

Sigfy!

Christophe.Delpierre@sigfy.fr

Club ISO 27001

Chez Akamai, Paris

Risk'n Tic

Management des risques

Le 19 mai 2016

Christophe Delpierre

Simple Is Good For You!

Sigfy!



Une approche simple, pragmatique, efficace



Une approche optimisée pour gérer les coûts



**Une approche efficace pour industrialiser
et améliorer les processus**



Une approche reproductible

**Il faut aussi dire oui
à une cyberdéfense efficace et
pragmatique**

Guillaume Poupard, Directeur Général de l'ANSSI

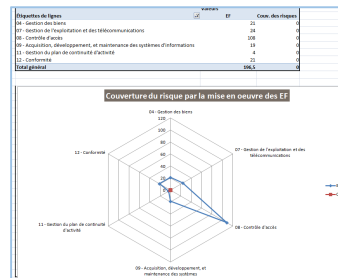
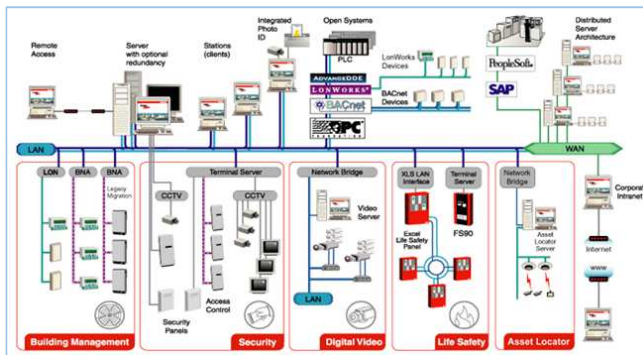
Simple Is Good For You!

LE RSSI



- Chef d'orchestre de la sécurité du S.I.
- Il protège les processus métier de l'entreprise et son patrimoine informationnel
- Il s'assure du niveau de sécurité d'application complexe et dans un milieu hétéroclite

- Un stratège
- Un communicant
- Un expert
- Un politique ("influenceur") de l'entreprise
- Un manager
- Un gestionnaire de contrats



Un gestionnaire de risques ...

Mais ne dispose que d'un tableur pour communiquer sur le niveau de sécurité atteint.

LE RSSI dans le SIH

Direction générale des offres de soins

Asip Santé

Haute autorité de santé

Agence régionale de santé

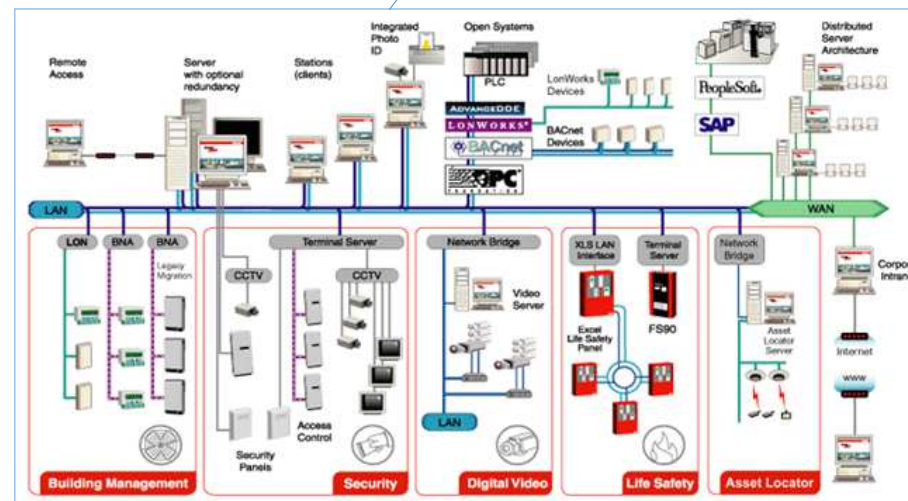
Gestion administrative du patient
Gestion du dossier (médical et paramédical) du patient
Gestion des ressources
Gestion des prescriptions et demandes d'examens
Gestion des activités médico-techniques
Urgences
Recueil d'activités, production des données T2A
Système d'information économique et financier
Système d'Information logistique et technique
Gestion des identités
Gestion des ressources humaines
Système d'Information Qualité et Gestion des risques
Système d'information de pilotage

PGSSI-S

CONNECTEE AU REFERENTIEL UNIQUE D'IDENTITES DES PATIENTS (Indicateur P1.1)
CONNECTEE AU REFERENTIEL DE SEJOURS ET MOUVEMENTS (Indicateur P1.3)

.....

