MINISTÈRE
DE L'ÉDUCATION
NATIONALE
ET DE LA JEUNESSE

Liberté
Égalité
Fraternité

Guide « téléservices »

Document d'accompagnement du kit sécurité des systèmes d'information pour les espaces numériques de travail

ENT

Espace numérique de travail

Document d'accompagnement
version 1.0
Juin 2022

Direction du numérique pour l'éducation – bureau SN1

Table des matières

1. Introduction

1.1. Avant-propos

Dans le cadre du déploiement et de la mise en œuvre des espaces numériques de travail dans le 1er et 2ème degré de l'enseignement scolaire, le ministère de l'Éducation nationale a élaboré un schéma directeur des espaces numériques de travail (SDET) dont l'objectif est de fournir un cadre de cohérence national pour les projets ENT et d'orienter l'offre de solutions ENT.

Le SDET pose « les principes directeurs de l'élaboration et de la mise en œuvre d'une solution ENT en partenariat avec les collectivités territoriales qui les financent et les académies qui assurent l'accompagnement des utilisateurs ».

Dans cette volonté d'accompagner les partenaires et acteurs, l'Éducation nationale propose un ensemble de guides thématiques portant sur la sécurité des espaces numériques de travail à destination des différents acteurs conçu comme un cadre de référence commun.

Ce kit SSI est proposé dans un contexte de sécurisation nécessaire et pour répondre tout à la fois aux exigences sociales des usagers et à la réglementation en termes de protection des données ou de continuité pédagogique.

1.2. Présentation du KIT SSI pour les ENT

Le Kit SSI pour les ENT est un ensemble de guides pratiques qui recouvrent les domaines suivants :

- La gouvernance de la sécurité des systèmes d'information
- La sous-traitance
- La mise en œuvre des téléservices
- La gestion des incidents

Il a pour objectifs :

- D'outiller les porteurs de projets ENT dans la mise en œuvre de la politique de sécurité tout au long du cycle de vie des ENT. En particulier, les guides prescrivent un ensemble de recommandations pour répondre à la réglementation et aux principes de la gestion de risque, aussi bien en phase de déploiement, d'utilisation ou d'évolution de l'ENT ;
- De fournir un cadre commun de références aux acteurs, partenaires et sous-traitants en rappelant en particulier les règles auxquelles se conforme l'Éducation nationale ;
- De répondre de façon simple et non ambiguë aux différentes situations et problèmes qui peuvent se poser aux responsables et acteurs des ENT.

Dans la continuité des guides proposés par l'ANSSI, en particulier le guide à destination de collectivités territoriales, ce kit SSI vise de façon plus générale à :

- Donner confiance aux usagers dans l'utilisation des services numériques ;
- Garantir la sécurité des données à caractère personnel conformément à la réglementation ;
- Appuyer la transformation numérique des administrations de l'État ;
- Renforcer la sécurité des acteurs critiques pour l'État.

1.3. Présentation du guide « Téléservices »

Note importante : le terme téléservice présente plusieurs acceptions. Dans ce document, l'acception utilisée sera celle de l'article 1 II-a de l'ordonnance n° 2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives qui définit un téléservice comme : « (..) *tout système d'information permettant aux usagers de procéder par voie électronique à des démarches ou formalités administratives.* »

Le présent guide traite de l'homologation des téléservices utilisés au sein des espaces numériques de travail. Dans le cadre de ENT, les services mis à disposition des parents d'élèves ou des responsables légaux pour échanger avec l'administration ou le corps enseignant doivent être considérés comme des téléservices dans la mesure ils permettent à des usagers « *de procéder par voie électronique à des démarches ou formalités administratives* ».

Ce guide propose des recommandations pratiques pour :

- Homologuer les téléservices conformément aux prescriptions légales citées dans le référentiel général de sécurité (RGS) ;
- Articuler la réalisation d'une homologation RGS avec une analyse d'impact pour la protection des données ;

- Définir les responsabilités des différents acteurs.

2. Objectifs détaillés

2.1. Objectifs détaillés du guide

Les objectifs sont détaillés ci-après avec un n° d'occurrence qui ne présume ni de l'importance ni de l'ordonnancement de l'objectif.

