



HAL
open science

L'homologation de sécurité RGS comme stratégie SécNum

Jacques Hertzberg

► **To cite this version:**

Jacques Hertzberg. L'homologation de sécurité RGS comme stratégie SécNum : À l'université de Pau et des Pays de l'Adour, la culture de l'évaluation du risque se développe à tous les niveaux de l'établissement. Collection numérique de l'AMUE, Agence de mutualisation des universités et établissements d'enseignement supérieur, 2024, 31, pp.78. hal-04505194

HAL Id: hal-04505194

<https://hal.science/hal-04505194>

Submitted on 14 Mar 2024

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.



Distributed under a Creative Commons Attribution - ShareAlike 4.0 International License

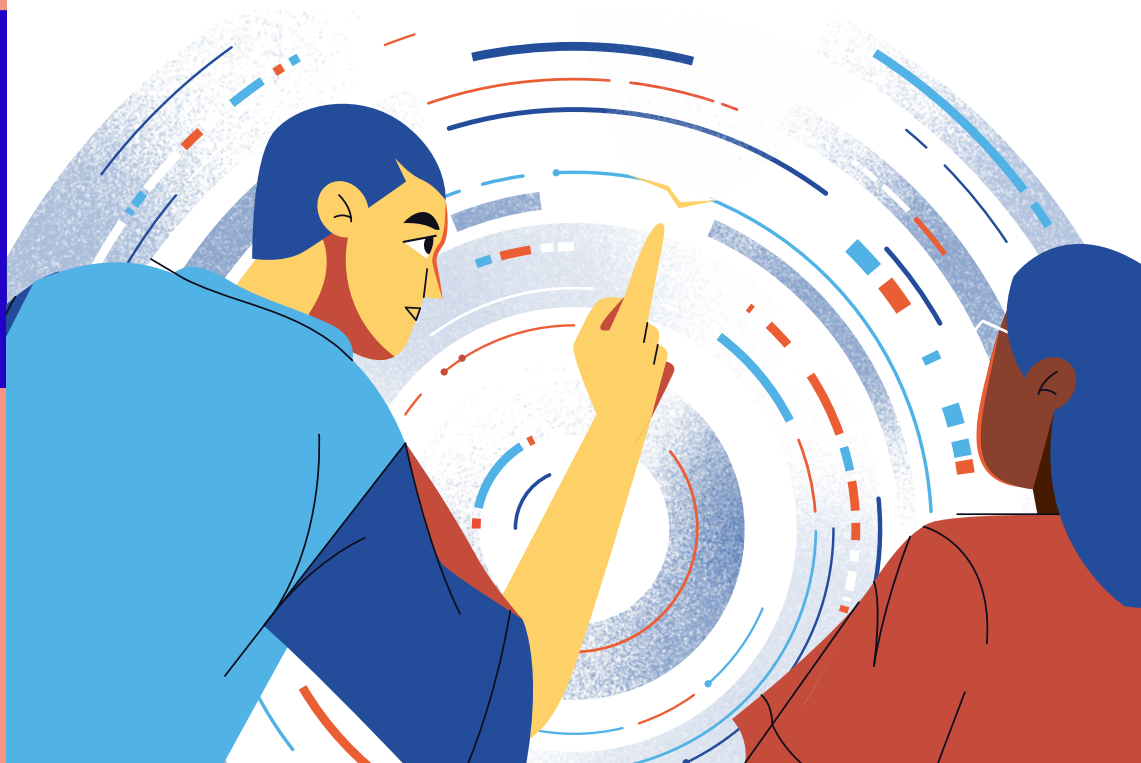
la collection numérique

de l'Agence de mutualisation
des universités et établissements
d'enseignement supérieur ou
de recherche et de support
à l'enseignement supérieur
ou à la recherche



