



Direction des systèmes d'information

MAINTENANCE DU LOGICIEL DE E-LEARNING SUR LA PREVENTION DES RISQUES

Cahier des Clauses Techniques Particulières (CCTP)

Livret 1/2 du CCTP n° DSI 23-002c

Accord cadre n° DSI 23-002

*Procédure adaptée
du Code de la commande publique
(Articles -L2123-1-1° et R2123-1 à R2123-5)*

Objet : Ce document décrit les exigences fonctionnelles, techniques, d'intégration dans le SI, de sécurité et d'organisation des prestations pour la maintenance du logiciel de E-learning sur la prévention des risques

SOMMAIRE

1	CONTEXTE GENERAL.....	5
1.1	Objet de l'accord-cadre.....	5
1.2	Présentation du CNRS.....	5
1.2.1	La direction générale déléguée à la science (DGD-S).....	5
1.2.2	La direction générale déléguée aux ressources (DGD-R).....	6
1.3	Présentation de l'Inserm.....	9
1.4	<i>Lieu d'exécution de l'accord-cadre</i>	10
1.5	Structure du CCTP et conventions de rédaction.....	10
2	CONTEXTE DU SI AU CNRS ET A L'INSERM.....	11
2.1	Conformités réglementaires.....	11
2.1.1	Politique Générale de Sécurité des systèmes d'Information.....	11
2.1.2	Protection des données à caractère personnel (DCP).....	12
2.1.3	Interopérabilité.....	13
2.1.4	Accessibilité numérique.....	14
2.2	Présentation des infrastructures du SI CNRS.....	15
2.2.1	Sites et utilisateurs du système d'information.....	15
2.2.2	Centres serveurs.....	15
2.2.3	Réseau.....	15
2.2.4	Infrastructures.....	16
2.3	Principes d'urbanisation et d'intégration dans le SI.....	16
2.3.1	Principes généraux :.....	17
2.3.2	Principes d'échanges.....	17
2.3.3	Plateformes transverses et services proposés.....	17
2.3.4	Prise en compte des changements de l'organisation structurelle des établissements CNRS et Inserm.....	19
3	DESCRIPTION DE LA SOLUTION EN PLACE.....	20
3.1	Présentation de la solution.....	20
3.1.1	Présentation fonctionnelle.....	20
3.1.2	Intégration dans le SI.....	31
3.1.3	Présentation technique.....	32
3.2	Volumétrie.....	33
3.2.1	Volumétrie des versions.....	33
3.2.2	Volumétrie des anomalies.....	33
3.2.3	Volumétrie des évolutions.....	33
3.3	Dimensionnement de l'application.....	33
3.4	Evolutions futures identifiées :.....	34
4	CADRE DE COHERENCE TECHNIQUE DE LA SOLUTION.....	35
4.1	Exigences d'intégration dans le SI.....	35
4.1.1	Répartition fonctionnelle.....	35
4.1.2	Echanges de données.....	35
4.1.3	Authentification, comptes utilisateurs.....	38
4.1.4	Stockage des documents.....	40
4.2	Exigences techniques.....	40
4.2.1	Eléments techniques structurants.....	40
4.2.2	Services d'infrastructure.....	40
4.2.3	Architecture applicative.....	42
4.2.4	Base de données.....	49
4.2.5	Engagements de qualité de service pour l'application.....	50
4.3	Exigences d'ergonomie-graphisme.....	50
4.3.1	Charte graphique.....	51

4.3.2	Règles d'ergonomie	51
4.4	Exigences de sécurité.....	52
4.4.1	Auditabilité.....	53
4.4.2	Protection des applications web	54
5	CADRE D'ORGANISATION DES PRESTATIONS.....	56
5.1	Système qualité	56
5.2	Organisation des équipes projet.....	56
5.2.1	Organisation de l'équipe CNRS/Inserm	56
5.2.2	Organisation et gestion des compétences de l'équipe projet du titulaire	57
5.3	Dispositifs de conduite de projet	58
5.3.1	Structures de pilotage projet.....	58
5.3.2	Pratiques de gestion de projet	58
5.3.3	Indicateurs de pilotage et qualité du projet.....	59
5.4	Méthode de développement.....	60
5.4.1	Cycle de vie.....	60
5.4.2	Activités de réalisation (à la charge du Titulaire).....	61
5.4.3	Activités de recette (à la charge du CNRS / Inserm).....	61
5.5	Gestion des environnements	62
5.5.1	Postes de travail du titulaire.....	62
5.5.2	Environnement de développement	62
5.5.3	Environnements CNRS	62
5.6	Gestion des livraisons.....	63
5.7	Gestion de la documentation	63
5.8	Capitalisation des connaissances	65
5.9	Outils de suivi et pilotage du projet.....	65
5.10	Mesures et clauses de sécurité.....	66
5.10.1	Gestion de la Sécurité par le titulaire	66
5.10.2	Protection des biens.....	67
5.10.3	Obligations du titulaire.....	69
5.10.4	Localisation des données	69
5.10.5	Audit.....	70
5.10.6	Application des plans gouvernementaux	71
6	ANNEXES	72
6.1	Documents joints	72
6.2	Référence des exigences.....	72
6.3	Abréviations et Glossaire	72
6.3.1	Abréviations	72
6.3.2	Glossaire.....	75

TABLE DES ILLUSTRATIONS

Figure 1 : Le CNRS en région	8
Figure 2 : Réseau RENATER.....	16
Figure 3 : Page d'accueil de NEO	21
Figure 4 : Procédure d'authentification au CNRS.....	21
Figure 5 : Procédure de création d'un autre compte au CNRS	22
Figure 6 : Bandeau de navigation de NEO.....	23
Figure 7 : Structure des modules de NEO.....	23
Figure 8 : Interface d'un cours de NEO	24
Figure 9 : Interface du QCM de validation d'un module de NEO.....	25
Figure 10 : Menu du profil ALN dans NEO	26
Figure 11 : Gestion de l'arborescence des services/équipes de l'unité dans NEO	26

Figure 12 : Définition du parcours de formation par défaut de l'unité dans NEO.....	27
Figure 13 : Paramétrage du délai des relances envoyées aux nouveaux entrants dans NEO.....	27
Figure 14 : Gestion des ressources documentaires locales associées à chaque module dans NEO	27
Figure 15 : Validation des comptes des entrants auto-inscrits dans NEO.....	28
Figure 16 : Ajustement et suivi du parcours de formation de chaque entrant dans NEO	28
Figure 17 : Attestation pour signature du Directeur dans NEO	29
Figure 18 : Gestion des modules pour une délégation dans NEO	29
Figure 19 : Gestion des unités d'une délégation dans NEO.....	30
Figure 20 : Menu du profil ANN dans NEO	30
Figure 21 : Présentation de la forge logicielle	47
Figure 22 : Cycle de vie en cascade itératif et incrémental	60

1 CONTEXTE GENERAL

1.1 OBJET DE L'ACCORD-CADRE

Le présent accord-cadre a pour objet la maintenance corrective et adaptative de l'application de e-learning sur la prévention des risques NEO, y compris les prestations annexes rendues nécessaires par les évolutions du système (formations, expertises, ...).

L'application NEO est déployée au CNRS et à l'Inserm à partir de la plateforme Moodle de e-learning avec des spécificités développées en PHP pour répondre au processus de formation de ces établissements. Elle a pour but de former les nouveaux entrants dans ces établissements à la prévention des risques présents dans les unités de travail afin de se conformer à la réglementation. L'application comporte des modules de formation mis à disposition pour une formation en ligne et un back office permettant à des profils d'administratifs des métiers de la prévention de suivre et de piloter les parcours de formation.

L'application initiale est le fruit d'une collaboration CNRS/Inserm de la région Occitanie – Ouest.

Suite à la refonte en 2012, la solution est déployée nationalement et les marchés de TMA sont gérés par le CNRS.

Le CNRS est propriétaire des codes sources ; ceux-ci sont mis à disposition de l'Inserm sans limitation de durée via une convention liant les deux établissements, chacun ayant toute liberté de mise à disposition de ces codes à d'autres établissements publics via des conventions spécifiques.

Chaque autre établissement détenteur de la solution NEO en assure lui-même l'exploitation et l'assistance de façon indépendante.

L'objet de de cette TMA est de prendre en charge les demandes et la maintenance émanant exclusivement des 2 plateformes CNRS et Inserm.

