Retour d'Expérience : Mise en conformité au RGPD

CGI Business Consulting – 11/04/2018

CGI | Business Consulting
La force de l'engagement[MD]

Panorama de la protection des personnes

Un hôpital de Saint-Malo épinglé pour manquement au secret médical

Un contrôle effectué en juin 2013 par la Commission Nationale Informatique et Liberté (CNIL), au centre hospitalier de Saint-Malo, a permis de constater qu'un prestataire mandaté par l'hôpital avait eu accès aux dossiers médicaux de 950 patients. Le 25 septembre 2013, la commission a mis en demeure le centre hospitalier de respecter la confidentialité des dossiers de santé. L'information a été rendue publique par un communiqué diffusé le 7 octobre par la CNIL.

Par Florian Gouthière, avec AFP
Rédigé le 08/10/2013

Ransomware : 16 hôpitaux anglais paralysés par une cyberattaque

Le vendredi 12 Mai 2017 à 18:30 par Christian D. | 84 commentaire(s) Source : The Guardian

Une quinzaine d'hôpitaux anglais ont vu leur fonctionnement fortement perturbé après une cyberattaque accompagnée de demandes de rançons pour débloquer les ordinateurs touchés.

Pacemaker : plus de 8 600 failles découvertes

Posted On 29 Mai 2017 By : Damien Bancal Comment: 0 Tag: défibrilateur, hack, pacemaker, sécurité

Des chercheurs en sécurité ont découvert plus de 8 600 vulnérabilités dans les systèmes de pacemaker et les bibliothèques tierces utilisées pour alimenter les cœurs sous défibrillateur cardiaque.

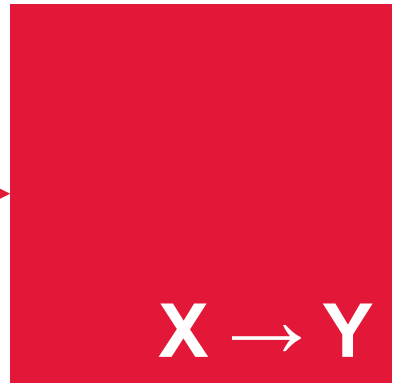
La CNIL juge les données de santé des Français trop mal protégées

La Commission nationale de l'informatique et des libertés a décidé de rendre public la mise en demeure faite à l'Assurance maladie de résoudre d'importants problèmes de sécurisation de nos données de santé.

Sécurité dans le RGPD

Le **chiffrement** est un procédé qui consiste à rendre illisible une donnée par un procédé cryptographique pour toute personne ne possédant pas la clé de déchiffrement.

des moyens permettant de **rétablir la disponibilité des données à caractère personnel et l'accès** à celles-ci dans des délais appropriés en cas d'incident physique ou technique



La **pseudonymisation** selon la CNIL « le remplacement d'un nom par un pseudonyme. C'est le processus par lequel les données perdent leur caractère identifiant (de manière directe). Les données restent liées à la même personne dans tous les dossiers et systèmes informatiques sans que l'identité ne soit révélée.»

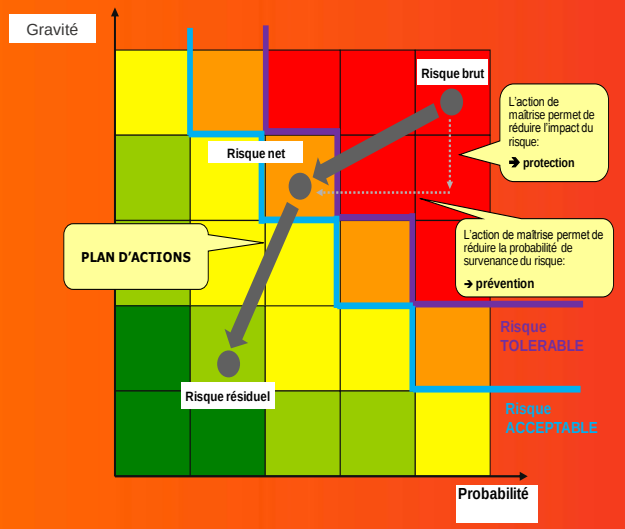
Moyens permettant de garantir la **confidentialité, l'intégrité, la disponibilité et la résilience** des systèmes et des services de traitement