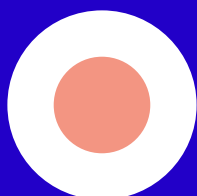
février
2024

Sécurité des SI : saison 2 La cybersécurité au cœur de la stratégie de l'ESRI

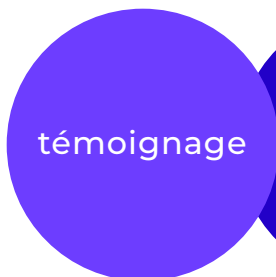


amue 

MUTUALISATION + SOLUTIONS



#31



auteur

Jacques Hertzberg,
RMSI, Université de Pau
et des Pays de l'Adour

L'homologation de sécurité RGS comme stratégie SécNum



**A l'université de Pau
et des Pays de l'Adour,
la culture de l'évaluation
du risque se développe
à tous les niveaux
de l'établissement**



La gouvernance Cyber, l'implication des acteurs du Numérique et l'acculturation des métiers sont ainsi les ingrédients indispensables pour la réduction des risques :

- la gouvernance exprime sa stratégie et impulse le mouvement. Elle soutient les chantiers SécNum intégrés au schéma directeur du Numérique ;
- les acteurs du Numérique font les choix technologiques adaptés, augmentent leurs compétences en se confrontant aux audits techniques. Ils participent activement à la procédure d'homologation ;
- les métiers prennent conscience des risques Cyber liés à leur activité et expriment les besoins de sécurité. Ils donnent à l'analyse de risque toute sa dimension protectrice.

Cette présentation fait le point sur l'organisation et les outils de la SécNum à l'Université de Pau et des Pays de l'Adour.





Organisation de la sécurité du numérique (SécNum) à l'Université de Pau et des Pays de l'Adour

PLAN

COPIL SécNum : objectifs stratégiques

Participation active de l'équipe de direction au COPIL. Cette implication permet d'assurer l'alignement stratégique de la SécNum sur la politique de l'établissement et le sponsoring de l'équipe de direction

COMOP SécNum : objectifs opérationnels

Participation active de la DN : directeur, urbaniste, responsable Cyber et responsables de services

Le COMOP assure le suivi des plans d'actions et alimente les sujets qui seront arbitrés en COPIL. Un des objectifs opérationnels, parmi les plus importants, est l'homologation de sécurité du SI.

Le volet pilotage et le système de management de la sécurité de l'information (SMSI) sont gérés avec l'application APOS de Fidens. L'amélioration continue est implémentée selon l'ISO 27000.

DO

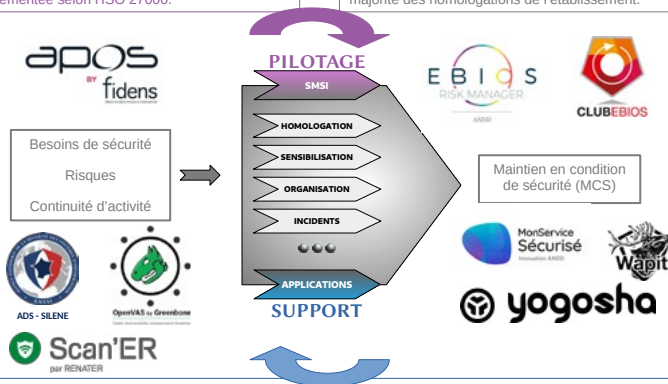
L'homologation de sécurité est un élément important du dispositif. Elle permet l'ISP numérique, depuis la phase de faisabilité jusqu'à la phase de recette.

Participation active des métiers et de la DN pour compléter le bilan d'impact sur l'activité (BIA) du projet ou de l'application.

Afin de s'adapter aux besoins de sécurité et de continuité d'activité, 3 niveaux d'homologation sont identifiés et outillés spécifiquement (adaptation du guide ANSSI) :

- niveau courant
Outils : MonServiceSécurisé
- niveau intermédiaire
Outils : MonServiceSécurisé + YOGOSHA
- niveau haut
Outils : EBIOS/PASSI + YOGOSHA

L'application MonServiceSécurisé permet de gérer la majorité des homologations de l'établissement.



