2007

INDICATEURS SECURITE

Guide pratique pour un tableau de bord sécurité stratégique et opérationnel

CIGREF

« Promouvoir l'usage des systèmes d'information comme facteur de création de valeur et source d'innovation pour l'entreprise »

Publications du CIGREF en 2006-2007

Analyse et Gestion des risques dans les grandes entreprises :
impacts et rôles pour la DSI

Baromètre Gouvernance SI :
Evaluer sa démarche de gouvernance du système d'information

Changement et transformation du SI :
Note de synthèse

Exemples d'offshoring :
Retours d'expériences et leçons apprises au sein de grandes entreprises

Faire face aux changements de périmètre d'entreprise :
guide de survie à l'usage des dirigeants en cas de changement de périmètre d'entreprise

Gestion des actifs immatériels :
kit de démarrage et études de cas

Les dossiers du Club Achats :
Synthèse des activités 2007

Management d'un Centre de Services Partagés informatiques :
Quels modèles ? Quels bénéfices pour l'entreprise ? Quels impacts sur le métier de DSI ?

Marketing de la DSI :
Cadre de mise en œuvre

Outil de scénarisation prospective des besoins Ressources Humaines de la SI :
Facteurs clés de l'évolution des métiers et des compétences

Pilotage économique du Système d'information :
Présentation des coûts informatiques et fiches d'amélioration par processus

Plan Stratégique Système d'Information

Tableau de bord des Ressources Humaines :
Indicateurs clefs

Tableau de bord Sécurité :
Indicateurs clefs de la sécurité système d'information

Le CIGREF tient à remercier les personnes qui ont participé à l'élaboration de ce document, pour leurs conseils, expériences et suggestions d'amélioration. Nous tenons à remercier tout particulièrement :

Xavier Bernaert	LVMH
Alain Bouillé	Caisse des Dépôts
Brigitte Cohen	BNP Paribas
Alain Delboy	Air Liquide
Jérôme Galerne	Auchan
Emmanuel Garnier	Systalians
Jean-Claude Gaume	GMF
Eric Grospeiller	ANPE
Jean-Christophe Krebs	Crédit Agricole SA
François Jolivet	Société Générale
Christophe Moreau	MAAF
Guy Nicolas	Nexans
Jean-Marie Pilot	CNAV
Didier Quincerot	SMABTP
Colette Rodionoff	EDF
Marie-Christine Sudre	GMF
Jean Vergnoux	Renault

Cette activité a été pilotée par Alain Bouillé, RSSI Groupe Caisse des Dépôts

Ce document a été rédigé par Stéphane Rouhier, chargé de mission au CIGREF

Sommaire

1 Contexte et objectifs 7
2 Destinataires 8
3 Liste des indicateurs retenus 8
3.1 Les indicateurs stratégiques 8
3.1.1 Conformité 9
3.1.2 Image de l'entreprise (et signaux faibles) 9
3.1.3 Protection de l'information 9
3.1.4 Efficacité de la politique (risques couverts et non couverts) 9
3.2 Les indicateurs opérationnels 10
3.2.1 Vols 11
3.2.2 Attaques et sinistralité 11
3.2.3 Protection de l'information 11
3.2.4 Efficacité de la politique / risques couverts / non couverts 11
4 Fréquence de collecte 13
5 Méthode de calcul 13
6 Représentation graphique 13
7 Enrichissement et processus d'amélioration du document 13
8 Contact CIGREF : 13

Avertissement

Ce document constitue une *boite à outils* pour les entreprises désireuses de mettre en place des indicateurs de mesure de la sécurité de leur SI. Il s'agit d'une boite à outils que chacun est libre de s'approprier dans son usage, après un travail d'adaptation au contexte et à l'organisation de son entreprise

1 Contexte et objectifs

Dans le cadre de ses travaux sur la gouvernance, la performance durable et le pilotage des SI, le CIGREF a décidé d'élaborer une série d'indicateurs, car la mesure est perçue comme un outil de diagnostic, de benchmarking, une démarche qualité mais aussi comme un élément d'un processus d'amélioration continue. Le CIGREF a déjà ainsi mis en place des indicateurs RH. La démarche a été étendue aux indicateurs sécurité.