1.2 PRESENTATION DU CNRS

Le Centre national de la recherche scientifique est un organisme public de recherche (Etablissement public à caractère scientifique et technologique) pluridisciplinaire placé sous la tutelle du [Ministère de l'Enseignement supérieur et de la Recherche](#) (MESR). Sa mission est de faire progresser la connaissance et être utile à la société.

Avec près de 33 000 personnes, un budget de 3,8 milliards d'euros, plus de 1100 laboratoires répartis en France et à l'étranger, le CNRS exerce son activité dans tous les champs de la connaissance qu'il s'agisse de biologie, chimie, écologie et environnement, homme et société, ingénierie et systèmes, mathématiques, nucléaire et particules, physique, sciences de l'information ou terre et univers.

Ces domaines de recherche sont regroupés au sein de dix instituts.

Sa gouvernance est assurée par le président-directeur général du CNRS, assisté de la directrice de cabinet et de trois directeurs généraux délégués à la science, aux ressources et à l'innovation.

Des informations plus complètes sont disponibles sur le site Web, à l'adresse suivante : <https://www.cnrs.fr/fr/le-cnrs>.

La présentation des services ci-dessous ne contient que le descriptif des services concernés par l'application NEO.

1.2.1 La direction générale déléguée à la science (DGD-S)

La **DGD-S** conduit, aux côtés du président-directeur général, la politique scientifique de l'établissement. Elle coordonne l'action des dix instituts du CNRS, veille à promouvoir l'interdisciplinarité et organise les partenariats avec les divers acteurs de la recherche, à l'échelle régionale, nationale, européenne ou internationale.

Pour remplir ses missions, la DGD-S s'appuie sur :

- les dix instituts et les unités de recherche qui leur sont rattachées,
- trois directions fonctionnelles :
 - la direction Europe et international (DEI),
 - la direction des données ouvertes de la recherche (DDOR),
 - la direction d'appui aux partenariats publics (DAPP),
- les missions pour les initiatives transverses et interdisciplinaires (MITI),

- la mission pour l'expertise scientifique (MPES),
- la mission programmes nationaux (MiPN)
- le Comité Très grandes infrastructures de recherche (TGIR),
- le secrétariat général du Comité national (SGCN).

Des informations plus complètes sont disponibles sur le site Web, à l'adresse suivante : <https://www.cnrs.fr/fr/le-cnrs>.

1.2.1.1 *Les unités (laboratoires)*

Le CNRS compte environ 1100 laboratoires répartis sur l'ensemble du territoire français.

Les **laboratoires** du CNRS sont les « briques de base » de l'établissement. Leurs équipes, formées de chercheurs, d'ingénieurs et de techniciens, sont à l'origine de la production et de la transmission des connaissances. Les laboratoires sont pour la plupart des unités mixtes de recherche, associant des partenaires du monde académique (universités, écoles et autres organismes de recherche) et industriel.

1.2.2 La direction générale déléguée aux ressources (DGD-R)

La **DGD-R** conduit, aux côtés du président, la politique administrative et financière de l'établissement. Elle a en charge le développement des ressources humaines et des activités de soutien à la recherche. Dans ce cadre, et en relation étroite avec la DGD-S, elle s'appuie sur les compétences des instituts du CNRS.

Pour remplir ses missions, la DGD-R s'appuie sur :

- dix-sept délégations régionales,
- six directions fonctionnelles,
- une structure transversale
- un pôle santé et sécurité au travail.

Des informations plus complètes sont disponibles sur le site Web, à l'adresse suivante : <https://www.cnrs.fr/fr/le-cnrs>.

1.2.2.1 *La direction des systèmes d'information (DSI)*

La **DSI** définit et met en œuvre les systèmes d'information **de gestion et de pilotage** des activités de l'établissement, en adéquation avec les orientations stratégiques et métiers de l'établissement (RH, finance, décisionnel, formation, référentiels, valorisation, missions...).

Elle gère également les outils mis en commun avec les partenaires du CNRS tels que l'Inserm et les universités, ainsi que la sécurité des systèmes d'information (outils et services, animation du réseau des correspondants sécurité...).

Enfin, la DSI met à disposition des laboratoires une offre de services numériques (ODS) destinée à simplifier, soutenir et sécuriser leur quotidien (travail collaboratif, mobilité, services cloud, sauvegarde des données, exploitation sécurisée de sites internet...).

La DSI comprend :

- **La Direction** : la directrice de la DSI est assistée d'un directeur adjoint et d'une directrice adjointe administrative.
- **Le Secrétariat Général** : chargé des aspects administratifs de la DSI, il gère les ressources humaines, le budget, le contrôle de gestion, la logistique et les achats.
- **Le département SI Finance** assure le maintien en conditions opérationnelles et la mise en œuvre des évolutions fonctionnelles et techniques de BFC (budget, finance, comptabilité) et de l'Infocentre métier Finance, SI financiers du CNRS.
- **Le département SI Laboratoires et soutien à la recherche** assure le maintien en conditions opérationnelles et la mise en œuvre des évolutions fonctionnelles et techniques des applications à destination des laboratoires et des services centraux notamment pour la gestion des achats, la gestion des missions, le dialogue de gestion, la gestion du patrimoine immobilier, la gestion de la valorisation et les appels à projets. Il assure également la conduite de projets de développement d'applications dans son périmètre d'activité.
- **Le département SI Ressources humaines et paie** assure le maintien en conditions opérationnelles et la mise en œuvre des évolutions fonctionnelles et techniques de Sirhus (Système d'Information Ressources Humaines des Unités et Services du CNRS), de l'infocentre métier RH et des convertisseurs équivalent temps plein travaillé (ETPT).

- **Le département SI Ressources humaines, santé prévention sécurité, décisionnel** assure le maintien en conditions opérationnelles et la mise en œuvre des évolutions fonctionnelles et techniques des applications ressources humaines, santé prévention et sécurité et décisionnel. Il réalise également la conduite de projets de développement d'applications dans son périmètre d'activité.
- **Le département Sécurité SI** apporte un support aux missions du responsable de la sécurité des systèmes d'information (RSSI) du CNRS (RSSIC). Il met en œuvre la politique de sécurité des SI du CNRS pour l'ensemble des SI qui sont sous la responsabilité de la DSI, il assure le pilotage des infrastructures de confiance en lien avec le ministère de tutelle.
- **Le département Plateforme des référentiels et de dématérialisation** met en œuvre les principaux référentiels structurants du SI. Il est chargé de les maintenir en conditions opérationnelles (plateforme MDM – Master Data Management). Il est aussi chargé de la mise en œuvre des plateformes de dématérialisation des documents, de préservation et de conservation de ces derniers (services de GED – Gestion Electronique de Documents et de SAE – Système d'Archivage Electronique).
- **Le département Architecture et assistance applicatives** pilote les marchés de maintenance transverses, il met en place et maintient les annuaires et outils de gestion d'habilitations, fournit de l'assistance en termes d'expertise développement et architecture applicative. Il met en place et maintient les outils d'intégration des données et assure l'assistance utilisateurs.
- **Le département Infrastructures SI** est chargé de spécifier, mettre en œuvre, opérer et maintenir les infrastructures (notamment réseaux, systèmes, bases de données) du SI du CNRS. Il accompagne toutes les activités portées par la DSI dans le domaine des infrastructures et de l'exploitation technique.
- **Le département Sites web, communication, accompagnement projet** conçoit et met en œuvre les outils pour la communication et le travail collaboratif au sein du CNRS (intranet, portails, espaces collaboratifs, sites web). Il accompagne le déroulement des projets SI au niveau urbanisation (études pour l'intégration de nouveaux besoins), qualité-méthodes et ergonomie des technologies interface homme machine (IHM). Enfin, il a en charge la communication interne et externe de la DSI.

La DSI est implantée sur deux sites Toulouse-Labège (31) et Meudon (92).

Des informations plus complètes sont disponibles à l'adresse suivante : <https://www.cnrs.fr/fr/dsi>.

