibilisation / Formation	**A 7.2.2** : Sécurité des ressources humaines / Pendant la durée du contrat / Sensibilisation, apprentissage et formation à la sécurité de l'information
Gestion des risques	**Clause 6 (6.1.2 et 6.1.3)**
Gestion du patrimoine informationnel	**A 8** : Gestion des actifs **A 10** : Cryptographie
Accès et habilitations	**A 9** : Contrôle d'accès **A 11.1** : Sécurité physique et environnementale / Zones sécurisées
Postes de travail et nomadisme	**A 6.2** : Organisation de la sécurité de l'information / Appareils mobiles et télétravail **A 11.2** : Sécurité physique et environnementale / Matériels
Exploitation et serveurs	**A 12** : Sécurité liée à l'exploitation
Réseaux et télécommunication	**A 13** : Sécurité des communications
Sécurité dans les projets	**A 14** : Acquisition, développement et maintenance des systèmes d'information
Gestion des incidents de sécurité	**A 16** : Gestion des incidents liés à la sécurité de l'information
Gestion des vulnérabilités	**A 18** : Conformité
Conformité	**A 15** : Relations avec les fournisseurs **A 18.2** : Conformité / Revue de la sécurité de l'information

Exemple : « Aspects de la sécurité de l'information dans la gestion de la continuité d'activité ». A ajouter si les indicateurs SSI traitent également de la continuité d'activité.

L'ESPRIT D'ÉCHANGE

CLUB DE LA SÉCURITÉ DE L'INFORMATION FRANÇAIS

11 rue de Mogador
75009 Paris
France
✆ +33 1 53 25 08 80
clusif@clusif.fr

Téléchargez toutes les publications du CLUSIF sur
www.clusif.fr

Le CLUSIF (association Loi 1901) est le 1er club professionnel des experts en sécurité des systèmes d'information et en cybersécurité en France. Ouvert à toutes les entreprises et institutions, ce club rassemble dans une parfaite équité au sein de deux collèges des Utilisateurs et Offreurs de solutions issus de tous les secteurs de l'économie. L'objectif principal du CLUSIF est de favoriser les échanges d'idées et les retours d'expériences par des groupes de travail, des publications et des conférences thématiques. Les sujets abordés, en relation avec la sécurité de l'information, varient en fonction de l'actualité et des besoins des membres de l'association.