Pas-de-Calais
Le Département

Homologation RGS

COTER NUMERIQUE

20 Octobre 2021

Direction des Services Numériques

Rappels sur le Référentiel Général de Sécurité (RGS)

Objectifs

- Gagner la confiance des usagers dans l'administration électronique
- Attester formellement de la prise en compte de la sécurité du télé-service (homologation)

Contexte

- Ordonnance n°2005-1516 du 8 décembre 2005 relative aux **échanges électroniques entre les usagers et les autorités administratives** et **entre les autorités administratives**
- Prérequis de l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) qui a publié la version 2.0 du RGS et le guide de l'homologation de sécurité en Juin 2014

Organisation liée à l'homologation

L'autorité d'homologation

- Elle assume la responsabilité afférente à la décision d'homologation notamment pour accepter les risques résiduels
- Pour prendre cette décision d'homologation, elle examine le dossier de sécurité du projet avec l'aide de la commission d'homologation

La commission d'homologation

- Elle est chargée d'examiner le dossier de sécurité du projet de télé-service
- Elle émet un avis sur l'homologation du télé-service après avoir recueilli l'avis des experts techniques et de sécurité

Démarche d'homologation

Identification des besoins de sécurité SI

Selon les critères de :
- Disponibilité
- Intégrité
- Confidentialité
- Traçabilité

Evaluation du niveau de sécurité SI

Sur la base de :
- Tests d'intrusion
- Bonnes pratiques SSI

Analyse des risques SSI

En fonction du :
- Niveau d'impact (besoin SSI)
- Niveau de vraisemblance (vulnérabilités SSI)

Décision d'homologation

- Par l'autorité d'homologation sur avis de la commission d'homologation
- En fonction des niveaux de risque

REFUS D'HOMOLOGATION → Arrêt / absence de mise en service du téléservice

HOMOLOGATION SOUS RESERVE → Mise en place du plan d'action sous le délai : XXX

HOMOLOGATION → Acte réglementaire d'homologation

Echelle d'impact

Impact/Gravité	Conséquences agents	Conséquences Usagers / bénéficiaires	Conséquences financières	Conséquences sur l'image	Conséquences juridiques	Conséquences organisationnelles
1. Négligeable	Conséquences négligeables pour l'agent (gênes, mécontentement)	Conséquences négligeables pour l'usager (gênes, mécontentement)	Perte financière négligeable	Image affectée uniquement en interne	Avertissement, plainte sans suite	Perte de temps sans conséquences pour l'activité
2. Modéré	Mise en difficulté financière modérée, retard ou difficulté dans l'exercice de ses missions peu impactant ou situation surmontable sans difficulté pour l'agent	Mise en difficulté financière modérée, retard de prise en charge peu impactant ou situation surmontable sans difficultés par l'usager / le bénéficiaire	Perte financière significative, mais modérée au regard des enjeux économiques	Image affectée à l'extérieur pendant un bref délai (dénonciation isolée sur un média alternatif : forum, tracts, ...)	Mise en demeure ou rappel à la loi, contentieux Pénalité	Ralentissement ou perturbation des activités
3. Grave	Mise en difficulté financière Important, retard ou difficulté dans l'exercice de ses missions impactant ou situation surmontable avec difficultés par l'agent	Mise en difficulté financière Important, retard de prise en charge impactant ou situation surmontable avec difficultés par l'usager / le bénéficiaire	Pertes financières Importants	Image affectée à l'extérieur à moyen terme (dénonciation dans la presse locale), mise en cause explicite (agents)	Délit entrainant une condamnation, sans responsabilité pénale Sanction financière, annulation d'actes	Arrêt partiel des activités
4. Critique	Mise en difficulté financière très importante, impossibilité d'exercer ses missions, mise en danger ou situation insurmontable par l'agent	Mise en difficulté financière très importante, mise en danger ou situation insurmontable par l'usager / le bénéficiaire	Pertes financières très importantes, remettant en cause le bon fonctionnement du Département	Image affectée à long terme (dénonciation dans la presse nationale), mise en cause explicite (Direction, Président)	Condamnation pénale	Arrêt total des activités essentielles Paralysie importante de l'organisation