1.2.2.2 L'organisation de la prévention au CNRS

LA prévention au CNRS se décline en trois niveaux d'intervention détaillés dans le tableau ci-dessous

Niveau	National		Régional	Local
Autorité	Président		Délégué.e régional.e	Directeur.ice d'unité
Prévention et sécurité	Pôle santé et sécurité au travail	- Coordonnateur national de prévention et de sécurité - Chargé.e.s de mission pour des risques spécifiques	Ingénieur.e régional.e de prévention et sécurité	- Assistant.e de prévention - Personnes compétentes pour un risque particulier
Médecine de prévention		Médecin coordonnateur national de médecine de prévention	Médecin animateur régional	Médecins du travail
Contrôle	Inspecteurs.ices santé et sécurité au travail			
Instance de concertation	<ul style="list-style-type: none"> - Comité social d'administration - Formation spécialisée en matière de santé, de sécurité et de conditions de travail^[1] 		Formation spécialisée en matière de santé, de sécurité et de conditions de travail ^[1]	Instance de concertation ou, à défaut, conseil de laboratoire

1.2.2.2.1 La Coordination nationale de prévention et de sécurité (CNPS)

L'activité de conseil et de coordination au niveau national pour toutes les questions concernant l'hygiène, la sécurité des personnes et des biens et la protection de l'environnement est confiée à la **CNPS** placée au sein de la DGD-R et qui est la MOA référente pour NEO au CNRS.

Des informations plus complètes sont disponibles sur le site Web du CNPS à l'adresse suivante : <http://www.dgdr.cnrs.fr/SST/CNPS/>

1.2.2.2.2 Les délégations régionales (DR)

Les dix-sept **DR** du CNRS sont les interlocutrices de premier plan des partenaires de l'organisme sur le terrain. Elles ont un rôle de gestion et d'accompagnement de proximité des laboratoires répartis sur le territoire. Elles apportent notamment leur aide pour le montage de projets industriels et de programmes européens.

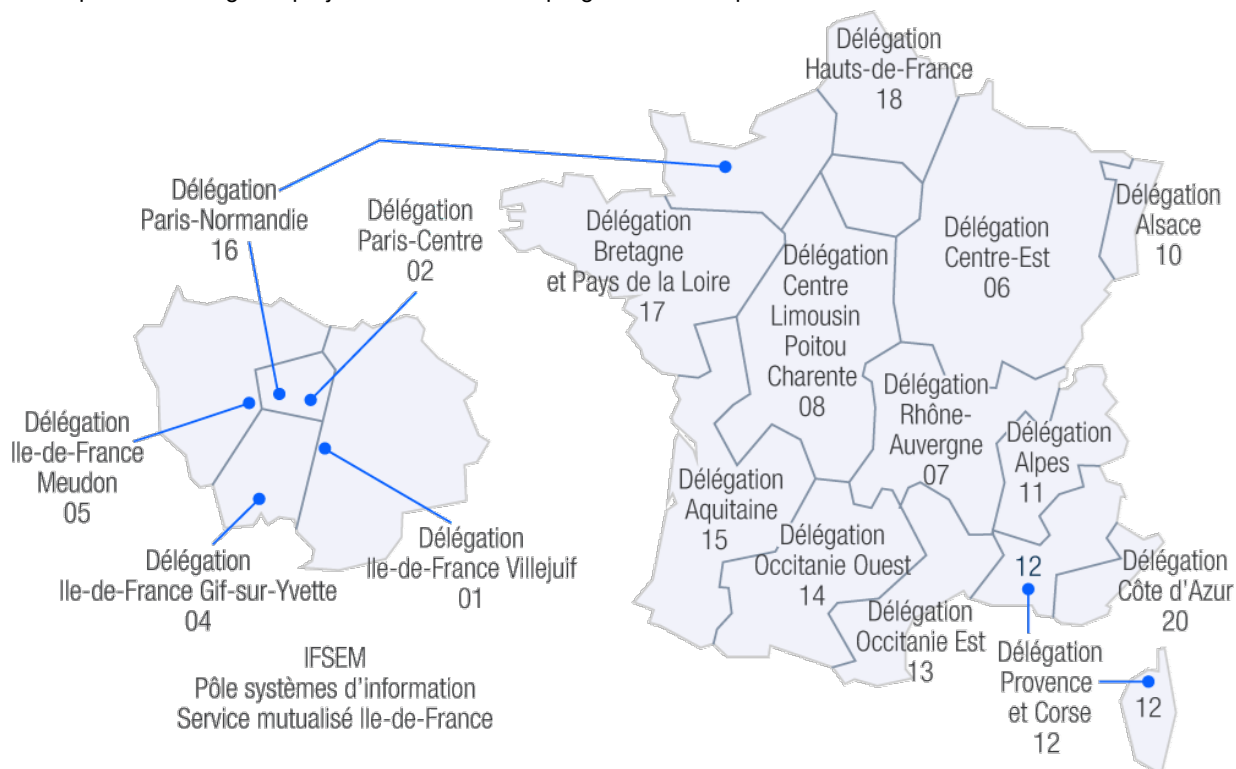


Figure 1 : Le CNRS en région

Des informations plus complètes sont disponibles sur les sites Web du CNRS en région à l'adresse suivante : <https://www.cnrs.fr/fr/delegations-regionales-du-cnrs>

Au sein des délégations régionales, les services de prévention et de sécurité sont menés par un ingénieur régional de prévention et de sécurité (IRPS).

Parmi les fonctions qui lui sont attribuées notons qu'il assiste le délégué régional pour tout ce qui concerne l'hygiène, la sécurité des personnes et des biens et la protection de l'environnement dans la circonscription. Il peut le représenter auprès de toutes les instances internes ou externes à la délégation.

L'IRPS anime et coordonne le réseau des Assistants de Prévention (AP) des unités et services propres de l'établissement et, pour les unités mixtes, il intervient dans ces domaines selon les termes de la convention établie avec l'établissement partenaire.

1.2.2.2.3 Les unités du CNRS

Au sein des unités du CNRS, les assistants de prévention (AP) mettent en œuvre la politique de prévention de l'établissement.

1.3 PRESENTATION DE L'INSERM

L'Inserm, Institut national de la santé et de la recherche médicale, est un établissement public à caractère scientifique et technologique (EPST) placé sous la double tutelle des ministères de la santé et de la recherche. Sa mission est de développer **une recherche biologique, médicale et en santé publique**. Le décret 83-975 du 10 novembre 1983 régit l'organisation et le fonctionnement de l'Inserm.

L'Institut comprend plus de **300 structures de recherche réparties sur l'ensemble du territoire sous le statut d'unités ou de services**. Ces structures scientifiques, technologiques ou administratives de taille très variable sont hébergées essentiellement, dans les milieux hospitaliers et universitaires et développent leur recherche ou leur activité en partenariat avec d'autres établissements de recherche ou de santé, ou avec des partenaires privés.

Ces unités ou services sont rattachées à **11 délégations régionales et à l'administration du siège**. Chacune de ces circonscriptions dispose d'une autonomie de gestion et assume la quasi-totalité des actes nécessaires à son fonctionnement.

Le siège regroupe la Direction générale et les directions centrales, une partie des activités de ces directions est déconcentrée dans les délégations régionales.

Au sein de l'Inserm, le **Département Système d'Information (« INSERM-DSI »)** propose, développe et maintient une architecture sécurisée et cohérente des informations nécessaires à la gestion de l'Institut.

Le DSI a pour missions :

- l'élaboration du schéma directeur du système d'information et l'exécution des projets ;
- le développement d'une démarche-qualité dans le traitement de l'information, la participation à l'optimisation des processus de gestion et à leur intégration cohérente dans le système de gestion de l'établissement ;
- la définition et la gestion des référentiels de données et de l'information sur les recherches ;
- la production informatique et la continuité du service des applications nationales ;
- l'animation du réseau des responsables régionaux du système d'information placés auprès des administrateurs délégués régionaux ;
- le fonctionnement sécurisé des réseaux et des applicatifs.

L'organisation de la prévention est définie par l'instruction générale pour la santé et la sécurité au travail à l'Inserm qui prend en compte le code du travail (Partie IV : Santé et Sécurité au travail, livres I à V) et le décret n° 82-453 modifié relatif à l'hygiène, à la sécurité ainsi qu'à la prévention médicale dans la fonction publique.

Le **service de coordination de la prévention des risques** et le **service de coordination de la médecine de prévention** sont les deux bureaux en charge du pilotage de la santé et de la sécurité au travail.

Ils ont pour mission de proposer la politique de prévention à la Direction Générale et de coordonner sa mise en œuvre. Ils s'appuient sur un réseau d'acteurs spécialisés présents aux différents niveaux de l'institut.

