



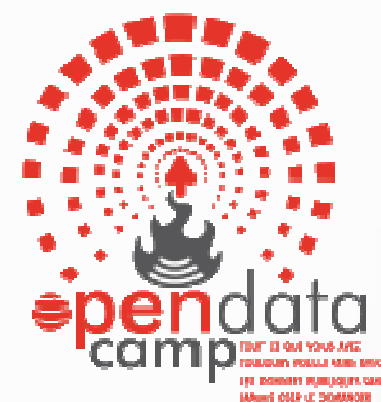
La gestion de l'info dans le secteur public

- Le 9 novembre 2011-

Yannick Bouchet
Romain Zerr

-Open Data

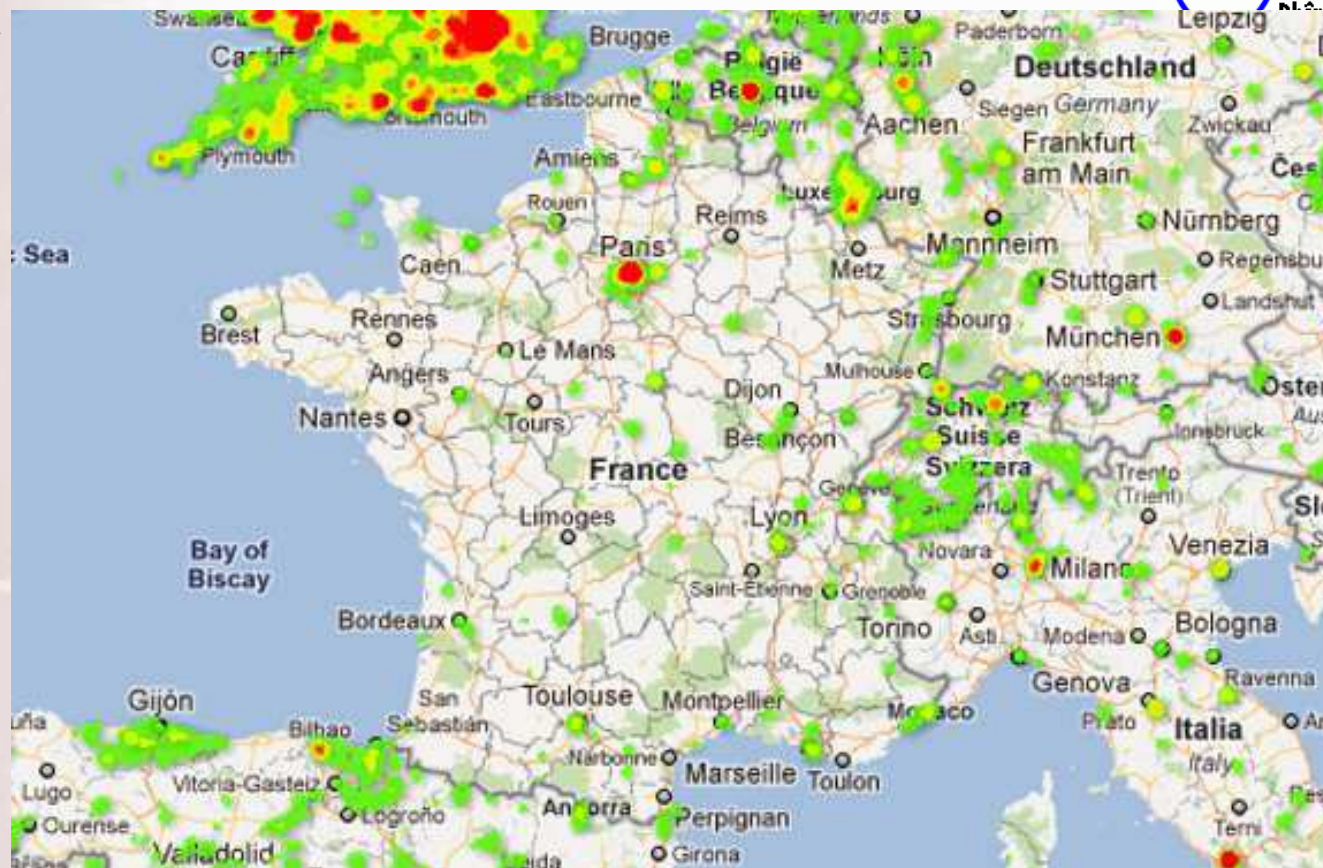
OPEN DATA



-Veille territoriale



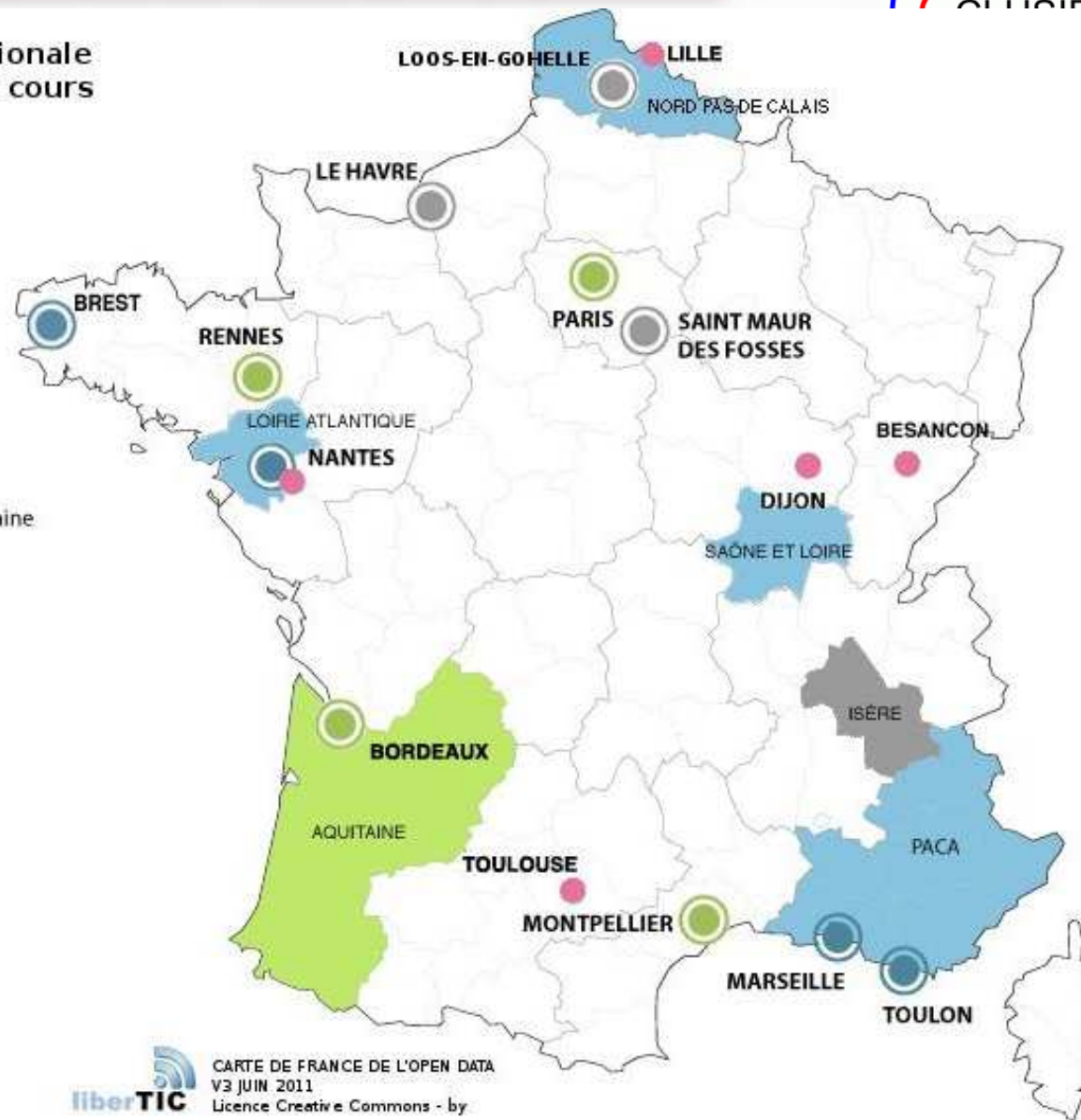
Open Data en France



Plateforme nationale
data.gouv.fr en cours

« Par exemple le portail de Paris et un projet de la région Sud-ouest (Datalocale) s'adossent à la licence ODbL (Open Database Licence) de l'Open Knowledge Foundation, tandis que le site de Rennes a choisi la licence APIE (« Licence de réutilisation des données publiques - Rennes Métropole en accès libre »), tout comme la ville de Montpellier. »*

- Ville et/ou Communauté Urbaine
- Déjà ouvert
- En cours
- Y réfléchit
- Mouvement citoyen



liberTIC
CARTE DE FRANCE DE L'OPEN DATA
V3 JUIN 2011
Licence Creative Commons - by

*Source : <http://www.lemagit.fr/article/france-donnees-open/9731/1/open-data-ecosysteme-francais-construit-petit-petit/>

Cet état de l'art a été initialement publié en anglais sur le site de l'Open Knowledge Foundation, le 20 janvier 2010. L'OKFN est une organisation anglaise en pointe sur l'OpenData. Elle est notamment à l'origine du projet WhereDoesMyMoneyGo.org, de l'OpenDefinition pour des standards de données ouvertes et du registre de données participatif CKAN. Ce registre, en cours de traduction dans plusieurs pays européens, est repris par le gouvernement anglais pour l'architecture de son projet data.gov.uk.