une procédure d'audit des mesures mises en œuvre

Notre approche basée sur 3 fondamentaux

1

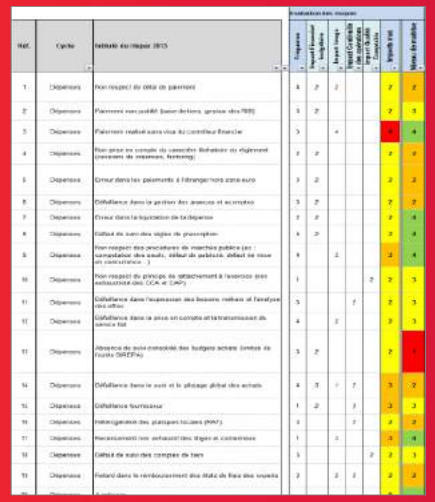
Maitriser le risque de fuite d'informations



- Cibler les périmètres à enjeux (données clientes et sensibles)
- Avancer en fonction du ROI

2

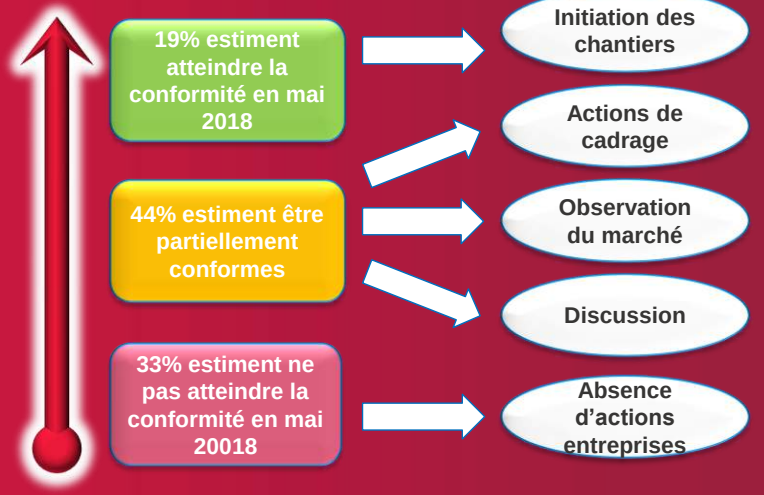
Maitriser son niveau de conformité du SI



- Eviter la fausse promesse d'être 100% conforme en mai 2018
- Mettre en place les 1ères briques importantes
- Faire adopter le RGPD par les projets et traiter à plus long terme l'« héritage »

3

Maitriser son positionnement



- Etre conforme sur la LIL et la loi Lemaire avoir engagé des moyens sur le RGPD
- Cadrer vite son projet
- Observer le marché :
  - pas de sur conformité,
  - pas de surinvestissement

Maitrise du risque

- AIPD : Analyse de risques avec la vision droit et libertés des personnes. Cet angle est un changement par rapport aux outils traditionnels d'Analyse de Risque comme la méthodologie ISO/IEC 27005.

- L'analyse se fait selon les trois propriétés habituelles en informatique disponibilité/intégrité/confidentialité.

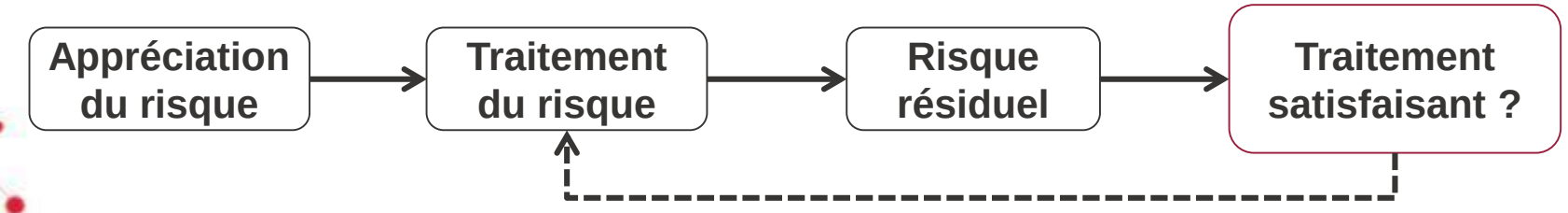


Illustration d'une analyse de risques (1/2)

Analyse du risque (exemple)