Les objectifs sont de permettre aux entreprises de disposer d'indicateurs communs, standards et partagés, leur permettant de :

- sensibiliser les métiers
- communiquer vers les directions générales,
- mesurer le niveau de maturité de leur politique et pratiques de sécurité,
- progresser et améliorer leur politique de sécurité,
- s'appuyer sur les bonnes pratiques de la communauté CIGREF,
- se comparer au sein de leur entreprise dans le temps,
- se comparer au sein de leur entreprise, entre filiales,
- se comparer entre entreprises, de taille, secteur et organisation similaires.

Dans un premier temps, l'objectif suivi à court terme est de permettre aux entreprises de disposer d'une boite à outils d'indicateurs afin de communiquer en interne et de se comparer en interne entre filiales.

Dans un second temps, les entreprises pourront éventuellement se comparer entre elles, si elles le souhaitent, soit de gré à gré, soit en se réunissant au CIGREF et en définissant une méthode commune de calcul des indicateurs.

2 Destinataires

Ces indicateurs sont destinés aux responsables sécurité des systèmes d'information, directeurs sécurité des systèmes d'information, *risk manager* de grandes entreprises.

Ces indicateurs ont pour vocation d'alimenter des tableaux de bords destinés à plusieurs cibles, directions générales ou pilotes opérationnels.

3 Liste des indicateurs retenus

Les travaux du groupe ont conduits à distinguer deux niveaux d'indicateurs :

- des indicateurs stratégiques pour un *reporting* vers la DSI et la direction générale
- des indicateurs opérationnels pour le pilotage de la sécurité au quotidien.

Les indicateurs ont été retenus en fonction de deux critères :

- leur pertinence
- leur mesurabilité

Selon l'objectif et la cible suivis, l'entreprise choisira de mettre l'accent sur les indicateurs stratégiques ou les indicateurs opérationnels.

3.1 Les indicateurs stratégiques

Les indicateurs stratégiques sont les suivants :

1. Analyse de risque
2. Classification de l'information
3. Plaintes internes et externes
4. Audit - Taux de contrôle
5. Audit - Taux de conformité
6. Audit - Taux de correction
7. Archivage - Propriétaires métiers ayant fait une démarche d'identification des données métiers à archiver
8. Continuité - Fréquence et réussite du test du Plan de Continuité d'Activité (PCA)
9. Nombre de composants matériels ou applicatifs non-conformes, non maintenus

10. Taux de prestataires externes sur les postes sensibles (administrateurs réseaux, chefs de projets…)
11. Taux de personnes sensibilisées / Cible
12. Nombre de sites web vitrines contrefaits / parodiés
13. Nombre de noms de domaines (marques…) usurpés
14. Pourcentage de projets pour lesquels la Maitrise d'Ouvrage (MOA) a procédé à une analyse de risque formalisée
15. Pourcentage de nouveaux projets dont la MOA a exprimé le besoin de sécurité
16. Pourcentage d'applications - sensibles ou non - couvertes par une politique d'accès
17. Tenue des comités sécurité stratégiques

Ces indicateurs stratégiques peuvent être reclassés en 4 grandes sous catégories – qui peuvent correspondre à des équivalents dans ISO 17799 ou Bâle 2 :

3.1.1 Conformité

- Audit - Taux de contrôle
- Audit - Taux de conformité
- Audit - Taux de correction

3.1.2 Image de l'entreprise (et signaux faibles)

- Nombre de sites web vitrines contrefaits / parodiés
- Nombre de noms de domaines (marques…) usurpés
- Plaintes internes et externes