Source : <http://www.regardscitoyens.org/>

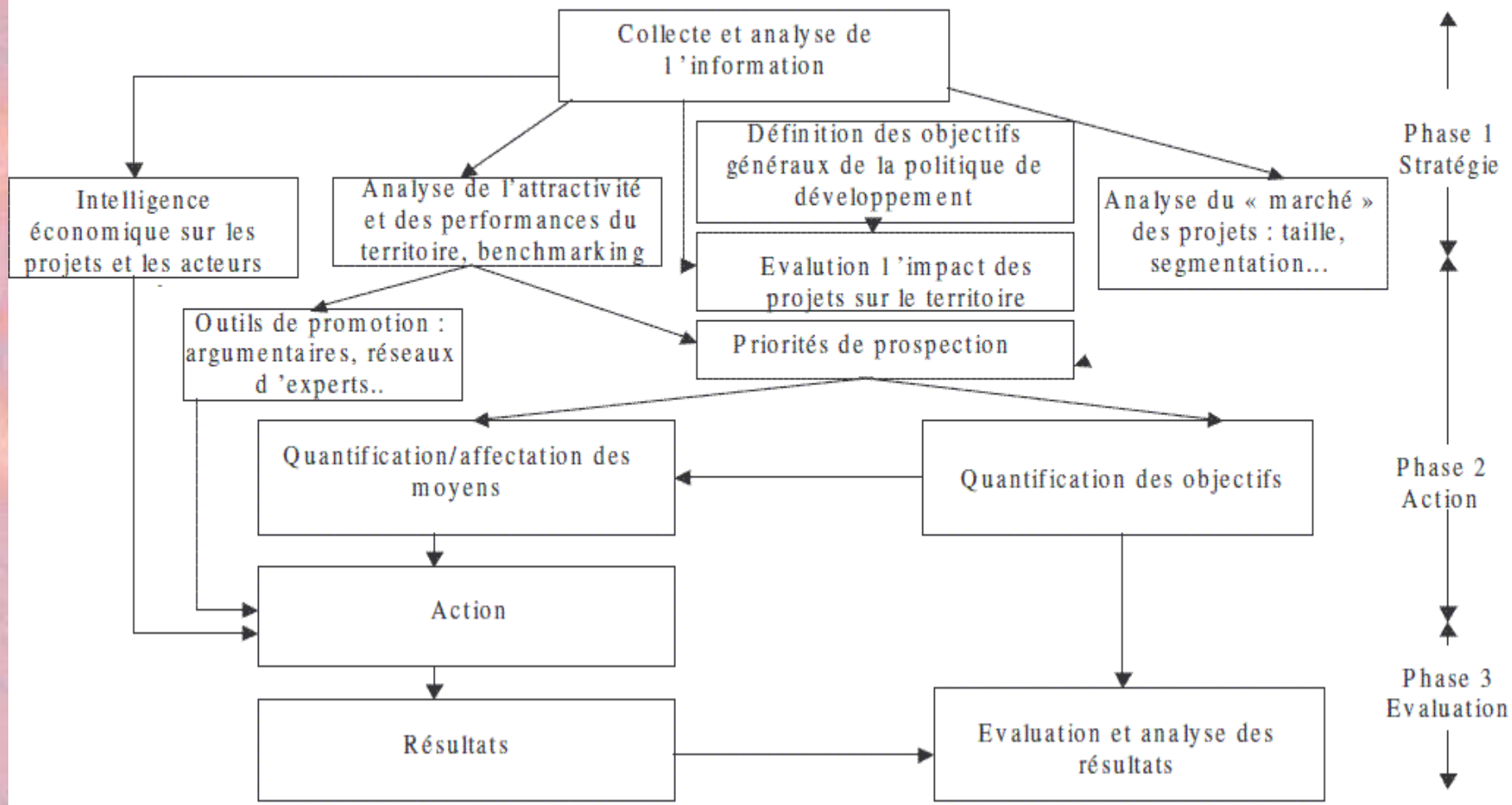
Images de la veille territoriale

La veille territoriale, un aide pour le marketing territorial ???

Le marketing territorial

Face à une compétition internationale de plus en plus dure pour l'attraction des projets d'investissement internationalement mobiles, les agences de promotion territoriales doivent définir des « stratégies marketing » destinées à accroître leur « part de marché » face aux territoires concurrents. Ce processus mobilise des outils qui ont des points communs importants avec le marketing d'entreprise, mais également des spécificités fortes liées à la nature du « produit » offert (une offre territoriale complexe) et du client (une entreprise à la recherche d'un lieu de localisation optimal). Il conduit à trois résultats essentiels : 1) l'identification des priorités de prospection ; 2) la rédaction des argumentaires promotionnels ; 3) l'identification des mesures