Quel est le taux d'applications des domaines concernés connectées au référentiel de séjours et de mouvements ?



LE CIL dans le SI

CNIL

Réglementation locale

Réglementation Européenne, G29

Juillet 2018

Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés

Les données à caractère personnel

Le transfert des données à l'internationale

Les 10 fiches de la CNIL

Le registre du CIL

Paquet télécom

Les Cookies

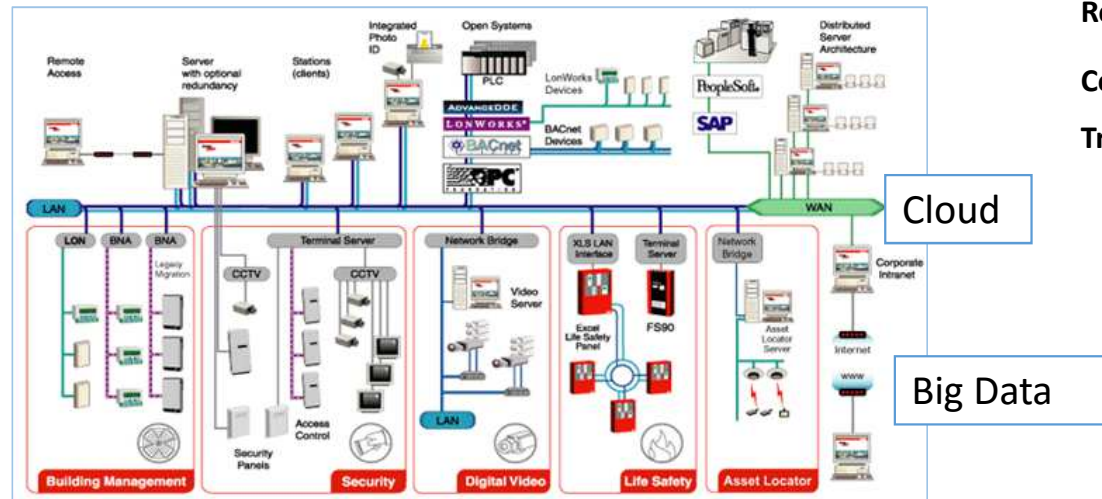
Le règlement général sur la protection des données