ACT

Nos plans d'action SécNum sont de trois types pour répondre à la réalité du terrain :

- programmatische (COMOP) : pour prendre en compte les objectifs opérationnels sous forme de projets intégrés au schéma directeur du Numérique
- riposte (COMOP + DGS/AH) : pour prendre en compte les situations conjoncturelles qui durent, par exemple les attaques sur les comptes informatiques ou les menaces persistantes
- crise (COMOP + DGS/AH + Président/AQSSI) : pour traiter les situations d'urgence

Cette étape du processus d'amélioration continue vise à agir sur le Numérique au travers des plans d'actions et à proposer les évolutions SécNum à la direction :

- corriger les objets numériques concernés
- adapter les plans d'action au contexte
- identifier les sujets du COPIL SécNum

CHECK

Conformément à la méthode EBIOS, les strates Infrastructures, physiques et logiques, et Applications doivent prendre en compte les mesures de la PSSI.

La vérification de la conformité à la PSSI s'appuie, pour la partie technique, sur plusieurs scanners automatiques :

- Infrastructures**
 - ADS/ANSI
 - Scan'ER/Renater
 - SILENE/ANSI
- Développement d'applications**
 - Wapiti/dev100p

Selon le niveau d'homologation, une phase d'audit technique avancé peut être réalisée sous forme de pentest ou de bug bounty. La plateforme utilisée est YOGOSHA (prestation). Outre son niveau d'expertise, elle permet la montée en compétence des équipes numériques par les échanges avec les hackers.

Organisation de la sécurité du numérique (SécNum) à l'Université de Pau et des Pays de l'Adour

Lexique :

AH : autorité d'homologation
ANSSI : agence nationale de la sécurité des systèmes d'information
APOS : assistance au pilotage par les objectifs de sécurité
AQSSI : autorité qualifiée
COMOP : comité opérationnel
COPIL : comité de pilotage
DGS : directeur général des services
DN : direction du Numérique
EBIOS : Expression des besoins et identification des objectifs de sécurité
ISP : intégration de la SécNum dans les projets
PASSI : prestataire d'audit de sécurité des systèmes d'information
RGS : référentiel général de sécurité
SécNum : sécurité du Numérique
Yogosha : défenseur (japonais)

Stratégie d'homologation et développement de la culture de la gestion des risques : Mon Service Sécurisé, la solution proposée par l'ANSSI pour faciliter le travail d'homologation

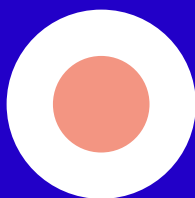
MonServiceSécurisé aide les entités publiques à sécuriser et homologuer rapidement leurs services publics numériques (site web, applications mobiles, API). Il est développé par l'ANSSI, en lien avec BetaGouv et la Direction interministérielle du numérique. Au-delà du service de conformité qu'il rend, ce service -gratuit- permet de faire collaborer toutes les parties prenantes (RSSI, DPO, DSI, directions métiers, chefs de projet, direction, etc.) et développe ainsi la culture de la gestion des risques cyber auprès des personnels participant à l'implémentation des SI.

En savoir plus : [MonServiceSécurisé \(ssi.gouv.fr\)](https://ssi.gouv.fr)

février
2024



+



amue.fr

prochain numéro

Le numéro d'avril 2024
sera consacré aux stratégies
du numérique
universitaire.

À suivre dans
les prochains
numéros: formes de
mutualisation dans
d'autres pays, Usages
saison 6



Ces sujets vous
intéressent, vous
avez une expérience,
un point de vue à
partager, vous avez une
proposition de thème
pour un prochain
numéro: contactez
l'équipe numérique
de l'Amue qui est
à votre écoute:
numerique@amue.fr

2 rue Albert Einstein + 75013 Paris
Nos réseaux sociaux: @Amue_com