Echelle de vraisemblance

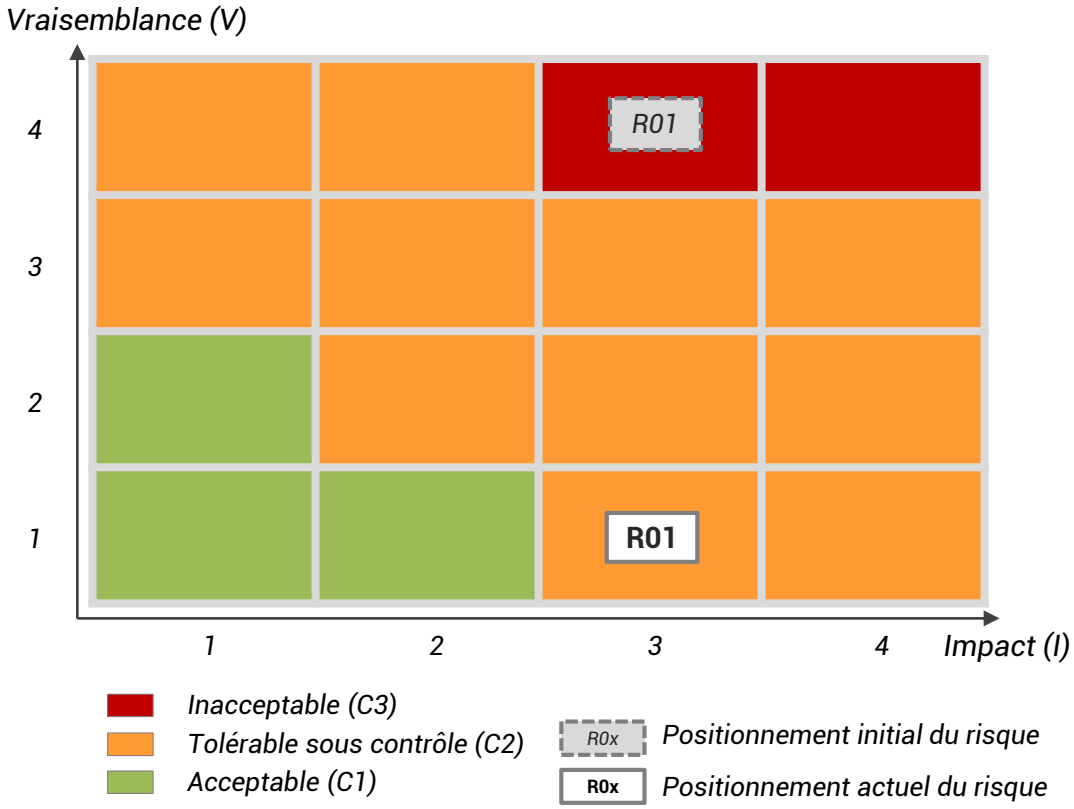
1 – Improbable	Fréquence de survenance supérieure à 5 ans, ou contexte limitant très fortement la survenance de l'événement
2 - Peu probable	Fréquence de survenance entre 1 et 5 ans, ou contexte limitant la survenance de l'événement
3 – Probable	Fréquence de survenance entre 6 mois et 1 an, ou contexte favorisant la survenance de l'événement
4 - Très probable	Fréquence de survenance inférieure à 6 mois, ou contexte favorisant fortement la survenance de l'événement

Echelle liée aux vulnérabilités des tests d'intrusion

Mineur	Pas de conséquence directe sur la sécurité du système d'information audité
Important	Conséquences isolées sur des points précis du système d'information audité
Majeur	Conséquences restreintes sur une partie du système d'information audité
Critique	Conséquences généralisées sur l'ensemble du système d'information audité

Gestion des risques - Principes

- Matrice utilisée



Exemple :

- Besoin SSI

Critère	Besoin	Type d'impacts en cas d'incident
Confidentialité	■■■□	• Image • Juridique • Financier

- Vulnérabilité SSI

Vulnérabilité	Niveau	Etat
Accès http au lieu de https	Majeur	Corrigé

- Risque SSI :

Risques consolidés - Exemple	V	I	C
R01 - Perte de confidentialité des données	4→ **1**	**3**	C2

Eléments transverses à prendre en compte dans le cadre de la commission d'homologation :

- Politique de Sécurité des Systèmes d'Information, et des politiques opérationnelles
- Charte de bon usage des moyens informatiques
- Démarche de sécurité Projets (fiche sécurité à compléter pour chaque nouveau projet DSN)
- Processus de gestion de crise SSI
- Actions de sensibilisation
- Mesures de sécurité techniques (Antivirus, Antispam, Firewall, salle informatique de secours, accès distants sécurisés, etc.)