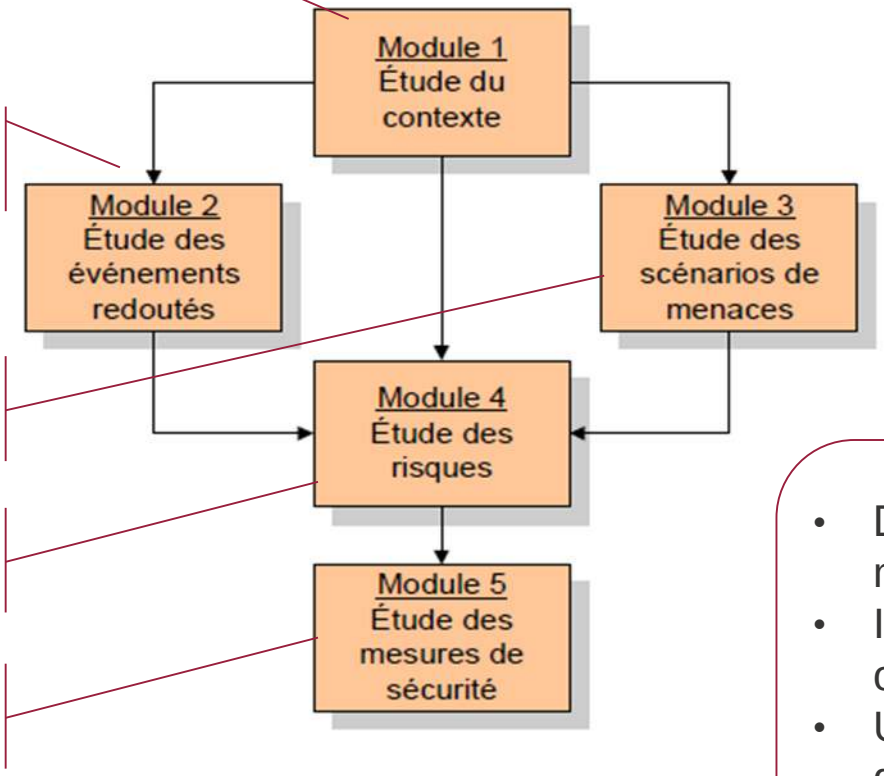
Contexte et Principes fondamentaux
Métriques
Besoins de sécurité

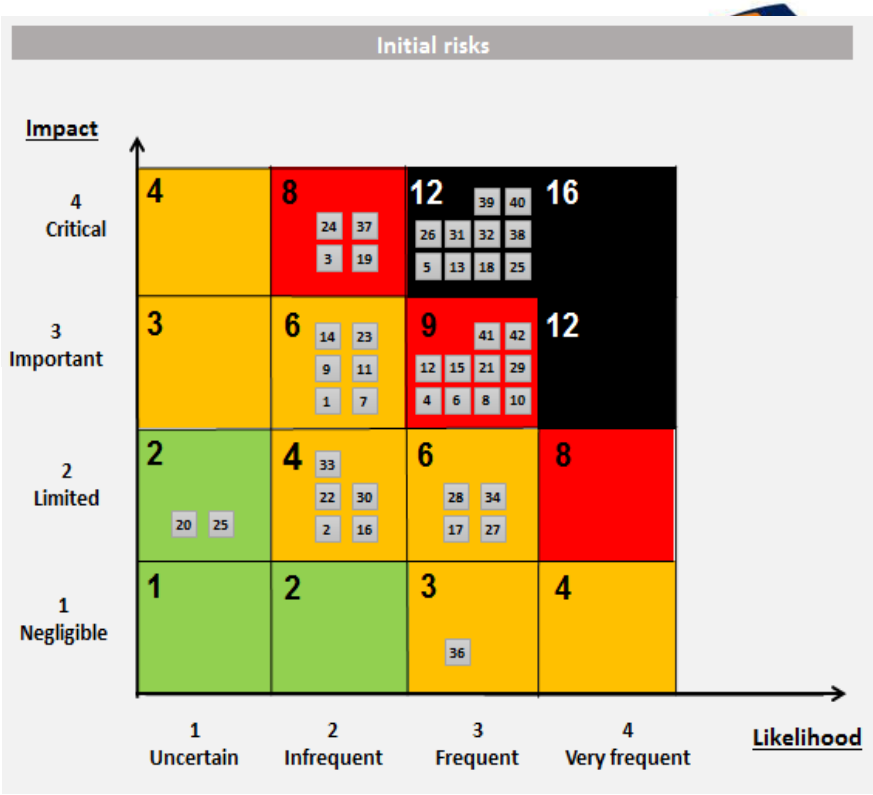
Identification des impacts **métiers**
Identification des sources de menaces