d'ordre interne destinées à améliorer l'attractivité du territoire. Enfin, il doit nécessairement s'intégrer dans un dispositif plus large de pilotage stratégique bouclé et itératif.

Schéma d'une démarche de diagnostic territorial



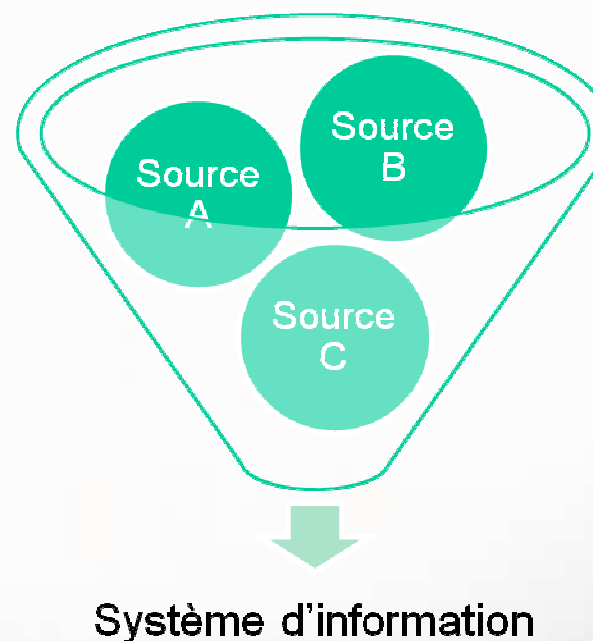
Le Marketing territorial : pourquoi, comment ? Par Fabrice Hatem Conseiller économique AFII

Le cycle de vie de l'information

Idéalement



fréquemment



Le référentiel général de sécurité

Un référentiel adapté à toutes les autorités administratives pour la mise en œuvre concrète des échanges sécurisés

Le RGS est un recueil de règles et de bonnes pratiques destiné aux autorités administratives pour les accompagner dans la sécurisation de leurs échanges électroniques. Il s'agit d'un référentiel adaptable aux enjeux et besoins spécifiques de chaque autorité administrative. Grâce au RGS, celle-ci connaît les exigences à respecter et les moyens de protection adaptés à ses besoins de sécurité propres.