	Responsabilité	Conseil et assistance	Instance de dialogue
National	Direction générale (PDG +DGD)	Service de coordination de la prévention des risques – BCPR Service de coordination de la médecine de prévention – BCMP	F3SCT
Régional	Délégué(e) régional(e)	Conseiller(e)s de prévention Médecins du travail Service prévention	F4SCT
Local	Directeur(rice) de structure de recherche (unité, département, centre, service...)	Assistant de prévention Chargé prévention de centre + autres acteurs de prévention	Conseil de service (de laboratoire, d'unité)

La **délégation régionale de l'INSERM** représente l'Institut auprès de l'ensemble des partenaires régionaux publics et privés. Elle a pour mission principale d'accompagner les laboratoires de recherche, en particulier en matière soutien administratif et technique. Il existe 11 délégations régionales (3 en Île-de-France et huit dans les autres régions) et une administration du Siège.

Au sein des délégations régionales, les services de prévention et de sécurité sont menés par un ou plusieurs conseillers de prévention, chargés de coordonner la politique de prévention et sécurité des structures de recherche de leur circonscription. Ils animent en particulier le réseau des assistants de prévention dans les unités et services et participent à la mise en place des formations en matière de santé, de sécurité et des conditions de travail.

1.4 LIEU D'EXECUTION DE L'ACCORD-CADRE

La réalisation et maintenance de l'application s'effectue dans les locaux du titulaire.

Les comités, réunions ou ateliers de spécifications et de conception, nécessitant la présence du CNRS, se tiennent soit en visioconférence entre les sites concernés, soit sur site CNRS, à la DSI de Labège ou de Meudon ou à la CNPS de Meudon.

Les modalités pratiques sont définies au démarrage de l'accord-cadre.

Les locaux du CNRS se situent :

à Meudon (CNPS et DSI) :

CNRS
1 place Aristide Briand
92195 MEUDON CEDEX

à Toulouse (DSI) :

CNRS - DSI
358 rue Pierre Gilles de Gennes
31670 LABEGE

1.5 STRUCTURE DU CCTP ET CONVENTIONS DE REDACTION

Le livret 1 du CCTP est composé essentiellement des chapitres suivants :

- contexte du SI au CNRS : contexte dans lequel s'inscrit la réalisation et la maintenance de la solution, en terme de conformité réglementaire, d'infrastructure, d'urbanisation et d'intégration dans le système d'information existant,
- description de la solution : caractéristiques fonctionnelles, techniques et volumétrie de la solution existante à maintenir,
- cadre de cohérence technique de la solution : exigences applicables à la solution initiale et à toute évolution lors de la maintenance de la solution,
- cadre d'organisation des prestations : exigences applicables aux processus de conduite de projet, développement et maintenance de la solution, ainsi que mesures de sécurité encadrant les prestations.

Le livret 2 du CCTP contient la description des prestations et unités d'œuvre, objets de la commande.

Les exigences vis-à-vis du titulaire sont décrites dans le présent document dans des tableaux de la forme ci-dessous. La référence est composée de 3 lettres définissant le groupe d'exigences (cf. « Référence des exigences » en annexe) et de 3 chiffres (pas nécessairement consécutifs). Les exigences sont classées selon 3 niveaux :

- Priorité 0 : exigence impérative à satisfaire obligatoirement par le titulaire
- Priorité 1 : exigence très fortement souhaitée, à justifier si non satisfaite
- Priorité 2 : exigence souhaitée, pouvant être satisfaite, partiellement ou pas par le titulaire (avec justification)

Référence	Libellé exigence	Priorité
XXX_NNN	Libellé de l'exigence	0/1/2

La solution en place actuellement n'est pas intégralement conforme à toutes les exigences présentées dans ce document du fait de son antériorité à leur existence. Les mises en conformité nécessaires sont déclenchées à l'initiative du CNRS lorsqu'elles sont nécessaires, sous la forme de demandes d'évolutions. **Les nouveaux développements réalisés dans le cadre de ce marché doivent être conformes aux exigences sauf dérogation expresse du CNRS.**

La plupart des exigences du cadre de cohérence technique (CCT) du CNRS (cf. - § 4) sont partagées par l'Inserm. Quelques exigences en lien avec des aspects d'intégration dans le SI du CNRS sont propres au CNRS, aussi le respect de ces exigences concernera de potentiels compléments de solution spécifiques CNRS.

2 CONTEXTE DU SI AU CNRS ET A L'INSERM

2.1 CONFORMITES REGLEMENTAIRES

Les applications mises en œuvre par le CNRS et par l'Inserm sont soumises à des conformités réglementaires définies dans des référentiels interministériels présentés dans les paragraphes suivants.

Référence	Libellé exigence	Priorité
REGL_001-a	Les téléservices (applications destinées à la communication interadministration ou destinées à réaliser des téléprocédures ouvertes à des usagers, c'est-à-dire application grand public) sont mis en œuvre conformément aux référentiels interministériels. Les téléservices sont conformes au RGS : https://www.ssi.gouv.fr/administration/reglementation/confiance-numerique/le-referentiel-general-de-securite-rgs	0
REGL_001-b	Les téléservices (applications destinées à la communication interadministration ou destinées à réaliser des téléprocédures ouvertes à des usagers, c'est-à-dire application grand public) sont mis en œuvre conformément aux référentiels interministériels. Les téléservices sont conformes au RGI (interopérabilité, selon le profil choisi par le CNRS) : http://references.modernisation.gouv.fr/interopabilite	0
REGL_001-c	Les téléservices (applications destinées à la communication interadministration ou destinées à réaliser des téléprocédures ouvertes à des usagers, c'est-à-dire application grand public) sont mis en œuvre conformément aux référentiels interministériels. Les téléservices sont conformes au RGAA (accessibilité) : https://www.numerique.gouv.fr/publications/rgaa-accessibilite/ (https://a11yproject.com)	0
REGL_002-a	Pour les applications qui ne sont pas des téléservices, l'objectif de conformité aux référentiels RGS est poursuivi.	2
REGL_002-b	Pour les applications qui ne sont pas des téléservices, l'objectif de conformité aux référentiels RGI est poursuivi.	2
REGL_003	La page d'accueil de la solution permet d'accéder aux mentions légales : licence d'utilisation du logiciel, point de contact éditorial et technique, éventuelles mentions légales réglementaires concernant les données à caractère personnel, l'utilisation des cookies.	0
REGL_008	La gestion des cookies est conforme à la réglementation en vigueur. La solution permet d'afficher la liste des cookies nécessaires à son fonctionnement et la manière de les supprimer dans les navigateurs supportés.	0
REGL_009	La solution s'interface avec ou gère une plateforme de gestion des consentements (consent management platform) permettant de débrayer le positionnement des cookies non essentiels.	1

2.1.1 Politique Générale de Sécurité des systèmes d'Information

Concernant les aspects sécurité, les objectifs de la Politique Générale de Sécurité des systèmes d'Information (PGSI¹) du CNRS sont les suivants :

- Protéger le savoir-faire du CNRS et les données permettant de valoriser la recherche ;
- Assurer la protection du potentiel scientifique et technique et le respect des engagements internationaux ;
- Garantir la disponibilité des moyens opérationnels du CNRS ;
- Assurer le respect par le CNRS de ses obligations légales, réglementaires et contractuelles ;
- Eviter les accidents qui résulteraient de la perte de contrôle d'un processus ou tout au moins en limiter les conséquences ;
- Conserver au CNRS un statut de partenaire de confiance.

A ces fins, le CNRS applique les principes de politique générale suivants (issus de la PGSI1 du CNRS) :

¹ PGSI : document diffusable sur demande à l'équipe sécurité de la DSI du CNRS

- L'ensemble du périmètre placé sous la responsabilité du CNRS doit être couvert ;
- Toutes les exigences légales et réglementaires doivent être prises en compte ;
- La gestion des risques doit être réalisée de façon systématique suivant la réglementation Française et les normes internationales en vigueur ;
- L'organisation qui est mise en place pour piloter et mettre en œuvre cette politique doit disposer des moyens humains compétents en nombre suffisant ;
- Les mesures de protection devront être complétées par des mesures de défense active efficaces ;
- L'application de cette politique est contrôlée.

L'Inserm applique une politique générale de sécurité des systèmes d'information identique.

D'un point de vue contractuel, le titulaire doit respecter au minimum les exigences sécurité du présent CCTP.