3.1.3 Protection de l'information

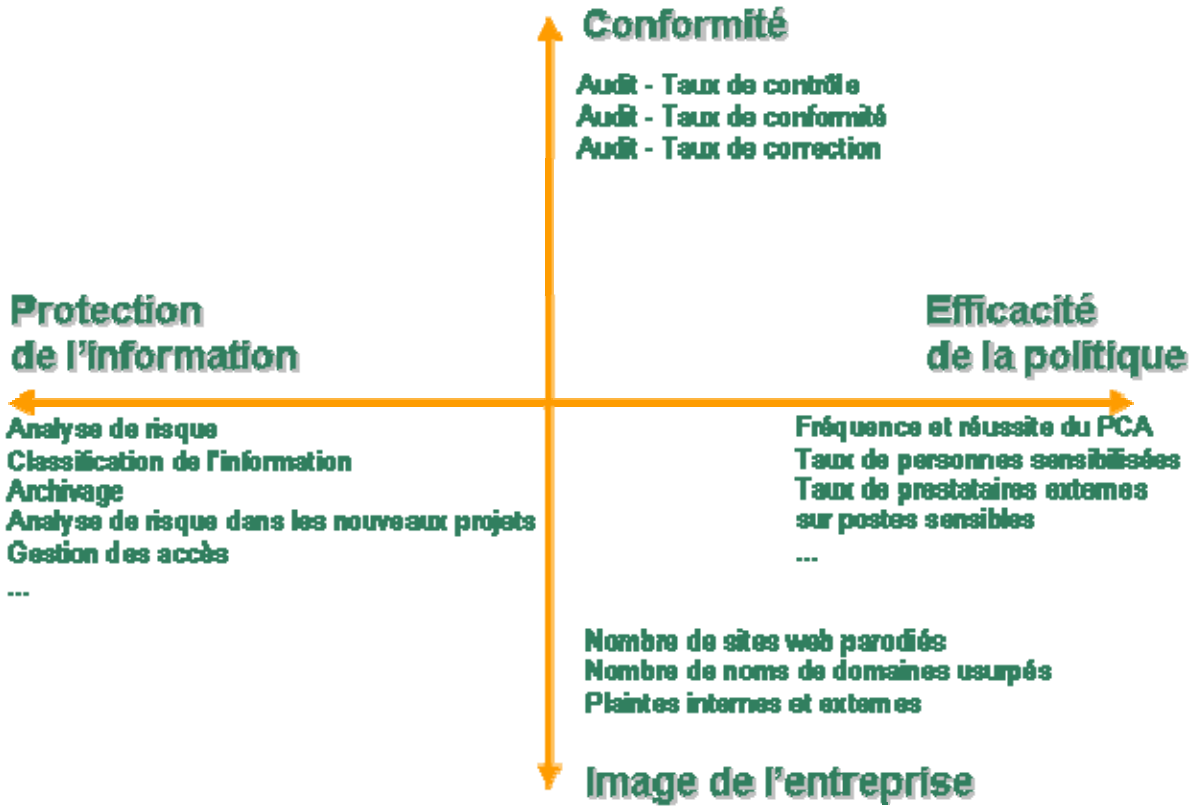
- Analyse de risque
- Classification de l'information
- Archivage - Propriétaires métiers ayant fait une démarche d'identification des données métiers à archiver
- Gestion des projets - Pourcentage de projets pour lesquels la MOA a procédé à une analyse de risque formalisée
- Gestion des projets - Pourcentage de nouveaux projets dont la MOA a exprimé le besoin de sécurité
- Gestion des accès - Pourcentage d'applications - sensibles ou non - couvertes par une politique d'accès

3.1.4 Efficacité de la politique (risques couverts et non couverts)

- Continuité - Fréquence et réussite du test du PCA

- Nombre de composants matériels ou applicatifs non-conformes, non maintenus
- Taux de prestataires externes sur les postes sensibles (administrateurs réseaux, chefs de projet, …) (indicateur non pertinent en cas d'infogérance globale)
- Taux de personnes sensibilisées / Cible
- Tenue des comités sécurité stratégiques