Droits de la personne concernée

Respect des dispositions

Contrôle et réparation

Transferts vers un pays tiers



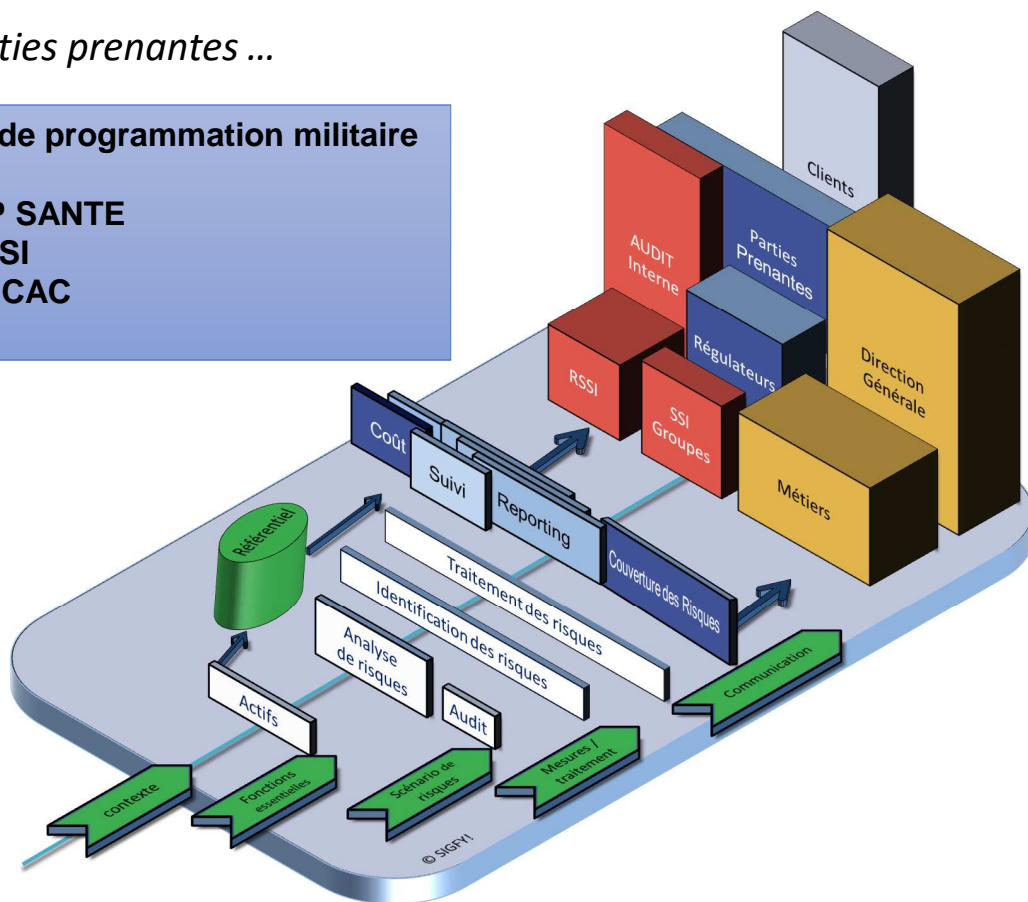
Le RSSI dans son contexte

Des parties prenantes ...

La loi de programmation militaire
L'AHS
L'ASIP SANTE
L'ANSSI
AMF / CAC
CNIL

Des référentiels

PSSI
Pre requis Hôpital Numérique
PGSSI-SANTE
L'ANSSI
PCI-DSS / ISAE3402
CNIL
27002 / Ebios



Une exigence :

Analyser les risques

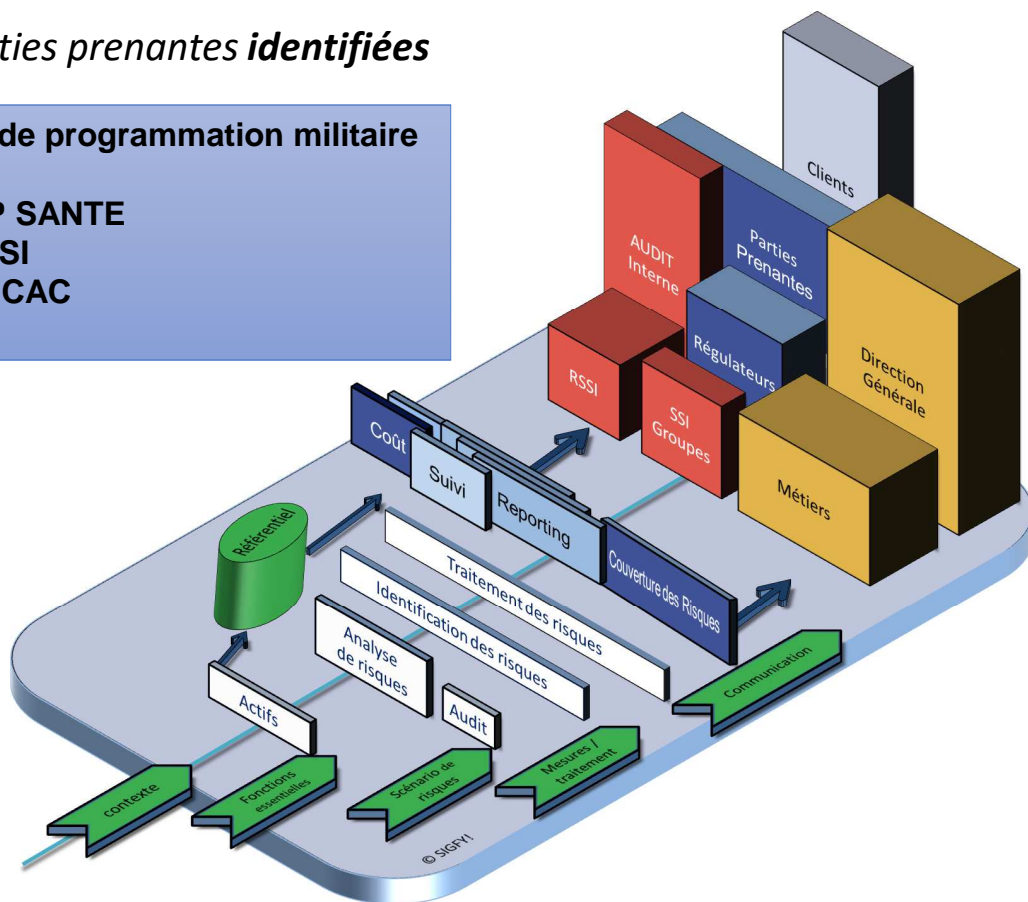
Risk'n Tic

Des parties prenantes *identifiées*

La loi de programmation militaire
L'AHS
L'ASIP SANTE
L'ANSSI
AMF / CAC
CNIL

Des référentiels *intégrés*

PSSI
Pre requis Hôpital Numérique
PGSSI-SANTE
L'ANSSI
PCI-DSS / ISAE3402
CNIL
27002 / Ebios



