Gouverner la Sécurité SI

Un retour d'expérience RSSI

Le contexte

- CUD: 200 000 habitants, 18 communes

- Ville: 89 000 habitants

- Mutualisation DSI juin 2016: création DSIM
- 60 agents
- 230 applications
- 3000 utilisateurs
- Schéma Directeur: 45 projets répartis en 5 chantiers
- Axe fort sur la mobilité, la GRC, la dématérialisation, le collaboratif, l'Open Data, + O365

Les 3 enjeux de la SSI

- **Assurer la continuité des activités réalisées par la Collectivité ;**
- **Prévenir la fuite d'informations sensibles ;**
- **Renforcer la confiance des agents, de la DG, des Elus, des citoyens et des partenaires**

⇒ Développer la Confiance numérique!

Les défis à relever

- La menace
  - Ransomware
  - Vol de données
  - Piratage

  - Téléservices, Cloud, BYOD, Collaboratif, …

- La connaissance du SI, des risques
  - Vision de l'état de la sécurité informatique
  - Cartographie: biens, risques
  - Les projets

Les défis à relever

- La culture sécurité
  - Les processus (gestion de comptes, inventaire, alertes, …)
  - Les usages, la sensibilité à la sécurité
  - La stratégie

- Conformité
  - CNIL, RGS, RGDP
  - Les référentiels: PSSI, charte
  - Normes (27001)

=> besoin de gouvernance de la SSI

Le SMSI mis en œuvre à Dunkerque

- Nomination d'un RSSI, rattaché directement au DSI

- Coordonner la SSI
- Etudier les risques
- Veiller à la conformité règlementaire (avec le CIL)
- Promouvoir la démarche globale de sécurité
- Évaluer périodiquement la qualité du SMSI
- Le RSSI n'intervient pas au plan opérationnel

- Le Comité de Sécurité SI

- Porter la SSI à un niveau stratégique
- Valider la PSSI, les responsabilités globales
- Surveiller l'évolution de l'exposition aux menaces
- Suivre les incidents de sécurité de l'information
- Approuver les initiatives renforçant la sécurité de l'information
- Valider, puis vérifier l'avancement des travaux

- Trimestriel
- DGAs concernés, DSI, RSSI, chefs de service DSIM, CILs, représentants DIRCOM

Le SMSI mis en œuvre à Dunkerque

- Le Comité Opérationnel de Sécurité

- Suivi opérationnel de la mise en œuvre des plans d'actions
- Processus opérationnels
- Contrôles
- Questions d'actualité
- Incidents de sécurité de la période

- Par quinzaine
- RSSI, chef de service Infrastructures, référents sécurité Infrastructures, chefs de service DSI

- Portage par l'encadrement fondamental!

- La sécurité dans les projets

- Etude de risques dès l'idée du projet (simple relecture du CCTP déjà trop tard!)
- Prendre en compte tout le processus, et toutes les origines de risque (organisationnelle, humaine, technique, ….)
- Tenir à jour une cartographie des données, des risques
- Responsabiliser les acteurs (DSI, Métiers)
- Intégrer la SSI tout au long du cycle de vie du SI

- Portage par l'encadrement fondamental!

Analyse de risques basée sur la méthode EBIOS: Evénements redoutés, critères de Disponibilité, Intégrité, Confidentialité, Preuve

Le cas particulier des applis RGS

- La méthodologie d'étude des risques est la même que pour les autres projets.
- Un cadre néanmoins plus formel