Figure 1 : Les 4 axes stratégiques d'un tableau de bord sécurité



Source : CIGREF

3.2 Les indicateurs opérationnels

Les indicateurs opérationnels sont les suivants :

18. Nombre de vols et pertes - PC fixes
19. Nombre de vols et pertes - Terminaux mobiles
20. Perte de mots de passe
21. Traçabilité – Pourcentage d'accès non autorisés sur les applications sensibles
22. Continuité - Taux de vulnérabilité
23. Attaques en environnement messagerie

24. Attaques en environnement intranet
25. Attaques en environnement internet
26. Disponibilité des applications critiques
27. Pourcentage de sites physiques audités
28. Mise à jour des antivirus / patches
29. Bonne installation des patches
30. Fréquence et écart mesurés dans les audits de comptes
31. Evolution du nombre d'identifiants génériques
32. Pourcentage d'application en production ayant un dossier sécurité formalisé
33. Tenue des réunions du comité de sécurité opérationnel
34. Nombre de correspondants SSI

Ces indicateurs opérationnels peuvent être reclassés en 4 grandes sous catégories :

3.2.1 Vols

- Nombre de vols et pertes - PC fixes
- Nombre de vols et pertes - Terminaux mobiles

3.2.2 Attaques et sinistralité

- Attaques en environnement messagerie
- Attaques en environnement intranet
- Attaques en environnement internet

3.2.3 Protection de l'information

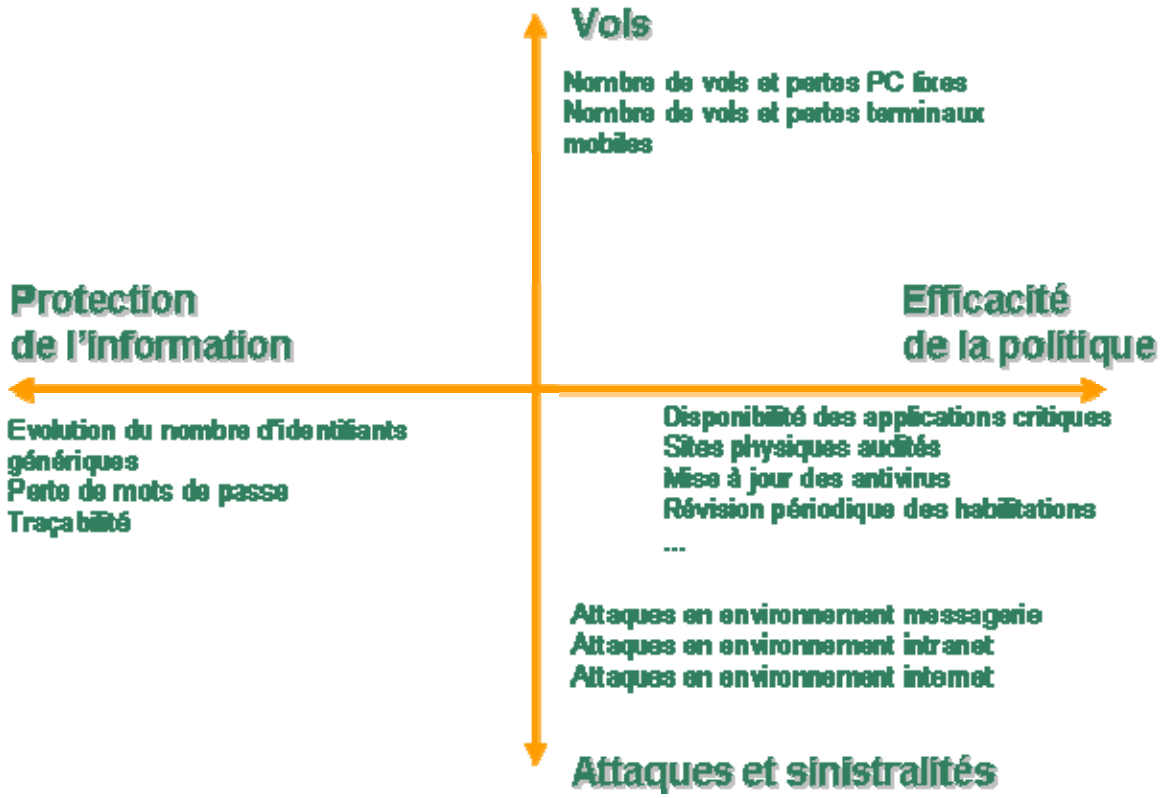
- Evolution du nombre d'identifiants génériques
- Perte de mots de passe
- Traçabilité - Pourcentage d'accès non autorisés sur les applications sensibles