Objectif n°1 : Définir les rôles et responsabilités dans le processus d'homologation entre les parties prenantes, en l'occurrence entre les deux autorités administratives impliquées pour la mise en œuvre d'un téléservice ;

Objectif n°2 : Proposer une articulation simple entre homologation RGS et AIPD ;

Objectif n°3 : Définir le cadre de l'homologation pour les ENT

3. Contexte

3.1. Périmètre

Les espaces numériques de travail offrent à chaque membre de la communauté éducative un accès simple, dédié et sécurisé aux outils et contenus dont il a besoin. Les utilisateurs bénéficient à travers un service web, d'un accès authentifié et de services spécifiques selon leur profil.

Dans la mesure où l'ENT offre des services aux parents d'élèves au sens de l'article 1 de l'ordonnance n° 2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives :

- Les parents d'élèves doivent être considérés comme des usagers qui échangent par voie électronique avec une autorité administrative ;
- Et les services qui leur sont offerts comme des téléservices ;

Ces téléservices doivent donc être homologués conformément aux prescriptions du référentiel général de sécurité.

Dans la mesure où l'ENT offre un bouquet de services dont une partie est destinée aux parents d'élèves, l'ENT peut être considéré dans son ensemble comme un téléservice. Il est donc recommandé avant sa mise en service de réaliser une homologation globale plutôt qu'une homologation par service mis à disposition de parents d'élèves ou responsables légaux.

3.2. Les acteurs de l'homologation

L'autorité administrative : sont considérés comme autorités administratives au sens de l'article 1 de l'ordonnance du 8 décembre « les administrations de l'État, les collectivités territoriales, les établissements publics à caractère administratif, les organismes gérant des régimes de protection sociale relevant du code de la sécurité sociale et du code rural ou mentionnés aux articles L. 223-16 et L. 351-21 du code du travail et les autres organismes chargés de la gestion d'un service public administratif ainsi que les commissions de coordination des actions de prévention des expulsions locatives prévues à l'article 7-2 de la loi n° 90-449 du 31 mai 1990 visant à la mise en œuvre du droit au logement. »

Il appartient à l'autorité administrative de protéger les téléservices qu'elle met à disposition de ses usagers et d'attester formellement auprès de ceux-ci qu'elle l'a fait conformément aux prescriptions du RGS.

Dans le cadre de l'ENT, les collectivités territoriales et les autorités académiques sont les autorités administratives.

L'autorité d'homologation : est la personne physique qui, après instruction du dossier d'homologation, prononce l'homologation de sécurité du système d'information, c'est-à-dire prend la décision d'accepter les risques résiduels identifiés sur le système. (Source : guide d'homologation en 9 étapes).

Elle est désignée par l'autorité administrative par arrêté ou délibération à un niveau hiérarchique suffisant. Aux termes du décret n° 2022-513 du 8 avril 2022[1,2] et pour ce qui relève de l'autorité académique en tant qu'administration déconcentré :

> *Chaque ministre désigne (..), une ou plusieurs autorités qualifiées en sécurité des systèmes d'information compétentes pour les systèmes d'information et de communication autres que ceux qui sont classifiés Dans le cadre de l'ENT, l'autorité d'homologation peut être unique ou multiple.*
>
> *L'autorité qualifiée en sécurité des systèmes d'information (..) définit la politique de sécurité numérique (..) et contrôle son application au travers notamment de l'homologation de ces systèmes d'information (..). Elle peut déléguer cette fonction d'homologation à des autorités d'homologation qu'elle désigne.*

Dans le cas d'une autorité d'homologation unique, une autorité administrative mènera l'homologation et attestera formellement de la sécurité de l'ENT auprès des usagers.

La maîtrise d'ouvrage représente les acteurs métier et assure la bonne prise en compte des contraintes liées à l'utilisation du système d'information. Elle joue un rôle-clé dans plusieurs étapes de la maîtrise des risques, y compris dans les arbitrages sur le traitement des risques (source : guide d'homologation en 9 étapes).

Dans le cadre de l'ENT, la maitrise d'ouvrage sera représentée :

- Pour l'autorité académique, par le DAN/DSI ou l'IA-DASEN ou tout autre représentant désigné par le recteur en sa qualité d'AQSSI,
- Pour les collectivités territoriales, par la direction générale de service, la direction de l'éducation, des lycées ou des collèges ou des représentants désignés par celles-ci.