Périmètre du RGS

Le RGS n'a pas pour vocation à simplifier le fonctionnement interne des Autorités Administratives, cela sera cependant un effet de bord bénéfique.

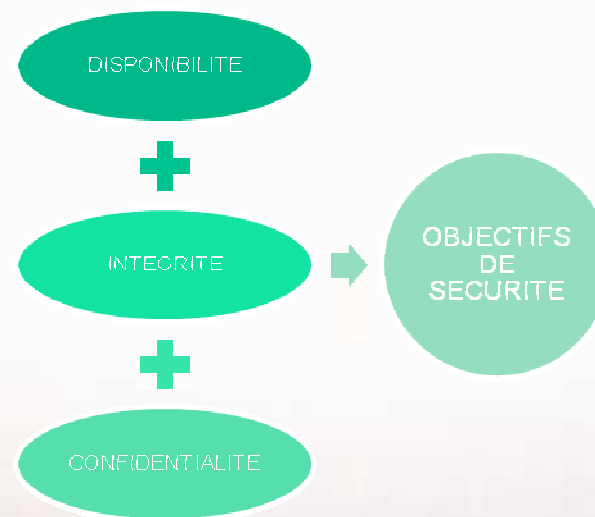
-Il s'applique à tout échange d'information quel qu'il soit entre les autorités administratives et les usagers de ces informations du moment que certaines fonctions de sécurités préalablement identifiés sont nécessaires :

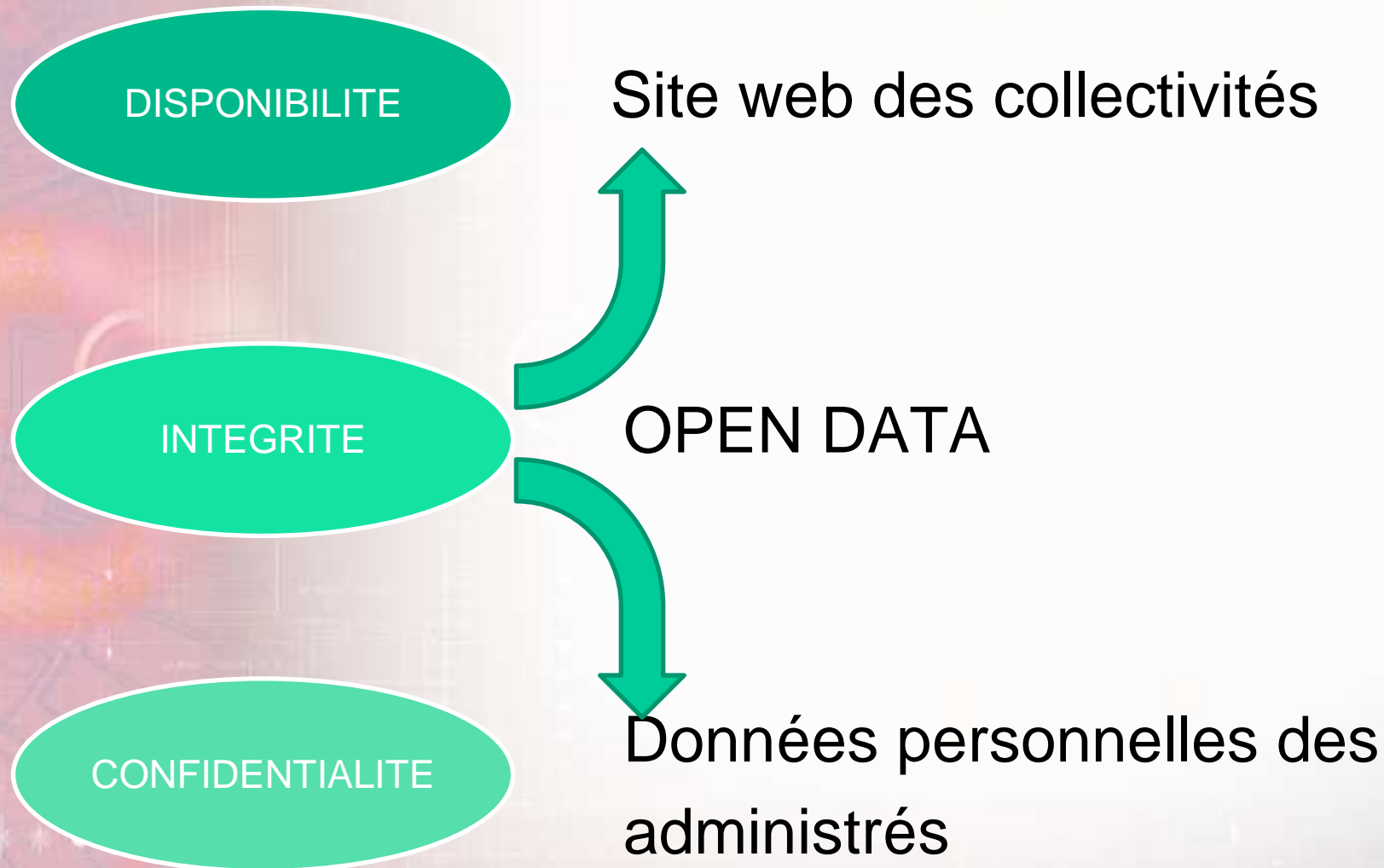
- Authentification
- Confidentialité
- Signature
- Horodatage