3.2.4 Efficacité de la politique risques couverts / non couverts

- Disponibilité des applications critiques
- Continuité - Taux de vulnérabilité
- Pourcentage de sites physiques audités
- Mise à jour des antivirus / patches
- Bonne installation des patches
- Fréquence et écart mesurés dans les audits de comptes
- Pourcentage d'application en production ayant un dossier sécurité formalisé
- Tenue des réunions du comité de sécurité opérationnel

- Nombre de correspondants SSI

Figure 2 : Les 4 axes opérationnels d'un tableau de bord sécurité



Source : CIGREF

4 Fréquence de collecte

La fréquence de collecte des données est variable, elle est généralement semestrielle ou annuelle. Les indicateurs stratégiques sont plutôt collectés sur une base annuelle, les indicateurs opérationnels pouvant être collectés selon sur une base semestrielle ou annuelle.

Certains RSSI préconisent même de collecter et communiquer tous les six mois sur les indicateurs stratégiques et tous les mois sur les indicateurs opérationnels.

5 Méthode de calcul

La méthode de calcul est expliquée en annexe. L'unité de mesure, l'échelle ou la valeur cible à respecter ou à atteindre ont également été fixées lorsqu'elles faisaient l'objet d'un consensus de la part du groupe.

6 Représentation graphique

Le groupe a également travaillé sur les modèles de représentation graphique. Une série de représentations graphiques des indicateurs est proposée en annexe.

7 Enrichissement et processus d'amélioration du document

Ce document est un processus dynamique. Il a vocation à évoluer et à être enrichi dans le temps. N'hésitez pas à nous soumettre vos indicateurs ou à nous faire part de vos suggestions.

8 Contact CIGREF :

Stéphane Rouhier

+33 1 56 59 70 11 / +33 6 85 40 27 91

stephane.rouhier@cigref.fr

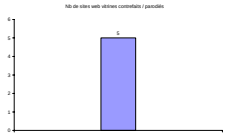
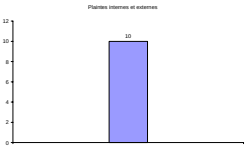
Annexe 1 – liste détaillée et représentation graphique des indicateurs stratégiques

Note : Les chiffres figurant dans les graphiques sont des données fictives

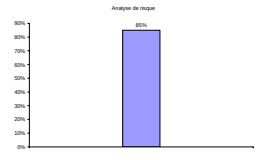
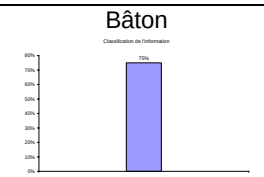
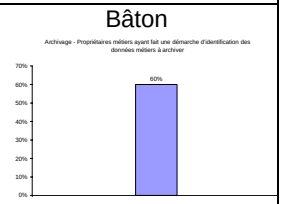
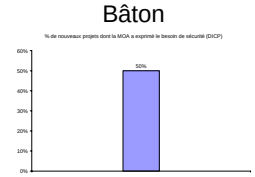
Axe 1 - Conformité