Référence	Libellé exigence	Priorité
REGL_004	<p>Le titulaire se conforme au cadre réglementaire applicable en terme de SSI, à savoir (de façon non exhaustive) :</p> <ul style="list-style-type: none"> - les annexes techniques du Référentiel Général de Sécurité (RGS) - la Politique de Sécurité des Systèmes d'Information de l'Etat (PSSI-E) - l'instruction interministérielle 901 (II 901) portant sur les informations sensibles marquées « diffusion restreinte » - la PSSI du CNRS (PSSI-C). <p>RGS : https://cyber.gouv.fr/le-referentiel-general-de-securite-rgs PSSI-E : https://www.legifrance.gouv.fr/circulaire/id/38641 II 901 : https://cyber.gouv.fr/instruction-interministerielle-n901 PSSI-C : document non public, disponible sur demande</p>	0
REGL_005	<p>D'un point de vue technique, le titulaire applique les différents guides de l'ANSSI : https://cyber.gouv.fr/publications?field_type_de_publication_target_id%5B934%5D=934</p>	1

2.1.2 Protection des données à caractère personnel (DCP)

Le transfert de données sensibles ou personnelles vers le SI du titulaire est interdit dans le cadre des prestations de cet accord-cadre. Il se peut cependant que par dérogation et de façon exceptionnelle, le CNRS le demande.

Dans ce cas, le responsable sécurité du titulaire sera amené à instruire un dossier de dérogation dont la durée initiale est limitée dans le temps (**maximum 1 an**). Ce dossier, qui constitue une annexe au PAS, explicitera quelles données à caractère personnel (DCP) seront accédées dans le cadre de réalisation des prestations, quels sont les risques et quelles mesures seront prises pour réduire ces risques. Ce dossier de dérogation initial est instruit en comité de suivi. Il est revu par ce même comité sur inscription à l'ordre du jour par le CNRS. Le titulaire ne peut s'opposer à cette demande, que le CNRS n'a pas à motiver.

A l'issue de la période initiale, le titulaire peut demander une reconduction de la dérogation. A cette fin :

- le responsable sécurité du titulaire met à jour le dossier de dérogation,
- ce dossier est instruit en comité de suivi,
- la reconduction ne peut intervenir que sur décision expresse du CNRS, pour une durée qui ne peut être supérieure à la durée initiale. Le CNRS peut toutefois, par une décision motivée, accorder une prorogation d'une durée supérieure.

Conformément aux dispositions réglementaires en vigueur (loi informatique et libertés en vigueur, règlement général pour la protection des données en UE RGPD), les traitements de DCP dont le CNRS est responsable de traitement sont inscrits au registre des traitements tenus par le Délégué à la protection des données de l'établissement.

Le titulaire est informé que s'il a lui-même recours à des sous-traitants, les dispositions qui lui sont applicables le sont automatiquement à ces sous-traitants, et qu'il fait son affaire de leur information et de la contractualisation écrite de ces obligations. Le CNRS demande communication de ces engagements lors de la phase de consultation et est à tout moment autorisé à vérifier, conformément à la clause d'audit, la réalité de cet engagement.

Le titulaire est responsable, dans les limites imposées par la loi, de la sécurité (confidentialité, intégrité et disponibilité) des DCP qu'il traite et auxquelles il a accès.

Registre de traitements

Le titulaire tient registre des traitements de DCP qu'il opère pour le compte du CNRS. Ce registre peut être consulté à tout moment par le CNRS, ou par l'autorité de régulation compétente (Commission nationale de l'informatique et des libertés – CNIL).

Traitement des incidents impactant les DCP

Le titulaire intervient dans le processus de gestion des incidents de sécurité liés à l'application ; son aide est requise pour :

- Evaluer l'impact d'un incident de sécurité sur les DCP (*par exemple* : divulgation de données, modification non autorisée des données, suppression de données...) en nombre d'utilisateurs et en quantité de données exposées ;
- Fournir les correctifs nécessaires à la résolution de l'incident.

Ces actions devront être réalisées dans un délai permettant au CNRS en tant que responsable de traitement de réagir de manière adéquate dans le délai légal de 72 heures. Le niveau de priorité accordé aux incidents de sécurité impactant les DCP est automatiquement le niveau le plus élevé.

Prise en compte de la sécurité et du respect de la vie privée par défaut dans les développements

Le titulaire répond aux exigences de sécurité du présent cahier des charges, et complète sa réponse en décrivant la démarche industrielle qu'il met en œuvre pour répondre aux exigences de l'article 25² du RGPD. Il indique quels outils et quelles méthodes il met en œuvre pour atteindre l'objectif de conformité. Ces éléments peuvent faire l'objet d'un contrôle par le CNRS.

Obligation d'information du CNRS en cas de faille de sécurité impactant le SI du titulaire

En cas d'incident de sécurité touchant le SI du titulaire et pouvant mettre en péril les DCP confiées par le CNRS (notamment, compromettant les accès au SI CNRS utilisés pour la réalisation des prestations), le titulaire informe immédiatement et de manière exhaustive le CNRS de l'événement.

Le CNRS peut demander tout complément d'information pour lui permettre d'apprécier la portée de l'incident, afin d'apprécier la nécessité d'informer l'autorité de régulation et/ou les personnes concernées dans les cas prévus par la réglementation. »

La position et les attentes de l'Inserm sur la protection des données personnelles est identique à celle du CNRS.

2.1.3 Interopérabilité

Le référentiel général d'interopérabilité (RGI) est un cadre de recommandations référençant des normes et standards qui favorisent l'interopérabilité au sein des systèmes d'information de l'administration.

Ces recommandations constituent les objectifs à atteindre pour favoriser l'interopérabilité. Elles permettent aux acteurs cherchant à interagir et donc à favoriser l'interopérabilité de leur système d'information, d'aller au-delà de simples arrangements bilatéraux.

Le RGI est défini dans 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. Dans l'article 11 de cette ordonnance, le « RGI fixe les règles techniques permettant d'assurer l'interopérabilité des systèmes d'information. Il détermine notamment les répertoires de données, les normes et les standards qui doivent être utilisés par les autorités administratives. Les conditions d'élaboration, d'approbation, de modification et de publications de ce référentiel sont fixées par décret ».

Le référentiel général d'interopérabilité applicable est disponible en libre accès :

<https://www.numerique.gouv.fr/publications/interoperabilite/>

https://www.numerique.gouv.fr/uploads/Referentiel_General_Interoperabilite_V2.pdf

Le titulaire respecte les dispositions du profil d'interopérabilité P1 et en prévision d'évolution ultérieures de l'application les profils P2 et P4 choisis par le CNRS conformément aux objectifs de présent accord cadre.

² <https://www.cnil.fr/fr/reglement-europeen-protection-donnees/chapitre4#Article25>

2.1.4 Accessibilité numérique

2.1.4.1 Contexte

Comme le définit l'article 47 de la loi 2005-102 du 11 février 2005, est concerné par l'obligation légale d'accessibilité tout type d'information sous forme numérique quels que soient le moyen d'accès, les contenus et le mode de consultation.

Sont donc concernés tous les services publics de type internet, intranet, extranet, applications web (développement spécifique ou progiciels intégrés au SI), applications mobiles ainsi que les documents émanant de tous ces services (pdf...).

2.1.4.2 Niveau attendu pour l'accessibilité numérique

La solution doit prendre en compte le niveau légalement attendu pour l'accessibilité numérique qui est à ce jour le niveau double A (AA).

Le référentiel d'accessibilité applicable est disponible en libre accès :

<https://accessibilite.numerique.gouv.fr/>

Les critères à retenir du référentiel général d'accessibilité pour les administrations (RGAA) dans sa version 4.0 sont donc tous ceux permettant de répondre aux niveaux déduits [A] et [AA] du WCAG (Web Content Accessibility Guidelines).

Niveaux de conformité WCAG :

Niveau	Définition de la conformité	Critères
A (niveau minimal)	La page web satisfait à tous les critères de succès de niveau A ou une version de remplacement est fournie.	Critères de succès essentiels pouvant raisonnablement s'appliquer à toutes les ressources web.
AA	La page web remplit tous les critères de succès de niveau A et AA ou une version de remplacement conforme au niveau AA est fournie.	Critères de succès pouvant raisonnablement s'appliquer à toutes les ressources web.