Premier ministre

Agence nationale de la sécurité des systèmes d'information

Référentiel Général de Sécurité

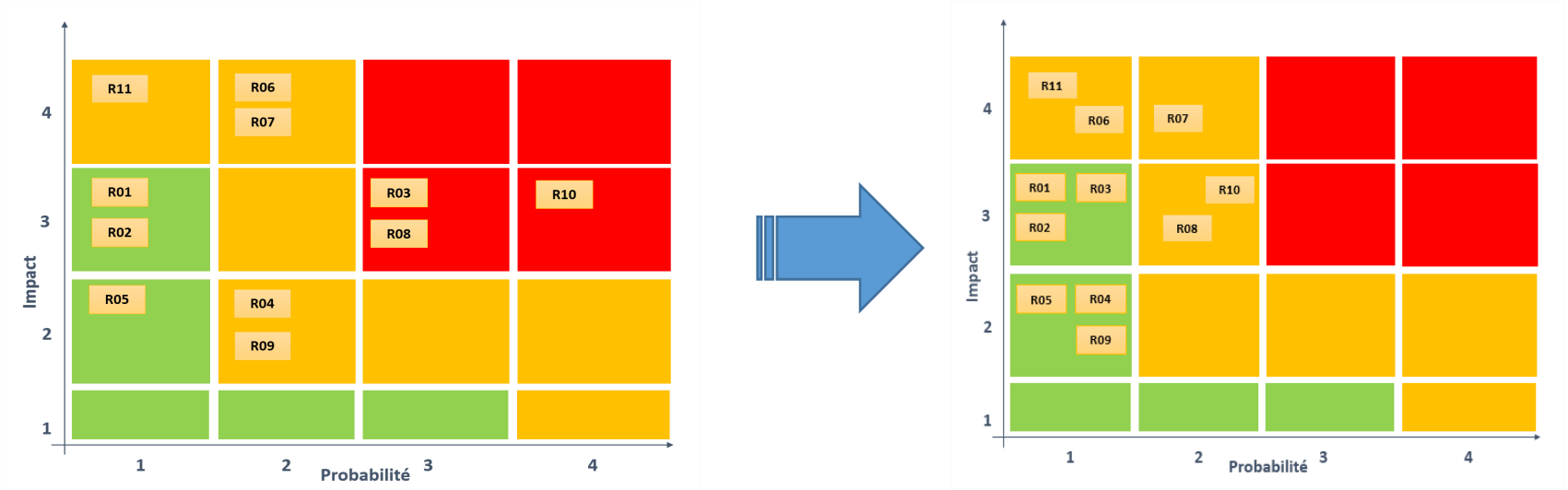
Version 2.0

- L'homologation est prononcée en interne par un Comité d'Homologation:
  - AUTORITE: DGA CUD ou Ville
  - Le CIL
  - Le DSI
  - Le RSSI
  - Représentant Maîtrise d'ouvrage
  - Chef de Projet
- Valable de 3 à 5 ans, revue annuelle

Méthodologie d'homologation au RGS

Actions	Quand	Acteurs
Réaliser l'étude initiale: événements redoutés, étude des risques initiaux Clauses dans les AO	Démarrage du projet	MOA, CdP, RSSI
Préconiser des mesures de sécurité (mesures techniques, juridiques, organisationnelles)	Lors de l'avancée du projet	RSSI, CdP, MOA
Faire une recette de sécurité (risques résiduels)	Avant le démarrage	RSSI - CdP
Ecrire le document de synthèse à destination du comité d'homologation	Avant le démarrage	RSSI, validation MOA
Procéder à l'homologation	Avant le démarrage	Comité d'homologation
Afficher l'homologation: arrêté et appli	Pour le démarrage	Juridique, CdP

Méthodologie d'homologation au RGS



M04	Habilitations	Vérifier l'adéquation avec la politique de mot de passe de la CUD, en particulier sur les points suivants : - A minima 8 caractères et lettres, chiffres et caractères spéciaux. - Verrouillage automatique des comptes après X tentatives infructueuses, pour une durée de 30 minutes - Renouvellement tous les 3 mois	OUI	A discuter et adapter Possibilité d'imposer des règles mdp dans l'appli? LDAP pour les agents CUD. Fonctionnalités chgt mdp désactivées. Raccordement prévu avec la fédération d'identité. Externes: formulaire et création par administrateur	Oui	En cours
M05	Habilitations	Formaliser le processus de création, suppression, modification de compte et les validations hiérarchiques nécessaires.	NON	A écrire	Oui	En cours
M06	Habilitations	Définir des profils applicatifs alignés sur les responsabilités métiers et les missions des utilisateurs.	NON	A écrire	Oui	En cours
M07	Habilitations	Définir le processus de revue des comptes par le propriétaire de l'application (contrôle des personnes autorisées et de leur profil).	NON		Oui	En cours de réflexion
M08	Habilitations	Mettre en place un mécanisme de délégation des droits.	OUI	Plusieurs admin, à définir, etc.	Non	RAS
M09	Habilitations	Tracer les opérations relatives aux modifications d'habilitations.	OUI		Non	RAS
Déploiement et RH						
M10	Formation	Former et sensibiliser les utilisateurs afin de les accompagner au changement. Charte utilisateurs à produire.	NON	Charte à présenter lors du Comité d'homologation	Oui	En cours

Méthodologie d'homologation au RGS

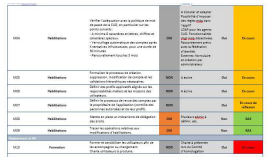
- Le dossier RGS prend la forme d'un dossier de sécurité, composé de plusieurs documents, qui sera présenté en synthèse au comité d'homologation.