Conformité	Unité de mesure	Périmètre	Echelle / Cible	Méthode de calcul	Fréquence de collecte	Illustration graphique
Audit -Taux de contrôle	%	groupe		Nb d'audits effectués / Nb d'audits cible	annuelle	Radar 
Audit - Taux de conformité	%	groupe		Nb d'audits effectués avec succès / nb d'audits effectués	annuelle	
Audit - Taux de correction	%	groupe		Nb d'audits corrigés / Nb d'audits défectueux	annuelle	

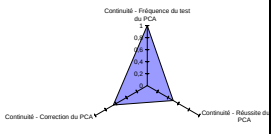
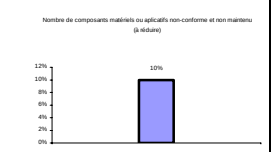
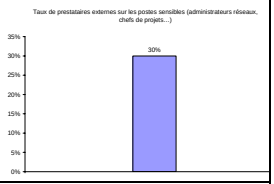
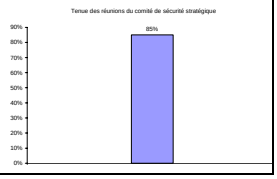
Axe 2 - Image de l'entreprise

Image	Unité de mesure	Périmètre	Echelle / Cible	Méthode de calcul	Fréquence de collecte	Illustration graphique
Nombre de sites web vitrines contrefaits / parodiés	nombre	groupe	0		annuelle	Bâton 
Nombre de noms de domaines (marques…) usurpés	nombre	groupe	0		annuelle	Bâton 
Plaintes internes et externes	nombre	groupe			annuelle	Bâton 

Axe 3 - Protection de l'information

Protection	Unité de mesure	Périmètre	Echelle / Cible	Méthode de calcul	Fréquence de collecte	Illustration graphique
Analyse de risque	%	groupe			annuelle	Bâton 
Classification de l'information	%	groupe	100%	« nb métiers en conformité	annuelle	Bâton 
Archivage – Propriétaires métiers ayant fait une démarche d'identification des données métiers à archiver	%	groupe		nb métiers en conformité / nb métiers concernés	annuelle	Bâton 
Pourcentage de projets dont la MOA a procédé à une analyse de risque formalisée	%	groupe	>50%	nb projet avec analyse de risque / nb de projets	annuelle	Bâton 
% de nouveaux projets dont la MOA a exprimé le besoin de sécurité (DICP)	%	entité	>50%	nb projet avec expression de besoin / nb projets	annuelle	Bâton 
Gestion des accès - Pourcentage d'applications sensibles ou non couvertes par une politique d'accès.	%	groupe			annuelle	Bâton 

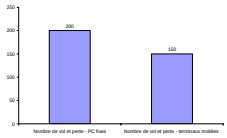
Axe 4 - Efficacité de la politique / risques couverts / non couverts

Efficacité	Unité de mesure	Péri mètre	Echelle / Cible	Méthode de calcul	Fréquence de collecte	Illustration graphique
Continuité - Fréquence et réussite du test du PCA	Fréquence / an	groupe	1 fois par an		annuelle	Radar 
Nombre de composants matériels ou applicatifs non-conforme, non maintenu	nombre	groupe	<10%	nb postes obsolètes, nb applicatifs obsolètes	annuelle	Bâton 
Taux de prestataires externes sur les postes sensibles (administrateurs réseaux…)	%	groupe	<20%		annuelle	Bâton 
Taux de personnes sensibilisées / Cible	%	groupe	100%	nb personnes ayant suivi une formation (qqsoit) dédiée SSI / nb personnes concernées	annuelle	Bâton 
Tenue des comités sécurité stratégiques	%	groupe			annuelle	Bâton 

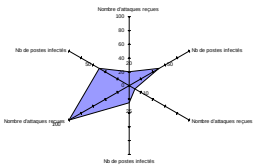
Annexe 2 – liste détaillée et représentation graphique des indicateurs opérationnels