2.1.4.3 Déclaration de conformité

Référence	Libellé exigence	Priorité
ACC_001	Sauf accord exprès du CNRS, le titulaire s'engage pour tout développement spécifique de page, à respecter un niveau de conformité supérieur à 50%.	0
ACC_002	Pour un progiciel, le titulaire s'assure que le progiciel fourni ou distribué est accompagné d'une déclaration d'accessibilité valide. Cette déclaration est consultable via un lien conforme au RGAA.	1
ACC_003	A minima la page d'accueil de chaque application doit contenir un lien dont le nom reflète le niveau de conformité (« Accessibilité : totalement conforme » ou « Accessibilité : partiellement conforme » ou « Accessibilité : non conforme »). Ce lien pointe vers la déclaration d'accessibilité fournie par le CNRS (pdf ou page html) ou le titulaire (cas des progiciels). La mise à jour de l'intitulé du lien et de la déclaration d'accessibilité doit être possible sans nouveau déploiement de l'application. Dans la mesure du possible, il est demandé de mettre le lien dans un pied de page (footer) visible sur toutes les pages de l'application.	0
ACC_004	Le titulaire est informé que le CNRS conduit des audits de conformité, par ses propres équipes ou par celles de tiers désignés par lui, ayant pour objectifs : - de vérifier le respect par le titulaire de ses engagements initiaux mis en œuvre concernant le RGAA sur un ensemble de pages représentatives de l'application ainsi que les pages réglementaires obligatoires - de publier la déclaration de conformité (créée ou mise à jour selon l'audit) Le résultat des audits conduit à la rédaction d'un plan d'action de la part du titulaire. Les actions inscrites ne conduisent pas à facturation supplémentaire de la part du titulaire si elles découlent directement d'un constat de non-conformité par rapport : - à ses engagements initiaux ou - à la réglementation en vigueur à la date de notification de l'appel d'offre. Dans tous les autres cas (évolution de la réglementation, évolution d'une application...), le titulaire propose une cotation pour la réalisation des prestations de mise en conformité.	0

L'échantillon sur lequel est réalisé l'audit de conformité porte **au moins** sur les pages listées sur le site RGAA (<https://accessibilite.numerique.gouv.fr/obligations/evaluation-conformite/>).

2.2 PRESENTATION DES INFRASTRUCTURES DU SI CNRS

Le CNRS et l'Inserm disposent chacun de leurs propres infrastructures.

Les infrastructures déployées pour la solution NEO sont similaires dans les deux établissements, seules les infrastructures CNRS sont décrites ci-dessous, les particularités propres à l'INSERM sont précisées le cas échéant.

2.2.1 Sites et utilisateurs du système d'information

Les utilisateurs du système d'information du CNRS sont principalement répartis :

- dans les 17 délégations, en régions et en Ile de France et sur le siège parisien de l'établissement. Ils représentent environ 3000 agents, dotés principalement de poste de travail de type PC sous Windows ;
- dans l'ensemble des laboratoires, répartis sur l'ensemble du territoire. Ils représentent plus de 60 000 personnes potentiellement utilisateurs du système d'information dont plus de 30 000 agents CNRS.

2.2.2 Centres serveurs

Toutes les applications du SI et services techniques associés sont hébergés sur des centres serveurs mutualisés qui disposent des caractéristiques physiques, techniques et organisationnelles pour ce type d'activité.

Le CNRS utilise deux centres serveurs. Le centre principal d'hébergement est situé à VILLEURBANE (69) est géré par une entité interne au CNRS.

2.2.3 Réseau

Les sites CNRS **et** Inserm sont connectés au réseau national de la recherche : RENATER.

RENATER offre plusieurs points de présence (Nœud de Raccordement) sur le territoire national à l'ensemble de la communauté enseignement supérieur et recherche.

Il permet de relier les sites de la recherche, directement ou au travers de réseaux métropolitains.

On trouvera sur le site du groupement d'intérêt public (GIP) en charge de ce réseau tous les éléments d'informations disponibles : <http://www.renater.fr/>

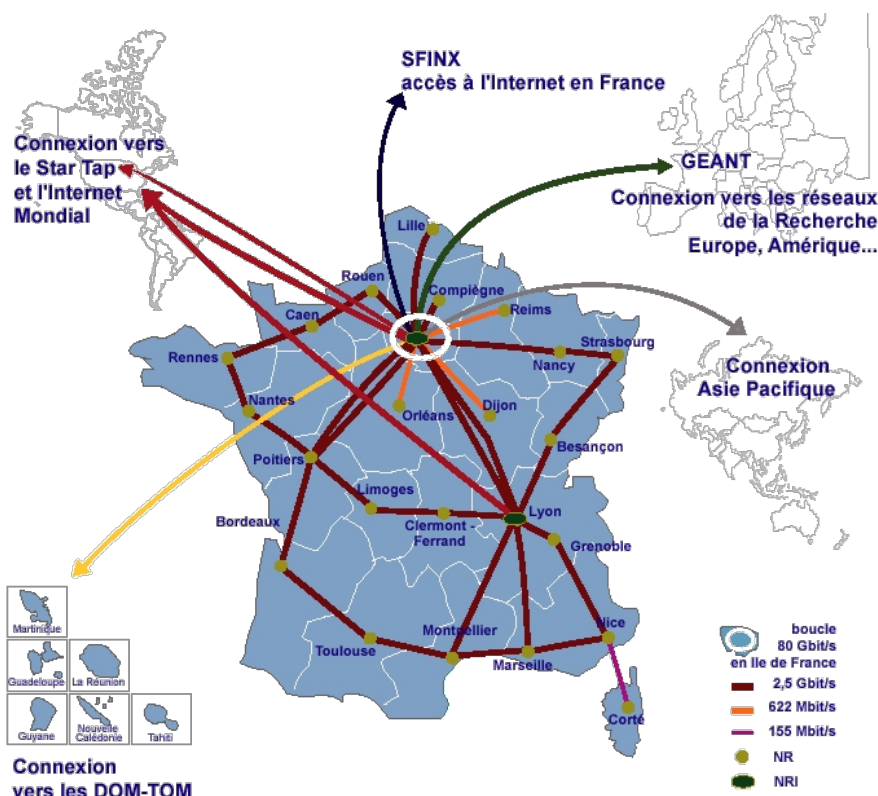


Figure 2 : Réseau RENATER

Afin d'avoir la maîtrise des flux spécifiques du système d'information du CNRS, la DSI a construit un réseau dédié, Sires, qui fédère l'ensemble des sites administratifs et des centres serveurs. Sires s'appuie sur l'infrastructure de RENATER et il est opéré au travers d'un marché d'infogérance.

Les centres serveurs sont directement reliés sur RENATER.

Tous les flux du SI sont aujourd'hui de type IPV4. La gestion du réseau s'appuie largement sur les technologies de réseaux privés virtuels (VLAN), de translation d'adresses IP (NAT) et de chiffrement (via une technologie de type VPN ou autre).

La sécurisation des flux est basée sur du filtrage de flux et des technologies de firewall standards.

2.2.4 Infrastructures

Les infrastructures matérielles utilisées sur les centres serveurs sont normalisées. La construction de ces architectures a été basée sur deux préoccupations majeures :

- Mettre en œuvre des technologies capables de répondre aux exigences de qualité de service du SI CNRS, en termes de performances, disponibilité, intégrité et sécurité.
- Rationaliser et homogénéiser les équipements pour favoriser la maîtrise technique et minimiser les coûts de possession.

Les applications du SI CNRS sont hébergées sur une infrastructure virtualisée, sauf en cas de contraintes spécifiques.

2.3 PRINCIPES D'URBANISATION ET D'INTÉGRATION DANS LE SI

Les principes d'urbanisation et d'intégration détaillés ci-dessous sont ceux mis en place au CNRS.

L'Inserm applique des principes identiques.

2.3.1 Principes généraux :

La démarche d'urbanisation mise en œuvre à la DSI du CNRS doit accompagner, faciliter et maîtriser la transformation continue et progressive du SI en le rendant de plus en plus agile et en assurant sa pérennité pour en tirer le maximum de plus-value, en cohérence avec les orientations stratégiques, métiers et opérationnelles de l'organisme.

Cette démarche doit aider l'évolution du SI par une optimisation de l'existant, tournée vers les objectifs suivants :

- capitaliser sur les socles existants ;
- poursuivre l'intégration des différents systèmes dans l'optique d'une gestion modernisée ;
- garantir la fiabilité des données de référence dans le système d'information global.