Mise en place de bonnes pratiques

Au-delà de ses obligations, il permet aux collectivités de se poser les bonnes questions quant aux données manipulées.

Cela amène donc à qualifier les données et les organiser selon les niveaux de sécurité requis déduit de leur qualification





Quel niveau de sécurité

Au-delà de ses obligations, il permet aux collectivités de se poser les bonnes questions quant aux données manipulées.

Cela amène donc à qualifier les données et les organiser selon les niveaux de sécurité requis déduit de leur qualification

Niveau des conséquences potentielles (Reportez ici la valeur maximale des réponses aux questions 1 à 3)						2
4	Le fait que les données de votre système soient inaccessibles est-il grave ? <i>Exemple : vous ne pouvez pas accéder aux données en raison d'une panne matérielle.</i>	Je ne sais pas	Non, le fait qu'il ne soit pas accessible ne gêne quasiment pas l'activité	Oui, le fait qu'il ne soit pas accessible perturbera l'activité de manière significative	Oui, le fait qu'il ne soit pas accessible peut être fatal pour l'activité	1
5	Le fait que les données de votre système soient altérées est-il grave ? <i>Exemple : un virus a modifié des valeurs dans une base de données, les remettant toutes à 0.</i>	Je ne sais pas	Non, le fait que les données soient altérées ne gêne quasiment pas l'activité	Oui, le fait que les données soient altérées perturbera l'activité de manière significative	Oui, le fait que les données soient altérées peut être fatal pour l'activité	2
6	Le fait que les données de votre système ne soient pas ou plus confidentielles est-il grave ? <i>Exemple : la liste des bénéficiaires du service social est dévoilée.</i>	Je ne sais pas	Non, le défaut de confidentialité ne gêne quasiment pas l'activité	Oui, le défaut de confidentialité perturbera l'activité de manière significative	Oui, le défaut de confidentialité peut être fatal pour l'activité	2

Besoin de sécurité

Somme des quatre valeurs	Besoin de sécurité du système
De 0 à 3, ou si l'un des totaux partiels est à 0	Attention, vous devez vous faire assister pour ce diagnostic.
De 4 à 6	1 - Faible
De 7 à 9	2 - Moyen
De 10 à 12	3 - Fort

Niveau de maturité (extrait)