Note : Les chiffres figurant dans les graphiques sont des données fictives

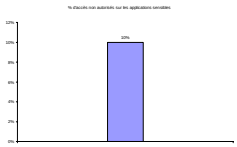
Axe 1 - Vols

Vols	Unité de mesure	Périmètre	Echelle / Cible	Méthode de calcul	Fréquence de collecte	Illustration graphique
Nombre de vols & pertes - PC fixes	nombre	groupe		PC fixes volés / Parc total de PC fixes	annuelle	Bâton 
Nombre de vols & pertes - Terminaux mobiles	nombre	groupe		Terminaux mobiles volés / Parc total de terminaux	annuelle	

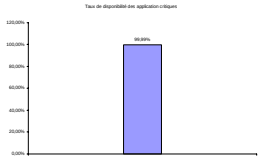
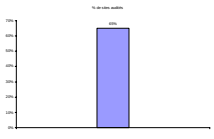
Axe 2 - Attaques et sinistralité

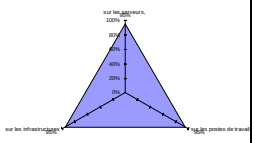
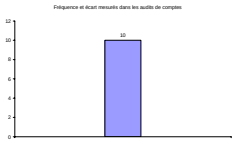
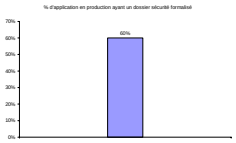
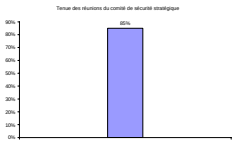
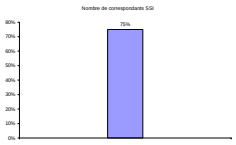
Attaques	Unité de mesure	Périmètre	Echelle / Cible	Méthode de calcul	Fréquence de collecte	Illustration graphique
• Attaques en environnement messagerie • Nombre d'attaques reçues • Nb de postes infectés	nombre	groupe			semestrielle	Radar 
• Attaques en environnement intranet • Nombre d'attaques reçues • Nb de postes infectés	nombre	groupe			semestrielle	
• Attaques en environnement internet • Nombre d'attaques reçues • Nb de postes infectés	nombre	groupe			semestrielle	

Axe 3 - Protection de l'information

Protection	Unité de mesure	Périmètre	Echelle / Cible	Méthode de calcul	Fréquence de collecte	Illustration graphique
Evolution du nombre d'identifiants génériques (à réduire)	nombre	groupe	< 5%	• soit nb id générique • soit nb id générique autorisé par dérogation / nb générique global	annuelle	Bâton Histogramme 
Perte de mots de passe	nombre	groupe		Nb de mots de passe réinitialisés	annuelle	Bâton 
Traçabilité – % d'accès non autorisés sur les applications sensibles	% ou nb	groupe	0%	• soit nb accès rejetés, • soit nb accès rejetés / nb accès total	annuelle	Bâton 

Axe 4 - Efficacité de la politique risques couverts / non couverts

Efficacité	Unité de mesure	Périmètre	Echelle / Cible	Méthode de calcul	Fréquence de collecte	Illustration graphique
Disponibilité des applications critiques	%	groupe	99%		semestrielle	Bâton 
Continuité - Taux de vulnérabilité (tout systèmes confondus)	feux (vert, orange, rouge)	groupe	vert	nb corrections menées / nb total de corrections à apporter	annuelle	Feux 
% de sites physiques audités (bâtiments)	note	groupe		liste des sites et note de conformité associée	annuelle	Bâton 