Le RSSI. *Lorsque l'entité dispose d'un responsable de la sécurité des systèmes d'information, celui-ci est impliqué dans la démarche d'homologation. Selon les cas, il peut être désigné responsable du processus d'homologation, chargé du secrétariat de la commission d'homologation ou être membre de droit de cette commission. (Source : guide d'homologation en 9 étapes).*

[1] Décret n° 2022-513 du 8 avril 2022 modifiant le décret n° 2019-1088 du 25 octobre 2019 relatif au système d'information et de communication de l'Etat et à la direction interministérielle du numérique

[2] Le décret entre en vigueur le 1er octobre 2022

Le responsable d'exploitation du système ou autorité d'emploi, *remplit le rôle opérationnel. Il s'agit de l'entité exploitant le système d'information destiné à être homologué*. (Source : *guide d'homologation en 9 étapes*).

Il pourra s'agir d'une collectivité territoriale, d'une autorité académique ou d'un prestataire choisi par une des parties de la convention de partenariat.

Le prestataire ou sous-traitant de l'ENT. Conformément à l'article 28 3.f du RGPD, le sous-traitant *« aide le responsable du traitement à garantir le respect des obligations prévues aux articles 32 à 36, compte tenu de la nature du traitement et des informations à la disposition du sous-traitant »*.

Il est donc fait obligation au sous-traitant d'assister son client dans la réalisation de l'analyse d'impact (article 35 du RGDP) et lui fournir toute l'information nécessaire. Cette assistance et les informations communiquées dans cadre sont utilisables pour l'homologation RGS.

4. Rôle de chaque acteur et actions attendues

4.1. Autorité administrative

Il peut s'agir d'une collectivité territoriale ou d'une autorité académique.

Action(s) à mener	Responsabilité(s)
Désigner l'autorité d'homologation	Obligation réglementaire. RGS V2.0 porté par arrêté du Premier ministre du 13 juin 2014. Ancienne ig 1300 art.90, nouvelle instruction à venir. Décret n° 2022-513 du 8 avril 2022[3]
Veiller au respect de la conformité RGS	Obligation réglementaire. Ordonnance du 8 décembre 2005
Signer l'attestation formelle	Obligation réglementaire. Décret 2010-112 article 5
Prévoir dans le marché la réalisation de l'homologation et de l'AIPD.	Note : il ne s'agit pas ici de prévoir que le prestataire réalise lui-même l'homologation ou l'AIPD mais qu'il aide le responsable de traitement dans la réalisation de ces dernières.

Tableau 1 : Actions attendues de l'autorité administrative

4.2. Autorité d'homologation

Il peut s'agir d'une collectivité territoriale ou d'une autorité académique.

Action(s) à mener	Responsabilité(s)
Prononcer l'attestation formelle	Obligation réglementaire. RGS V2.0 porté par arrêté du Premier ministre du 13 juin 2014.
Désigner le responsable de l'homologation	Recommandation guide ANSSI.

[3] Le décret entre en vigueur le 1er octobre 2022

Action(s) à mener	Responsabilité(s)
Réunir la commission d'homologation	Obligation réglementaire.

Tableau 2 : Actions attendues de l'autorité d'homologation

4.3. Commission d'homologation

Il peut s'agir d'une collectivité territoriale ou d'une autorité académique.

Action(s) à mener	Responsabilité(s)
Assister l'autorité d'homologation	Recommandation guide d'homologation ANSSI.
Préparer la décision d'homologation	Recommandation guide d'homologation ANSSI.

Tableau 3 : Actions attendues de la commission d'homologation

4.4. Responsable de l'homologation

Il peut s'agir du RSSI ou de toute autre personne désignée par l'autorité d'homologation.

Action(s) à mener	Responsabilité(s)
Piloter ou réaliser l'homologation	Recommandation guide d'homologation ANSSI.

Tableau 4 : Actions attendues du responsable d'homologation

4.5. RSSI de l'académie

Action(s) à mener	Responsabilité(s)
Être le responsable de l'homologation	Recommandation guide d'homologation ANSSI.
Assurer le secrétariat de la commission d'homologation	Recommandation guide d'homologation ANSSI.

Tableau 5 : Actions attendues du RSSI

4.6. Sous-traitant

Action(s) à mener	Responsabilité(s)
Assister le responsable de l'homologation	Obligations légales (induite par RGPD art 28 3.f)

Tableau 6 : Actions attendues du sous-traitant

Note : le sous-traitant à l'obligation d'assister son client dans la réalisation de l'AIPD. Nombre des actions et informations qu'il doit fournir à son client sont identiques à celles qu'ils devraient fournir pour une homologation.