Questions	Oui / Non
Les activités de sécurité sont-elles réalisées en utilisant des pratiques de base (bonnes pratiques de sécurité, référentiels de mesures...)?	Oui.
Si la case précédente est à Oui, alors votre organisme est situé à un niveau de sécurité élémentaire, sinon, une démarche assistée est indispensable.	niveau élémentaire
Les activités de sécurité sont-elles planifiées ?	oui
Les acteurs affectés à des activités de sécurité sont-ils formés (en interne ou par un organisme de formation) à la SSI (niveau de compétence en sécurité jugé suffisant) ?	Oui
Certaines pratiques de sécurité sont-elles formalisées dans des documents spécifiques (procédures) ?	Oui.
Des mesures de sécurité sont-elles en place ?	Oui, les sauvegardes, le pare-feu, l'antivirus.
Les autorités compétentes sont-elles informées des mesures effectuées ?	Oui.
Si toutes les cases précédentes sont à Oui, alors votre organisme a un niveau de sécurité moyen	Niveau moyen

On en déduit la démarche RGS

		Besoin de sécurité du Système		
		Faible	Moyen	Fort
Niveau SSI de l'organisme	élémentaire	<i>Pianissimo</i> : Démarche autonome à minima	<i>Mezzo</i> : Démarche assistée approfondie	<i>Mezzo</i> : Démarche assistée approfondie
	moyen	<i>Pianissimo</i> : Démarche autonome à minima	<i>Mezzo-Forte</i> : Démarche autonome approfondie	<i>Mezzo</i> : Démarche assistée approfondie
	avancé	<i>Pianissimo</i> : Démarche autonome à minima	<i>Forte</i>	<i>Forte</i>

Définition du dossier de sécurité

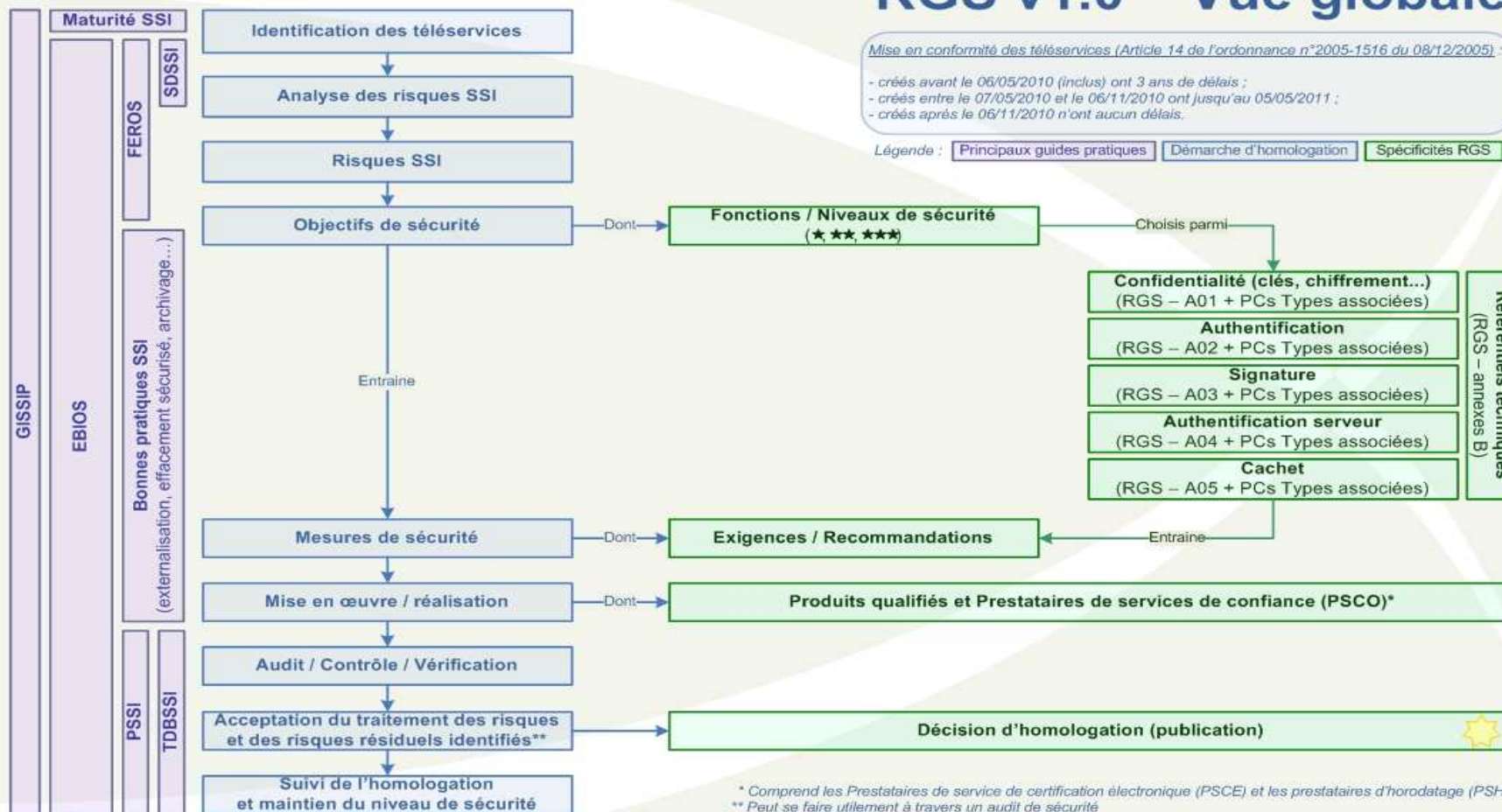
	Pianissimo	Mezzo	Mezzo Forte
Stratégie d'homologation*	Indispensable		
Référentiel de sécurité existant*	Si existant		
Document présentant les risques identifiés et les objectifs de sécurité*	Indispensable		
Procédures d'exploitation sécurisée du système*	Indispensable		
Journal de bord de l'homologation*	Fortement recommandé		
Certificats de qualification des produits ou prestataires	Si existant		
Résultats d'audits	Fortement recommandé	Indispensable	
Décision d'homologation	Indispensable		
<i>Spécifiquement pour les systèmes déjà en service :</i>			
Tableau de bord des incidents et de leur résolution*	Indispensable		
Résultats d'audits intermédiaires		Recommandé	
Journal des évolutions du système*	Indispensable		