Efficacité	***Unité de mesure***	***Périmètre***	***Echelle / Cible***	***Méthode de calcul***	***Fréquence de collecte***	***Illustration graphique***
Mise à jour des antivirus / patches (serveurs, postes de travail, infrastructures)	%	groupe	100%	nb poste mis à jour / nb postes total Idem pour les serveurs…	annuelle	Radar 
Bonne installation des patches	%	groupe	100%	% des machines patchées	annuelle	Radar 
Fréquence et écart mesurés dans les audits de comptes	Fréquence / période	groupe			annuelle	Bâton 
% d'application en production ayant un dossier sécurité formalisé	%	entité	>50%	nb applis avec dossier sécurité / nb applis	annuelle	Bâton 
Tenue des réunions du comité de sécurité opérationnel	%	groupe	>80%	nb réunions (théorie 3/an) / nb filiales	annuelle	Bâton 
Nombre de correspondants SSI	%	groupe		Nb CSSI filiales / Nb filiales	annuelle	Bâton 

Annexe 3 – exemple de fiche de présentation d'un indicateur

Chaque indicateur pourra faire l'objet d'une présentation sous la forme de fiche mise à disposition du répondant ou de la personne chargée d'administrer le questionnaire. La fiche résumera l'objectif, la description, les destinataires, la source, la procédure de fabrication de l'indicateur, la fréquence, la méthode de calcul, l'unité et la représentation.

Champs	**Description**
Nom	**Sites Internet avec Tests d'Intrusion**
Objectif	S'assurer de l'application de l'obligation de tests des sites internet
Thème	Réseau - Protection contre la Malveillance
Description	% des sites internet faisant l'objet de tests d'intrusion annuels
Destinataires	Comité des RSSI ; Comité Sécurité Groupe
Source	Niveau entité (choix dépend de l'organisation) : a) RSSI b) Cellules MOE Internet c) Cellules MOA internet Pour le Groupe : RSSI
Procédure de fabrication	Niveau entité (choix dépend de l'organisation) : Pour le Groupe : Intégré au Questionnaire d'Evaluation Groupe
Fréquence de remontée	Pour le Groupe : 1) Indicateur de contrôle : tous les ans dans le cadre du Questionnaire d'Evaluation Groupe 2) Indicateur de correction : idem plus en Comité tous les trimestres
Méthode de calcul	Sont remontés le numérateur et le dénominateur ; le pourcentage est calculé au final (relativise le pourcentage) 1) Indicateur de contrôle $\frac{\text{nb adresses IP publiques faisant l'objet de tests d'intrusion annuels}}{\text{nb adresses IP publiques}}$ 2) Indicateur de correction $\frac{\text{nb de vulnérabilités corrigées}}{\text{nb de vulnérabilités à corriger}}$ Le "nb de vulnérabilités à corriger" correspond aux vulnérabilités identifiées par le test et validées comme devant faire l'objet d'une correction. La mesure n'étant faite qu'annuellement, il convient de suivre spécifiquement le taux de correction.
Unités & Valeur cible	Nb & % ; cible 100%
Présentations	Niveau entité : Courbes historiques : 1) et 2) numérateur ; dénominateur ; taux Pour le Groupe : Annuel : radar Groupe

Le CIGREF, Club Informatique des Grandes Entreprises Françaises, est une association d'entreprises. Sa mission est de promouvoir l'usage des systèmes d'information comme facteur de création de valeur et source d'innovation pour l'entreprise.

Le CIGREF regroupe des grandes entreprises de tous secteurs (assurance, banque, distribution, énergie, industrie, services, services sociaux et santé et transport).

Le CIGREF favorise le partage d'expériences et l'émergence des meilleures pratiques. C'est un interlocuteur des pouvoirs publics français et européens sur les domaines des technologies de l'information.

Le CIGREF fait valoir les attentes légitimes des grands utilisateurs d'informatique et de télécommunications. Les thématiques d'échanges du CIGREF sont *le SI au service des métiers de la DG*, *la performance durable du SI* et le *management de la fonction SI*.

CIGREF
21, avenue de Messine
75008 Paris

Tél. 01 56 59 70 00
Fax 01 56 59 70 01

E-mail : cigref@cigref.fr
www.cigref.fr