Remarques :

- Les aspects RGPD ne sont pas traités dans le cadre de ces analyses de risques (mentions d'information, minimisation des données, durée de conservation, etc.) : à traiter en parallèle, mais non pris en compte dans l'évaluation des risques de sécurité.

- Les expérimentations d'une durée inférieure à 6 mois ne sont pas prises en compte dans le périmètre d'homologation.

Autour de moi

- Description :

  Permet aux usagers de géolocaliser précisément chaque lieu de service public et de rechercher les informations via une cartographie interactive. Complémentaire à Wikisol62

- Catégories de données traitées
  - Adresse IP
  - Coordonnées du formulaire de contact (Coordonnées professionnelles)
  - Critères de recherche

- Précisions
  - Site autourdemoi.pasdecalais.fr : développé en interne et hébergé chez DRI

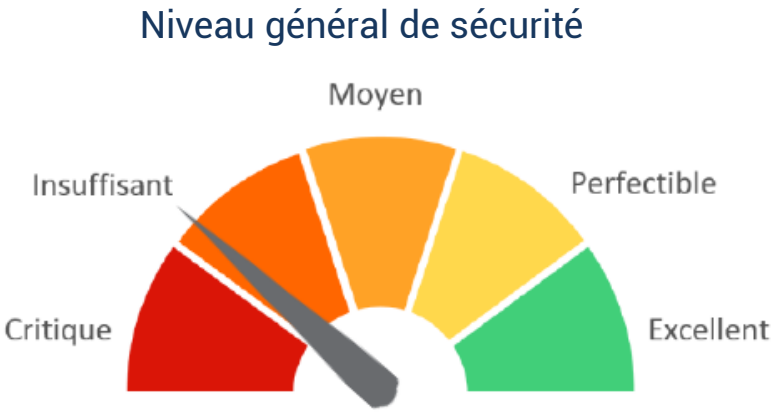
Autour de moi

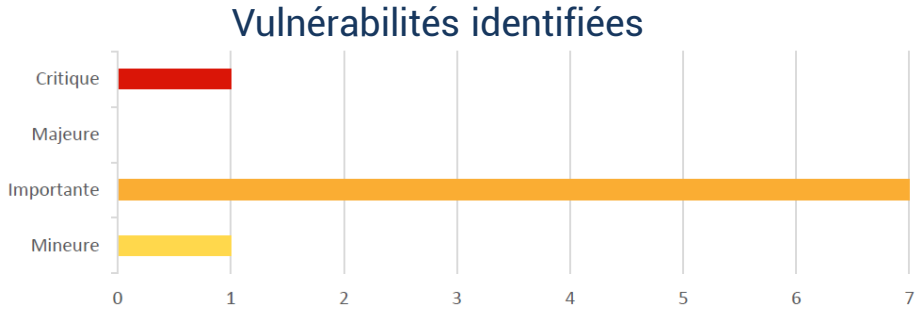
- Synthèse des besoins de sécurité métier :

Critère	Besoin	Type d'impacts en cas d'incident	Commentaires
Disponibilité	■■□□	• Image • Usager • Organisationnel	Impact notamment d'image
Intégrité	■■□□	• Image • Usager • Organisationnel	Impact notamment d'image
Confidentialité	■□□□	• Image	
Traçabilité	■■□□	• Juridique	

Autour de moi

- Synthèse des tests d'intrusion (Janvier 2021) :