5. Recommandations aux acteurs dans le cadre d'un projet ENT

5.1. Principes

Les espaces numériques de travail manipulent des données à caractère personnel et entrent donc dans le champ du RGPD et de la loi informatique et libertés. La mise en œuvre d'un ENT nécessite d'apprécier les risques et de déterminer des mesures de sécurité proportionnées afin de réduire ces risques et les ramener à un niveau jugé acceptable.

Ces objectifs sont communs aussi bien à l'analyse d'impact sur la protection des données qu'au référentiel général de sécurité.

5.1.1. Référentiel général de sécurité et ENT

« Le référentiel général de sécurité prévu par l'article 9 de l'ordonnance du 8 décembre 2005 susvisée fixe les règles auxquelles les systèmes d'information mis en place par les autorités administratives doivent se conformer pour assurer la sécurité des informations échangées, et notamment leur confidentialité et leur intégrité, ainsi que la disponibilité et l'intégrité de ces systèmes et l'identification de leurs utilisateurs. » Art. 1 du décret 2010-112

L'espace numérique de travail étant ouvert aux parents d'élèves ou responsables légaux, il constitue un téléservice au sens de l'ordonnance du 8 décembre 2005 dans la mesure ou les parents ou responsables légaux doivent être considérés comme des usagers.

Le RGS prescrit les règles auxquelles doit se conformer le système d'information mis en œuvre par les autorités administratives pour échanger avec leurs usagers ou avec d'autres autorités administratives. Ces règles constituent la garantie apportée par l'autorité administrative aux citoyens et aux autres administrations quant au niveau de sécurité du système d' information.

Le RGS v2.0 prévoit en particulier de réaliser une démarche d'homologation qui réside dans la réalisation d'une étude de risque et d'un audit.

5.1.2. Analyse d'impact sur la protection des données

L'analyse d'impacts sur la protection des données est « une étude qui doit être menée lorsqu'un traitement de données personnelles est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes concernées. » (Source CNIL).

En pratique l'analyse consiste à :

1. Déterminer le contexte du système d'information en décrivant les enjeux, les traitements, et le périmètre détaillé des données, acteurs et systèmes d'informatique et de communication ;
2. Étudier Les principes fondamentaux
3. Étudier les risques liés à la protection des données
4. Valider l'analyse d'impact

5.1.3. Articulation entre homologation et analyse d'impact relative à la protection des données

L'homologation RGS implique de réaliser une étude de risque qui déterminera les risques, les mesures pour le traiter et aboutir à un niveau de risque résiduel acceptable du point de vue de l'institution. L'analyse d'impact relative à la protection (AIPD) consiste à réaliser une étude de risque spécifiquement pour évaluer les risques que l'organisme fait courir aux personnes concernées par le système d'information qui manipule leurs données personnelles.

Il est tout à fait envisageable de mener une étude de risque qui traite l'ensemble des risques du point de vue institutionnel et du point de vue utilisateur et optimiser le temps de réalisation de l'homologation et de l'AIPD. Dans ce cas, l'étude de risque RGS pourra alimenter les parties 1 et 3 de l'AIPD.

Dans le cadre des espaces numérique de travail, compte-tenu de la nature des traitements et de la potentielle multiplicité des acteurs, il est recommandé de mener une étude de risque qui alimentera le dossier d'homologation et l'AIPD qui constituera d'ailleurs un élément du dossier.

5.2. Recommandations

R1

Désigner l'autorité d'homologation [4]

L'ANSSI préconise que l'autorité d'homologation soit unique mais il reste possible de désigner une autorité d'homologation multiple. Dans le cadre d'un partenariat pour la mise œuvre d'un ENT, l'autorité d'homologation sera multiple, sauf accord entre les parties.

La désignation de l'autorité d'homologation doit faire l'accord des parties prenantes de la convention de partenariat et être mentionnée dans la stratégie d'homologation.

Cas d'une autorité unique

Dans le cas d'une autorité d'homologation unique (exemple d'une collectivité territoriale qui homologue un ENT pour l'académie et d'autres collectivités) cette dernière désignera en son sein un responsable de l'homologation qui communiquera aux autres entités les éléments du dossier d'homologation. L'attestation formelle ou homologation sera signée par l'autorité administrative dont relève l'autorité d'homologation unique.