RGS v1.0 – Vue globale

Mise en conformité des téléservices (Article 14 de l'ordonnance n°2005-1516 du 08/12/2005) :

- créés avant le 06/05/2010 (inclus) ont 3 ans de délais ;
- créés entre le 07/05/2010 et le 06/11/2010 ont jusqu'au 05/05/2011 ;
- créés après le 06/11/2010 n'ont aucun délais.

Légende : Principaux guides pratiques | Démarche d'homologation | Spécificités RGS



Les délais

- Tout nouveau téléservice mis en place doit être à ce jour homologué RGS.
- Les téléservices antérieurs ont jusqu'en mai 2013 pour se mettre en conformité
- Les collectivités sont en retard. Manque de compétences internes, manque de prestataires externes, conséquences juridique minimales.

Prise de conscience variée:

appel a projet opendata la rochelle 2012 :

Le choix du lauréat se fera à partir de l'analyse d'un dossier technique qui regroupera notamment les spécifications générales et détaillées de l'application. Hormis le rôle central que devra occuper la donnée publique, il sera également pris en compte le respect des recommandations du Référentiel Général d'Interopérabilité (R.G.I.), du Référentiel Général de Sécurité (R.G.S.) ainsi que du Référentiel Général d'Accessibilité (R.G.A.).

opendata71 : aucune référence au RGS

Plateforme de dématérialisation stela du SICTIAM

L'occasion pour le Président du SICTIAM de voir le travail mené pendant un an par son équipe couronné de succès. « Nous avons travaillé de concert avec l'Agence Nationale de la Sécurité des Systèmes d'Information pour mettre en œuvre cette méthode d'homologation RGS. Aujourd'hui c'est avec beaucoup de fierté que je vous annonce que la plateforme Stela servant à la télétransmission d'actes entre les collectivités territoriales et les services de l'Etat est le 1er système d'information en France homologué RGS ».