Identification des scénarios de menaces **(techniques)**

Calcul du risque

Identification des mesures techniques et fonctionnelles





Exemple d'impacts :

- Décès suite à l'administration d'un mauvais médicament
- Impossibilité de tracer la stérilisation des outils
- Un assureur refuse la couverture suite à la divulgation du dossier patient
- Demande de rançon suite à la prise en main à distance d'un DM connecté

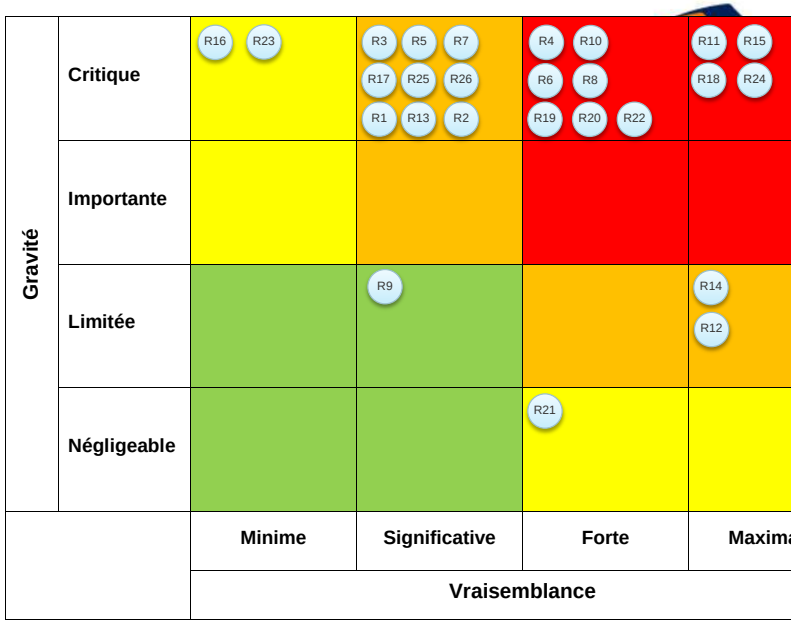
CGI | Business Consulting

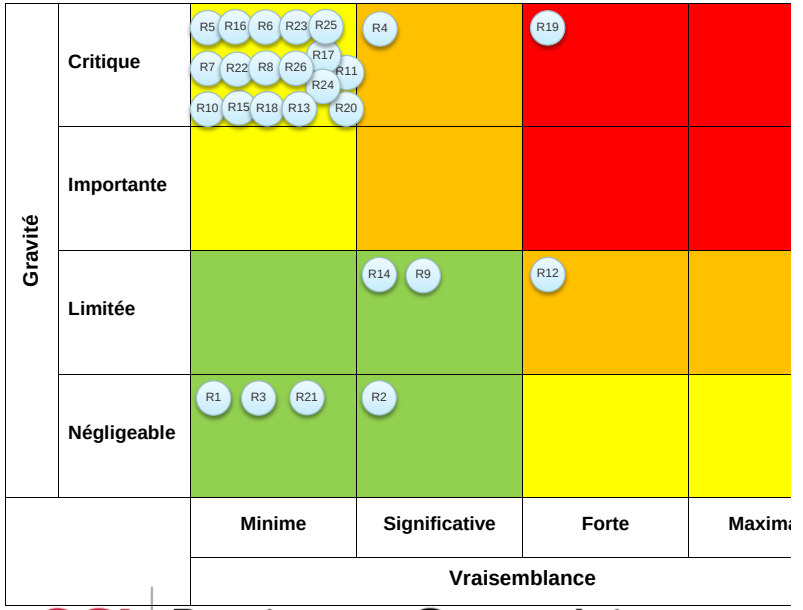
Illustration d’une analyse de risques (2/2)

Mesures et risque résiduel

Exemple de mesures	Type de mesure
Procédures et politiques	Organisationnelle
Contrôles des accès logiques	Technique/organisationnelle
Contrôles des actifs	Technique
Contrôle des sous-traitants	Juridique/Organisationnelle
Mise en place de mesures techniques	Technique
Contrôle des demandes d’exercices des droits	Juridique/Organisationnelle
Gestion des incidents	Organisationnelle/Technique

Exemple : *Définir les modalités de contrôle d'identité d'une personne souhaitant faire exercer ses droits au regard de ses données personnelles. Cela nécessite le nom, la carte d’identité et l’attestation de sécurité sociale stipulant tous les ayants droits de moins de 3 mois*





CGI | Business Consulting

Maitriser son niveau de conformité

1. Eviter la promesse du 100% conforme, alors que :
   a) le projet de révision de la LIL est encore en discussion (ex: chiffrement bout en bout) ;
   b) certains guides de bonnes pratiques sont en attente .