Cas d'une autorité multiple

Dans le cas d'une autorité d'homologation multiple, une des entités sera désigné comme autorité déléguée pour mener à bien l'homologation. Cette autorité déléguée désignera un responsable qui communiquera en direction des autres entités sur les étapes clés de l'homologation et fournira le dossier d'homologation sur lequel elles seront amenées à se prononcer.

Dans ce cas, l'attestation formelle ou homologation sera signée par l'ensemble des parties prenantes de la convention de partenariat.

[4] Pour l'autorité académique, se référer au décret n° 2022-513 du 8 avril 2022, pour les collectivités territoriales se référer aux guides ANSSI.

Les collectivités territoriales peuvent avoir désigné une autorité et une commission d'homologation par délibération. Dans ce cas, le choix d'une collectivité territoriale comme autorité unique désigne l'autorité actée par la délibération.

Dans le cas d'une autorité d'homologation multiple, l'homologation est réalisée de facto par une des entités partenaires. Il appartient à l'autorité d'homologation de chacune des entités partenaires de signer l'homologation. Pour les académies, l'autorité d'homologation pourra être le DAN/DSI ou l'IA-DASEN.

R2

Constituer la commission d'homologation

La commission d'homologation d'un ENT est classiquement composée par :

- La maitrise d'ouvrage qui peut être une direction des lycées ou collèges, l'IA-DASEN ou le DANE. Dans le cas d'une autorité d'homologation multiple, il est conseillé d'associer les représentants des différents partenaires de la convention ;
- La maitrise d'œuvre représentée par une DSI d'une collectivité territoriale ou une DSI académique ;
- Le responsable de l'homologation qui peut être le RSSI ;
- Les RSSI ;
- Le ou les sous-traitant ;

Cas d'une autorité d'homologation unique : la commission d'homologation est celle constituée par l'autorité d'homologation unique désignée par les différents partenaires.

Cas d'une autorité d'homologation multiple : elle est placée auprès de l'autorité d'homologation chargée de mener à bien l'homologation. Toutefois, la commission d'homologation peut avoir des représentants des différentes entités.

Si l'autorité d'homologation peut avoir été désignée par arrêté ou délibération, la constitution de la commission d'homologation chargée de l'assister est adaptable. Le guide d'homologation de l'ANSSI précise que

> « *La taille et la composition de cette commission doivent être adaptées à la nature du système et proportionnées à ses enjeux* »

Dans le cas d'une autorité d'homologation multiple, il est recommandé que les directions métiers participent à la commission d'homologation à minima en tant que membres invités.

R3

Définir la stratégie d'homologation

Il appartient à l'autorité d'homologation unique ou déléguée de définir la stratégie d'homologation de l'ENT. Cette stratégie décrit l'organisation et les modalités pratiques de l'homologation.

Conformément au guide ANSSI, elle décrit :

- Le cadre réglementaire applicable ;
- L'organisation (acteurs, missions, etc.) ;
- La démarche ;
- Le périmètre ;
- Le calendrier ;
- La criticité des données utilisées.
- Les pièces constitutives du dossier d'homologation

Le document de stratégie d'homologation ne diffère pas selon que l'homologation est réalisée avant ou après la mise en œuvre.

Toutefois, dans le cas d'une homologation intervenant après la mise en service de l'ENT, il sera possible d'utiliser les résultats de l'AIPD confortés par l'identification et l'analyse des scénarios de haut niveau (atelier 2 et 3 d'Ebios RM) ;

R4

Signer l'attestation formelle

L'homologation est l'attestation formelle de l'autorité administrative que l'ENT est protégé conformément aux prescriptions du RGS.

Dans le cas d'une homologation unique de l'ENT, cette attestation est signée uniquement par l'autorité administrative dont relève l'autorité d'homologation. Cette signature n'emporte pas la responsabilité exclusive de l'autorité administrative signataire.

En particulier, les responsabilités fixées par la convention « *relative à la sécurisation juridique du traitement de données à caractère personnel portant sur le déploiement entre collectivités territoriales et autorités académiques* » demeurent.

Dans le cas d'une homologation multiple, l'homologation sera signée par l'ensemble des partenaires. Dans ce cas, il est préférable que les autorités administratives sollicitent leur propre autorité d'homologation.