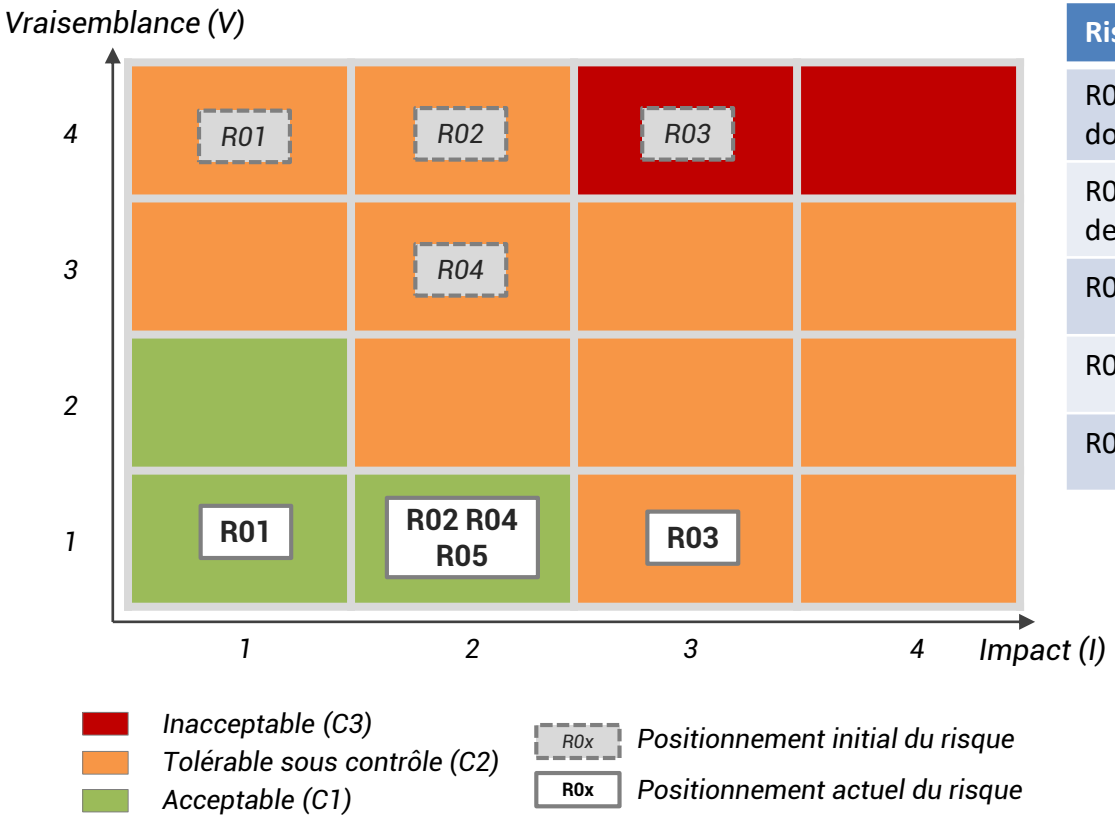




N°	Libellé de la vulnérabilité	Niveau	Etat
1	L'application est vulnérable aux attaques par injection SQL	Critique	Corrigé
2	L'application est accessible via le protocole HTTP	Important	Corrigé
3	Le cookie n'est pas conforme aux bonnes pratiques de sécurité	Important	Corrigé
4	L'application est vulnérable aux attaques automatisées	Important	Corrigé
5	L'application divulgue des informations techniques dans ses messages d'erreurs	Important	Corrigé
6	La protection CAPTCHA n'est pas fonctionnelle	Important	Corrigé
7	Une interface d'administration est accessible depuis internet	Important	Corrigé
8	L'application est vulnérable aux attaques Cross Site Scripting réfléchies	Important	Corrigé
9	Le système de gestion de base de données n'est pas à jour	Mineur	Non corrigé

Autour de moi

- Synthèse de l'analyse de risques liés à la sécurité SI :



Risques consolidés	V	I	C
R01 - Perte de confidentialité des données	4 → **1**	**1**	C1
R02 – Modification non souhaitée des données	4 → **1**	**2**	C1
R03 – « Piratage » du site web	4 → **1**	**3**	C2
R04 – Indisponibilité du site web	3 → **1**	**2**	C1
R05 – Défaut de traçabilité	**1**	**2**	C1

Autour de moi

Décision d'homologation

- ❑ HOMOLOGATION
- ❑ HOMOLOGATION SOUS RESERVE
- ❑ REFUS D'HOMOLOGATION

Commentaires

- XXX
- XXX