2. Prendre en compte dans les contrats le RGPD

3. Poser les premières briques importantes pour s'engager dans la démarche de conformité (ex: plan d'action)

4. Impliquer les métiers

Le RGPD ne s'arrête pas au 25 mai

CNIL.

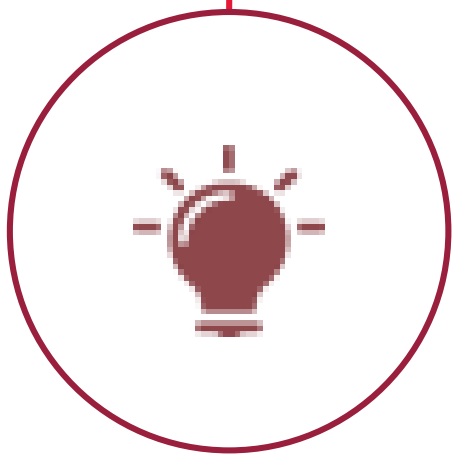
*« […] pour ce qui est des **nouvelles obligations ou des nouveaux droits** résultant du RGPD (droit à la portabilité, analyses d'impact, etc.), les contrôles opérés auront essentiellement pour but, dans un premier temps, d'accompagner les organismes vers une bonne compréhension et la mise en œuvre opérationnelle des textes. »*

CNIL.

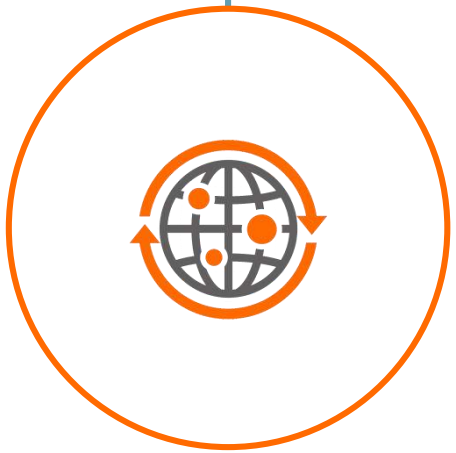
« Tout le monde ne sera pas forcément conforme le 25 mai, l'essentiel est d'avoir pris conscience et de s'engager dans cette démarche de conformité »

Maitriser son positionnement

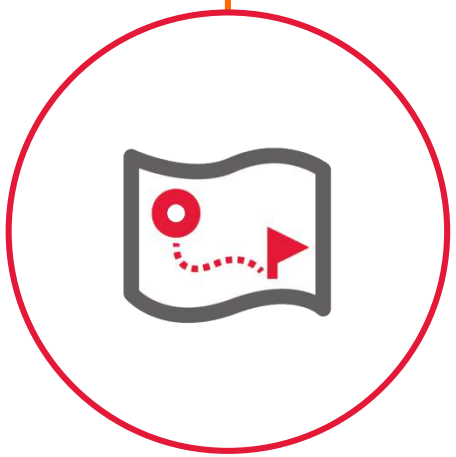
Traiter en priorité les points existant dans la législation française



Mettre en place des processus



Mettre en place la sécurité sur les nouveaux projets, corriger les écarts de l'existant dans un second temps



<u>Le secteur de la santé est très visible</u>

- ✓ Ex : SNIIRAM
- ✓ Sensibilité particulière de l'opinion publique

Exemple de planning de réalisation

Première date butoir : 25 mai 2018

Choisir le juste niveau des mesures adapté aux risques

Traçabilité

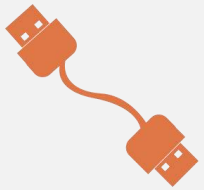
- **Rétention des logs sur les machines** ✚
- **Centralisation / Corrélation des logs** ✚✚
- **Centre Opérationnel de surveillance** ✚✚✚

Intégrité
Exactitude & Complétude

- Contrôle d'accès fonctionnels ✚
- Mise en place d'outils de gestion des accès ✚✚
- Contrôle techniques d'intégrité de base de données ✚✚✚