R5

Définir le contenu du dossier d'homologation

Le dossier d'homologation contiendra à minima :

- La convention juridique liant les partenaires ;
- La stratégie d'homologation ;
- Le plan d'assurance sécurité ou la politique de sécurité du prestataire de l'ENT ;
- Le rapport d'étude de risque ;
- Le ou les rapports d'audits ;
- La synthèse des risques résiduels ;
- Le document d'architecture technique ;
- Le document d'exploitation

Il pourra également contenir :

- L'analyse impact ;
- Les décisions d'homologations antérieures.

Dans le cas d'une autorité d'homologation multiple, l'autorité en charge de l'homologation communiquera dans la stratégie d'homologation le contenu envisagé aux entités partenaires.

R6

Réaliser l'homologation avant le déploiement

Il est recommandé de réaliser l'homologation de sécurité avant le déploiement de l'espace numérique de travail.

L'homologation de sécurité consistera (cf. chapitre 1 du RGS v2.0) à :

- Mener une étude de risque. Dans le cadre de l'ENT, celle-ci sera menée concomitamment avec l'analyse d'impact pour la protection des données ;
  (Étapes 1, 2 et 3 de la démarche d'homologation avant mise en œuvre)
- Réaliser un audit technique[5] ;
- Rédiger une synthèse de la couverture des risques et du risque résiduel pour que l'autorité d'homologation puisse homologuer le système (étape 4 de la démarche).

L'homologation prend l'ensemble de l'espace numérique de travail comme périmètre de l'homologation. De ce fait, les politiques de sécurité ou des

[5] Même si l'audit technique n'est pas explicitement prévu dans la démarche d'homologation avant mise en œuvre du système d'information, il est indispensable pour vérifier l'effectivité et l'efficience de mesures de sécurité et apprécier le risque résiduel, préalable à la décision d'homologation.

homologations de composants de l'ENT fournis par les entités partenaires constituent des entrées de l'homologation de sécurité.

L'homologation peut être menée par des ressources propres à l'autorité administrative qui a la charge de l'homologation ou un prestataire. Dans ce cas, le prestataire réalisant l'étude de risque où l'audit sera choisi de préférence parmi un prestataire d'audit qualifié RGS (PASSI RGS).

La conduite de l'étude de risque nécessite l'implication forte du prestataire de l'ENT, en particulier en amont pour déterminer le périmètre technique et le socle de sécurité ainsi que la définition de scénarios opérationnels de risque et le traitement des risques.

L'article 28 3.f du RGPD implique que le prestataire de l'ENT quand il s'agit d'un sous-traitant aide son client dans la réalisation de l'AIPD, cette assistance devant être prévue dans le contrat. Il pourra être sollicité sur cette base lorsque l'homologation et l'AIPD sont menées de concert.

R8

Réaliser l'homologation après le déploiement

Dans le cas où l'espace numérique de travail est en exploitation sans homologation, il est possible de réaliser l'homologation ultérieurement à sa mise en œuvre.

Dans ce cas, la démarche mis en œuvre sera celle proposée dans le RGS v2.0 (homologation après mis en œuvre) et consistera à :

- Réaliser un audit technique ;
- Réaliser une étude adaptée ;

Dans le cas où la démarche d'homologation met en évidence des risques qui ne peuvent pas être acceptés en regard de l'appréciation des risques, l'autorité d'homologation :

- Délivrera une autorisation préalable d'emploi pour un délai n'excédant pas une année | 6 mois ;
- Assorti de mesures conservatoires, d'un plan d'action et d'une clause de revoyure.

L'étude de risque adaptée consistera soit à réaliser :

- Identifier et analyser les scénarios de haut niveau, intégrant l'écosystème (atelier 2 et 3 d'Ebios RM) ;

- Réaliser une étude préliminaire de risque pour identifier les axes prioritaires d'amélioration de la sécurité (atelier 1 adapté, 2, 3 et 4b d'Ebios RM).

Les conditions d'application des recommandations 1 à 5 sont inchangés.

R9

Articuler l'homologation avec l'AIPD

L'analyse d'impact pour la protection des données est une obligation dans le cadre de la mise en œuvre des ENT.

L'étude du contexte, l'appréciation des risques, le traitement des risques sont des principes directeurs commun aux analyses d'impact et aux études de risques. Il est donc conseillé d'articuler l'étude de risque et l'AIPD pour éviter de mener deux études.

De façon générale, l'étude de risque devra être menée avant ou concomitamment à l'AIPD :

- Menée avant, elle alimentera les étapes 1 et 3, et servira de support pour l'étape 4 de l'AIPD.
- Menée concomitamment, l'étude et l'AIPD pourront être fusionnés dans un document unique.