✓Analyse de risque RGS calquée sur l'organisation sécurité

✓ Document de synthèse à destination de l'autorité d'homologation

Questionnaire sécurité

Analyse de risque



Suivi des mesures

Dossier de sécurité

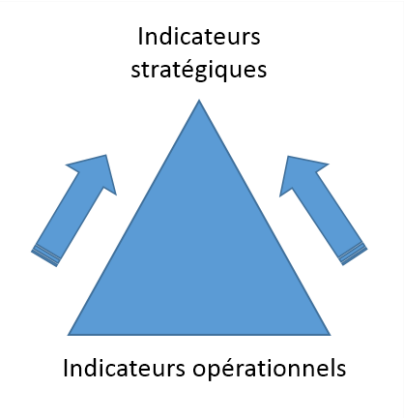
Autres éléments primordiaux

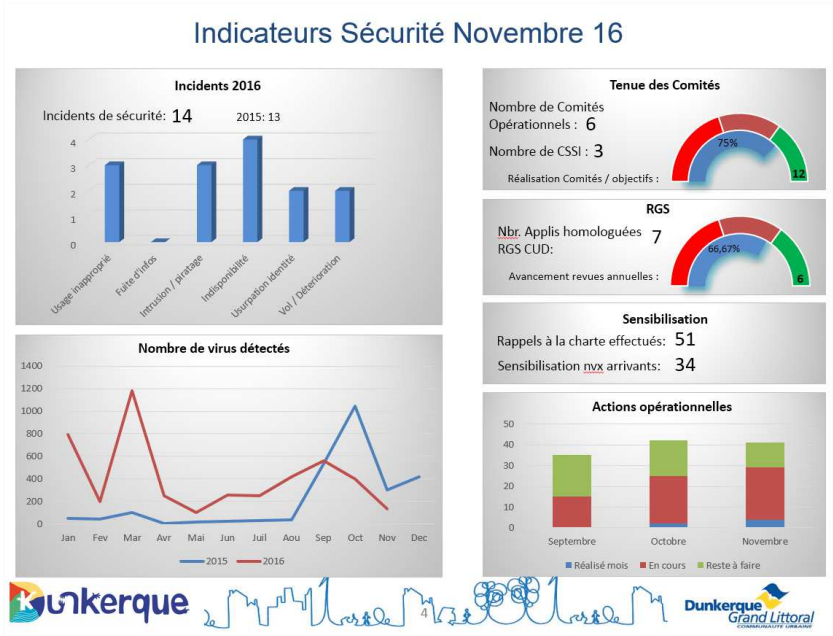
- Maîtrise des risques informatiques
  - Equipements de sécurité: analyse de logs (à faire)
  - Tests de vulnérabilités réguliers
  - Tests d'intrusion pour certains projets
  - Audit général de sécurité: test intrusion interne, externe, physique, ingénierie sociale

Connaissance des menaces, fondamental!

Autres éléments primordiaux

- Indicateurs:





Conformité Règlement Européen?

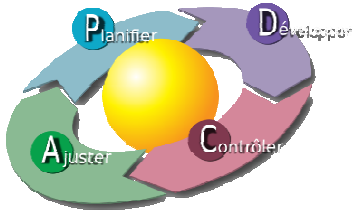
- Sensibilisation, intégration en amont de chaque projet
- Analyses d'impacts relatives à la protection des données
- Cartographie des données personnelles
- Sécurité des données: droits, processus, pseudonymisation
- Nomination du DPO
- Détection des atteintes aux données, procédure d'alerte
- Renforcement des obligations des sous-traitants (marchés publics)

Les leviers essentiels

- Conformité (CNIL, RGS, RGDP, ISO 27001): levier essentiel!
- Expliquer
- Transversalité, responsabilisation, impliquer!
- Ne pas privilégier la stricte vision technique, ni trop « projet » ou juridique

Les leviers essentiels

- S'appuyer sur des prestataires reconnus, mais garder l'initiative!
- Vision Direction Générale: risques concrets, plans d'action et suivi: « Dire ce que l'on fait »
- Revisiter régulièrement le SMSI (roue de Deming)



<u>Démontrer</u> la capacité de la Collectivité à fournir un SI de confiance.

- Contexte de mutualisation de DSI
- Ouverture d'un catalogue de services