Plus particulièrement, 4 grands principes sont mis en avant par la démarche d'urbanisation et d'intégration dans les SI :

1. Principe de cohérence forte pour aider à répartir les contours fonctionnels et informationnels entre les applications du SI dans le but d'éviter toute redondance fonctionnelle et de limiter les flux entre applications participant au même processus métier. Un modèle informationnel et un modèle des processus métier sont fortement recommandés, voire attendus, pour aider à ces choix de répartition applicative ;
2. Principe de couplage faible entre applications pour réduire les dépendances entre applications et ainsi limiter les impacts sur le SI en cas d'évolution d'une partie de ce SI ;
3. Développer l'utilisation de briques numériques, fonctionnelles et/ou applicatives communes et mutualisées dans une logique de plateformes transverses ;
4. Prendre en compte la dimension « laboratoire » et ainsi découpler de façon modulaire (modules applicatifs disjoints) autant que faire se peut les fonctionnalités « Etablissement » des fonctionnalités « Laboratoire » dans la perspective de futures mutualisations potentielles des fonctionnalités « Laboratoire » et d'éventuelle répartition dans des SI distincts des fonctionnalités « Etablissement » et « Laboratoire » ; le tout en cohérence avec les actions parallèles éventuelles sur les mêmes sujets par les SI des établissements partenaires du CNRS.

2.3.2 Principes d'échanges

Pour mettre en œuvre le principe de couplage faible, des protocoles d'échanges sont établis, préconisant l'utilisation de :

- systèmes d'intermédiation (cf. § 2.3.3.1) pour éviter les échanges point à point entre deux applications en procédant par ½ flux via ces systèmes d'intermédiation ;
- formats d'échange communs sous la forme de format pivot par objet métier échangé. Le format pivot, indépendant des applications et de leur modèle de données, est une représentation partagée et intrinsèque d'un objet (métier ou technique), tenant compte de l'ensemble de ses cas d'usages. Il précise aussi les référentiels et nomenclatures communs et partagés à utiliser éventuellement pour ses attributs ;
- fonctions d'intégration (ou services applicatifs) de ces formats pivots dans le cadre des flux entrants ;
- fonctions d'exposition (ou services applicatifs) des informations vers ces formats pivots dans le cadre des flux sortants.

Ces principes s'appliquent aussi bien aux échanges de données et informations internes au SI qu'aux échanges avec l'extérieur.

2.3.3 Plateformes transverses et services proposés

2.3.3.1 *Systèmes d'intermédiation*

Actuellement les systèmes d'intermédiation mis en œuvre dans le SI du CNRS sont :

- un gestionnaire applicatif d'échanges et de services « outil EAI/ESB CNRS » (découpage en ½ flux, format pivot des objets métiers échangés) qui a la responsabilité et la gestion des échanges en termes d'orchestration, de chronologie des flux le cas échéant, de transcodification des données vers les SI cibles ou depuis les SI sources ;
- un proxy de services web ;
- une exposition de services web de données de référence (mise à disposition des formats pivots persistés des objets métiers de référence)

2.3.3.2 *Gestion des données de référence*

La DSI du CNRS dispose d'un outil MDM (Master Data Management) nommé Réséda et proposant des services de gouvernance et de mise en qualité des données, de recherche approchante...des données de référence.

Actuellement Réséda gère les référentiels suivants (liste non exhaustive) :

- Structures organisationnelles du CNRS ;
- Personnels des structures du CNRS ;
- Fournisseurs ;
- Contacts.
- Partenaires

Ainsi qu'un certain nombre de nomenclatures.

La mise à disposition, au reste du SI CNRS, des données de ces référentiels se fait par les services web de données de référence (cf. plus haut).

2.3.3.3 *Fournisseur d'identité*

Les services d'authentification web centralisée du CNRS (web SSO) via le protocole SAML 2.0, sont regroupés sous la dénomination de Janus. Ils consistent en plusieurs fournisseurs d'identités (IdP) dépendant de la population à authentifier (Personnel des unités CNRS, Prestataires et usagers des unités CNRS, Externes) et du niveau d'authentification nécessaire.

Dans le cas où plusieurs fournisseurs d'identités peuvent être utilisés pour accéder à la solution, un mécanisme de sélection par l'utilisateur du fournisseur d'identité est mis en place. Ce mécanisme est nommé WAYF (Where Are You From).

Il s'appuie sur le référentiel des comptes utilisateurs alimenté par le service IAM (cf. § 2.3.3.4).

2.3.3.4 *Service référentiel de comptes et gestion des accès et habilitations (IAM)*

Ce service recouvre des outils qui permettent la mise à jour du référentiel de comptes utilisateurs du SI CNRS à partir des données du référentiel des personnels des structures du CNRS.

Les données du référentiel des comptes utilisateurs sont exposées par des services Web à l'usage des applications. Elles sont également pour certaines transmises à l'application via le processus d'authentification.

Une gestion des accès applicatifs est également en place mais va évoluer dans le futur pour prendre en compte une plus grande automatisation et de nouvelles fonctionnalités pour l'attribution de rôles applicatifs à des comptes utilisateurs.

2.3.3.5 *Gestion électronique de document (GED) et archivage*

Le système de gestion électronique de document (GED) du CNRS est basé sur l'outil EverSuite (<http://www.ever-team.com/>).

La GED du CNRS propose des services dédiés aux applications pour stocker, gérer, mettre à disposition voire archiver les documents nécessaires et/ou produits par ces applications.

2.3.3.6 *Services de recueil et de mise à disposition des consentements (RGPD) (bientôt disponible)*

Le CNRS propose un service de gestion des consentements, au sens du Règlement général sur la protection des données (RGPD), dont les principales fonctions sont la captation, la conservation, l'historisation et la diffusion des consentements des personnes sur les traitements de leurs données personnelles.

Les entrants de ce service sont la définition des populations cibles (en extension ou en compréhension), les documents d'information des personnes, la liste des traitements concernés, et éventuellement les consentements pour ceux recueillis par ailleurs.

2.3.4 Prise en compte des changements de l'organisation structurelle des établissements CNRS et Inserm

Dans le cadre de la poursuite de la transformation vers un système d'information qui permet un alignement sur les stratégies de l'établissement, les outils proposés pour les SI et applications doivent prendre en considération, le plus nativement possible, les différentes restructurations du CNRS qui peuvent être classées en 2 types :

- les restructurations cycliques :
 - chaque année, une partie des unités de recherche est renumérotée, fusionnée, éclatée, ... (changement de référence métier) ;
 - les instances (conseils scientifiques du CNRS et des instituts, sections et commissions interdisciplinaires) du Comité National de la recherche scientifique (changement de périmètre sans changement systématique de référence métier) renouvelées tous les 4 ans ;
 - ... ;
- les restructurations organisationnelles : *exemples, le remplacement en 2009 des départements scientifiques par des Instituts ; la fusion en 2022 de la délégation régionale de Normandie (DR19) avec la Délégation Paris-Michel-Ange (DR16).*

Référence	Libellé exigence	Priorité
URB_001	La solution est en capacité de fournir une continuité de service fonctionnelle dans le temps, en tenant compte des différents types de restructuration de l'organisation CNRS, impactant les SI et applications.	1

Le référentiel d'organisation du CNRS est géré via l'outil MDM, et plus particulièrement dans le référentiel Réséda Structure.

Les restructurations cycliques de l'organisation du CNRS, sont diffusées à l'ensemble du SI à partir de ce référentiel, au travers de web services.

Référence	Libellé exigence	Priorité
URB_002	La solution s'alimente du référentiel d'organisation structurelle du CNRS, à partir de ses services web dédiés.	1

3 DESCRIPTION DE LA SOLUTION EN PLACE

3.1 PRESENTATION DE LA SOLUTION

3.1.1 Présentation fonctionnelle

Une des étapes clés pour assurer la sécurité et protéger la santé des personnels est la formation des nouveaux arrivants. Cette étape, qui est une obligation réglementaire, fait partie des missions assurées par les assistants de prévention. L'objectif de NEO, localement, est d'aider l'assistant de prévention dans sa mission et, au niveau national, de diffuser un message homogène et validé par les experts de la prévention.

NEO est une solution en e-learning basée sur une plateforme Moodle réalisée spécifiquement pour les besoins du CNRS/Inserm afin de dispenser une formation générale à la Prévention et à la sécurité dans chaque unité de travail à tous les nouveaux entrants.

NEO propose à ce jour 4 modules de formation destinés aux entrants : Prévention, Incendie, Risques Biologiques et Risques chimiques.