Il est possible de fusionner les deux documents en distinguant les risques institutionnels d'une part et les risques que les parties prenantes font courir à la communauté éducative en termes d'atteinte à leurs données personnelles.

Ce choix devra être mentionné dans la stratégie d'homologation et dans le document d'étude de risque et d'analyse d'impact.

R10

Assurer le suivi de l'homologation

La démarche d'homologation s'inscrit dans un processus d'amélioration continue de la sécurité.

Le RGS prescrit que « *les mesures de protection d'un système d'information doivent être accompagnées d'un suivi opérationnel quotidien ainsi que de mesures de surveillance et de détection, afin de réagir au plus vite aux incidents de sécurité et de les traiter au mieux* »

Ce suivi opérationnel, pris en charge par l'autorité d'emploi ou son prestataire, doit à minima recenser :

- Les incidents ;
- Les vulnérabilités ayant affectés l'ENT ou ses composants ;
- Les mesures correctives ou préventives.

Ces éléments seront communiqués à l'autorité d'homologation qui devra réunir la commission d'homologation une fois par an, « *afin de juger de l'opportunité d'un renouvellement plus approfondi de l'homologation* »

Le renouvellement de l'homologation sera obligatoire, dans les cas suivants :

- D'incident grave sur l'ENT ayant entraîné une altération ou une divulgation significative de données à caractère personnel, une compromission significative de comptes ou une indisponibilité supérieure à une semaine ;
- Mise en œuvre de nouveau(x) services(s) susceptibles d'avoir un impact significatif sur l'appréciation des risques (voir règle 12) ;
- Arrivée à terme de la convention de partenariat ou de la durée de l'homologation.

Évaluer l'impact d'une modification sur l'ENT

Les évolutions sur l'espace numérique de travail qu'il s'agisse d'évolutions organisationnelles, d'ajout de services en direction d'utilisateurs, de modifications de composants de base doit faire l'objet d'une appréciation des impacts.

En cas de modification substantielle touchant au périmètre ou aux modalités de traitement, la commission d'homologation doit être réunie pour envisager un avenant à l'homologation existante ou une ré-homologation.

Fixer la durée de l'homologation

La durée d'une homologation recommandée par le RGS se situe entre trois et cinq ans. Les conventions de partenariat ont une durée sensiblement de même ordre.

La durée de l'homologation sera calée sur celle du partenariat.

6. Référentiels applicables

Nom	Objet	Ressources/Liens
Ordonnance n° 2005-1516 du 8 décembre 2005	Ordonnance relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives.	https://www.legifrance.gouv.fr/loda/id/JORFTEXT000000636232/
Décret 2010-122 dit décret RGS	Décret d'application	https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000022318092
RGS V2.0	Référentiel général de sécurité	https://www.ssi.gouv.fr/uploads/2014/11/RGS_v-2-0_Corps_du_texte.pdf
Décret n° 2022-513 du 8 avril 2022	Sécurité numérique du système d'information et de communication de l'Etat et de ses établissements publics	https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000045537693
Décret n° 2019-1088 du 25 octobre 2019	Système d'information et de communication de l'Etat et à la direction interministérielle du numérique (est modifié au 1er octobre 2022 par le décret sus-cité en particulier sur le rôle de l'AQSSI et la désignation des autorités d'homologation par celui-ci)	https://www.legifrance.gouv.fr/loda/id/JORFTEXT000039281619/
Loi informatique et libertés	Loi	Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés
Décret d'application de la loi informatique et libertés	Décret d'application	Décret n° 2005-1309 du 20 octobre 2005 pris pour l'application de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés

Nom	Objet	Ressources/Liens
RGPD	Règlement européen	Règlement européen 2016/679 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE
Gestionnaire d'accès aux ressources	Arrêté	https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000043914692
Gestionnaire d'accès aux ressources	FAQ	https://gar.education.fr/etablissements-et-ecoles/faq-traitement-des-donnees-personnelles/
EBIOS RM	Méthode de gestion de risque EBIOS Risk Manager	https://www.ssi.gouv.fr/entreprise/management-du-risque/la-methode-ebios-risk-manager/
Guide d'homologation en 9 étapes	Guide d'homologation RGS de l'ANSI	https://www.ssi.gouv.fr/guide/lhomologation-de-securite-en-neuf-etapes-simples/