Pour

Analyser les risques

Risk'n Tic

Une seule interface simple, accessible via client léger et tablette

Un mode SAAS, Security as a service

Un outil modulable et évolutif

Un outil d'aide à la communication et à la décision

Risk'n Tic, un outil de management des risques :

- des processus essentiels
- Des processus métiers
- Du périmètre
- Echelles et critères de décision
- Matrice des risques
- Tableaux analytiques et fractales
- Référentiels
- Plans d'actions
- Exposition aux risques,
- coût de traitement ...

The screenshot displays the Risk'n Tic software interface, which is a risk management tool. It features a dashboard with several key components:

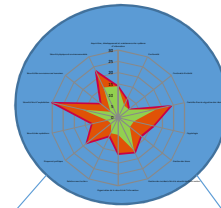
- Processus essentiels:** A table listing essential processes with columns for 'Nom', 'D', 'I', 'C', 'P', 'Actif', and 'Support'. Processes include 'Personne/Personne', 'Personne/OS', and 'Personne/OS/Network/Personne/Organisation'.
- Scénario de risques:** A section for defining risk scenarios, including 'attaque d'un Site Web Internet' and 'Maintenance liée à un défaut d'alimentation'. It includes details like 'Période', 'Impact', 'Probabilité', and 'Coût'.
- Exigences de sécurité:** A table listing security requirements with columns for 'Poids', 'Nom', 'I', 'P', 'ISO 27002', 'Ouv.', 'D.', 'Progrès', 'Statut', 'Mise à jour', and 'Historique de Statut'. Requirements include '11.1.1', '12.2.4', and '10.1.1 Politique d'utilisation des mesures cryptographiques'.
- Matrices des risques:** Three heatmaps showing 'Risque Brut', 'Risque Courant', and 'Risque Net'. Each matrix plots 'Impact' (1-4) against 'Probabilité' (1-4) with color-coded cells (red, orange, yellow, green) and numerical values.
- Référentiel:** A detailed view of a security requirement (10.1.1) with its objective and description: 'Définir une politique de chiffrement selon la sensibilité des données échangées et le support utilisé. La politique doit préciser quelles techniques sont utilisées et quelles fonctionnalités sont assurées.' It lists sub-points a), b), and c) regarding data classification, confidentiality, and encryption methods.

Simple Is Good For You!

Risk'n Tic

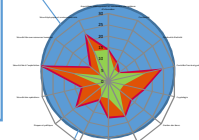
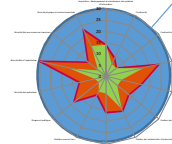
Direction
Comité sécurité

- Plan d'action par branche
- Couverture des risques majeurs

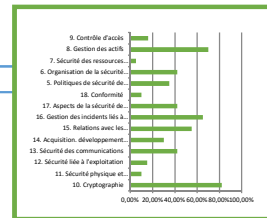


Branche Métier
ou processus métier

Plan d'action global par
branche
Matrice des risques
« branche métier »



Application



Allons voir !

The screenshot displays a risk management software interface with several key sections:

- Processus essentiels:** A table listing essential processes with columns for Name, D, I, C, P, Acct, Support, and Ref. Menace. It includes items like 'Personne/Personne', 'Réseau/Personne', and 'Réseau_OS,Hardware,Éléments,Personne,Organisation'.
- Scénario de risques:** A table of risk scenarios with columns for Name, D, I, C, P, Acct, Support, Ref. Menace, Impact Int, Impact Cible, Prob. Int., Prob. Cible, Risque, and Coûts. Scenarios include 'attaque d'un Site Web Internet' and 'malveillance les a un défaut d'habilitation'.
- Exigences de sécurité:** A table of security requirements with columns for Poids, Nom, I, P, ISO 27002, Cha..., D..., Progrès, Status, Mise à jour, and Historique de Status. It lists requirements like 'Politique d'utilisation des mesures cryptographiques'.
- Référentiel:** A sidebar on the right showing the ISO 27002 standard, specifically the 'Politique d'utilisation des mesures cryptographiques' requirement (10.1.1), which details the need for a policy on cryptographic measures based on data sensitivity.

Christophe.delpierre@sigfy.fr