Confidentialité
Non diffusion & Non divulgation

- Contrôle d'accès, NDA, marquage des documents ✚
- Chiffrement des ordinateurs ✚✚
- Chiffrement de bout en bout, Pseudonymisation ✚✚✚



Disponibilité
Accessibilité & Utilisabilité

- Sauvegarde/Restauration, gestion des incidents, test de restauration ✚
- Plan de reprise d'activité, plan de continuité d'activé, tests techniques ✚✚
- Processus résilients avec des exercices de crises ✚✚✚

✚ Complexité de mise en œuvre

CGI | Business Consulting

Exemple de ré identification

Un numéro non réversible (par séjour)

Un numéro anonyme premier est créé à l'échelon de l'établissement […] par un procédé sécurisé dénommé fonction d'occultation des informations nominatives (FOIN) »

Dans les faits : 10,5 millions de patients en 2008

- Empreinte chronologique
- Mois du 1er séjour
- Age
- Sexe
- Code postal
- Etablissement

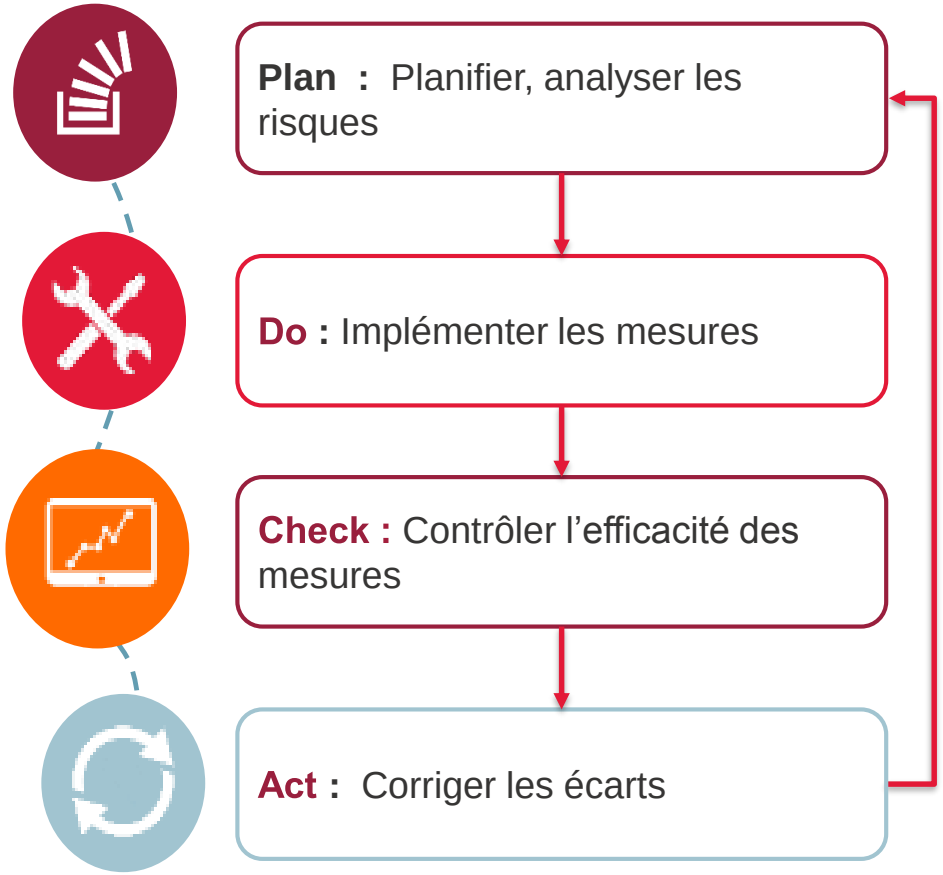
89% identifiable individuellement
100% si plus d'un séjour

Source : Présentation du Dr Blum à l'AFCDP 22/01/2012

Pour aller plus loin : un Système de Management

Un Système de Management repose sur quatre principes majeurs:

Roue de Deming ou PDCA



Notre engagement

Nous réalisons chaque mandat dans un seul but : contribuer au succès de nos clients.

CGI | Business Consulting

Thomas NGUYEN

Consultant – Conformité, Gouvernance, Security & Risk Management

caotrithomas.nguyen@cgi.com
M : +33 6 22 76 27 02

CGI | Business Consulting

Amaury COTHENET

Manager – Conformité & gouvernance Security & Risk Management

cmaury.cothenet@cgi.com

La force de l'engagement[MD]