L'enrichissement de NEO avec d'autres modules (radioprotection, rayonnements optiques artificiels...) est d'ores et déjà prévu.

Chaque module dure environ 30 minutes et comporte des cours et des animations et jeux réalisés avec H5P.

Une attestation délivrée par l'outil, mais signée manuellement du Directeur de l'unité de travail valide la formation.

Par extension des formations destinées à d'autres acteurs de la prévention et de la Sécurité peuvent aussi être déployées dans NEO :

- C'est le cas au CNRS avec des formations destinées aux Assistants de Prévention (AP) sur les missions des AP.

L'application permet aussi :

- de produire dans NEO des contenus de formation selon une charte graphique définie
- d'intégrer et/ou d'adapter des cours de formation provenant d'autres plateformes moodle
- de diffuser les cours à différents périmètres de population en leur associant des ressources documentaires
- de définir des parcours de formation adaptés au profil de chaque unité
- de piloter le suivi des sessions de formations
- de communiquer sur l'avancement des parcours en générant des alertes à destination des entrants ou des AP
- de s'interfacer via des flux avec les structures et les nomenclatures du CNRS et avec les personnels au CNRS et à l'Inserm
- de gérer différents niveau de droits selon les rôles des utilisateurs
- de gérer 2 modes de connexion : authentifié pour personnels des unités ou non authentifié en mode auto-inscription pour les personnes non référencées dans le SI

3.1.1.1 Paramétrage de l'application

L'application fonctionne de façon similaire au CNRS et à l'Inserm mais des paramétrages sont mis en place pour s'adapter aux nuances des SI respectifs :

- Un système d'authentification différent : CAS (Central Authentication Service) à l'Inserm et Janus basé sur Shibboleth au CNRS
- Une mise à jour des unités et des délégations via un flux structure et nomenclature exclusivement au CNRS ; une mise à jour manuelle de ces données à l'Inserm
- Une intégration du flux des entrants avec des données supplémentaires facultatives côté CNRS pour analyser plus finement les caractéristiques des entrants.

L'Inserm et le CNRS s'accordent toujours sur les évolutions souhaitées de façon à garantir l'usage d'une même application et conserver le principe de la mutualisation.

Si un établissement ne souhaite pas une fonctionnalité nécessaire à l'autre établissement un point de paramétrage permet à l'autre établissement d'inactiver cette fonctionnalité.

3.1.1.2 Accès à l'application

L'utilisateur se connecte à une page d'accueil lui permettant de choisir sa modalité de connexion selon s'il est déjà référencé dans le SI ou non.

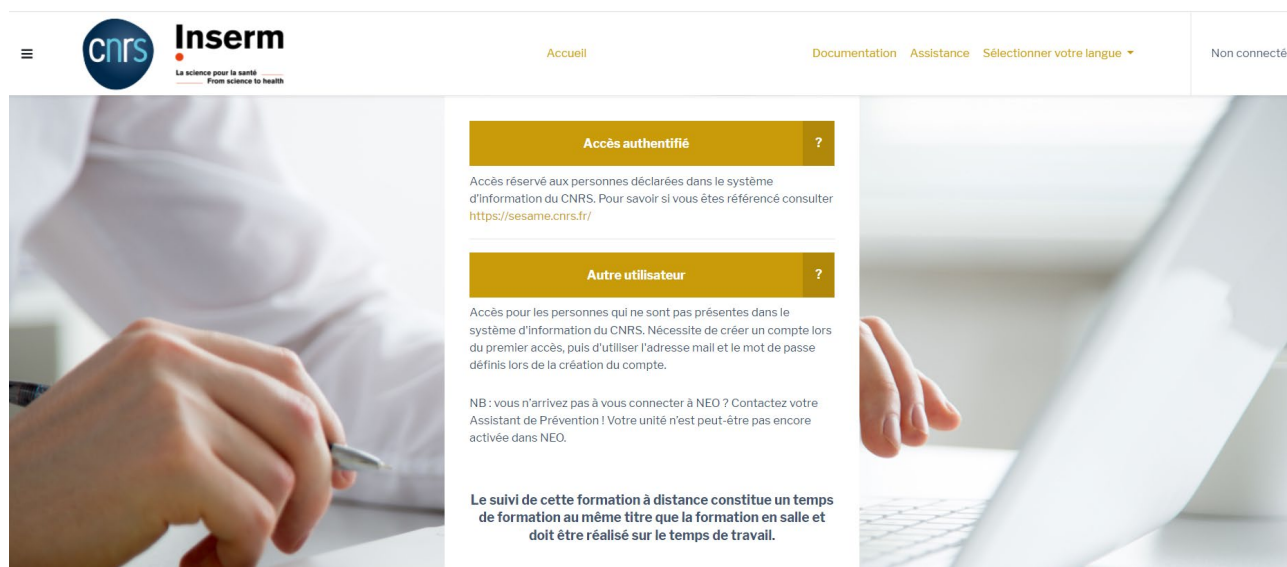


Figure 3 : Page d'accueil de NEO

Donc un utilisateur qui n'est pas présent dans le CAS de l'Inserm ou Janus au CNRS peut faire une demande de compte directement via NEO : ce compte pourra être validé par un gestionnaire de NEO si la demande est justifiée.

Un utilisateur qui choisit le mode « Accès authentifié » accède aux fonctionnalités de l'application définies pour son profil si l'authentification est réussie. Cette modalité concerne les entrants et tous les profils administratifs de NEO. Si l'utilisateur dispose de plusieurs profils dans l'application, NEO lui propose d'abord de sélectionner un profil de connexion parmi les siens.

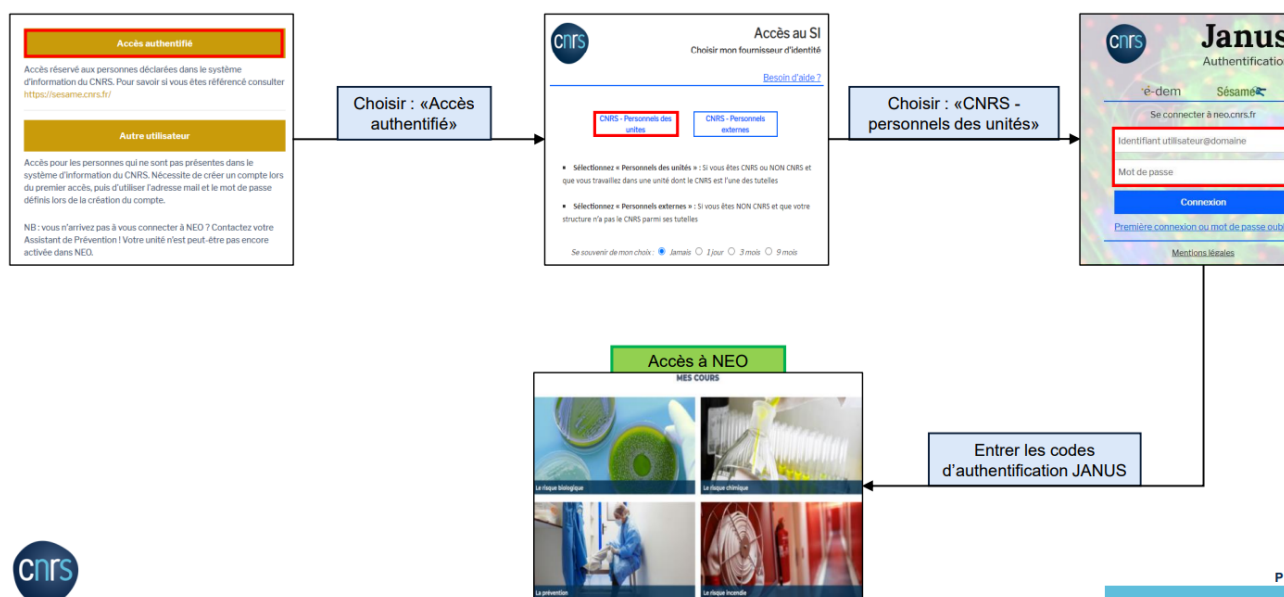


Figure 4 : Procédure d'authentification au CNRS

Un utilisateur qui choisit le mode « Autre utilisateur » devra confirmer sa demande de connexion depuis un email reçu et devra attendre que sa demande soit validée dans NEO pour accéder à l'appliquatif.

Une synchronisation entre le flux quotidien des entrants et les comptes déjà référencés dans NEO permet de les fusionner ou de les mettre à jour.

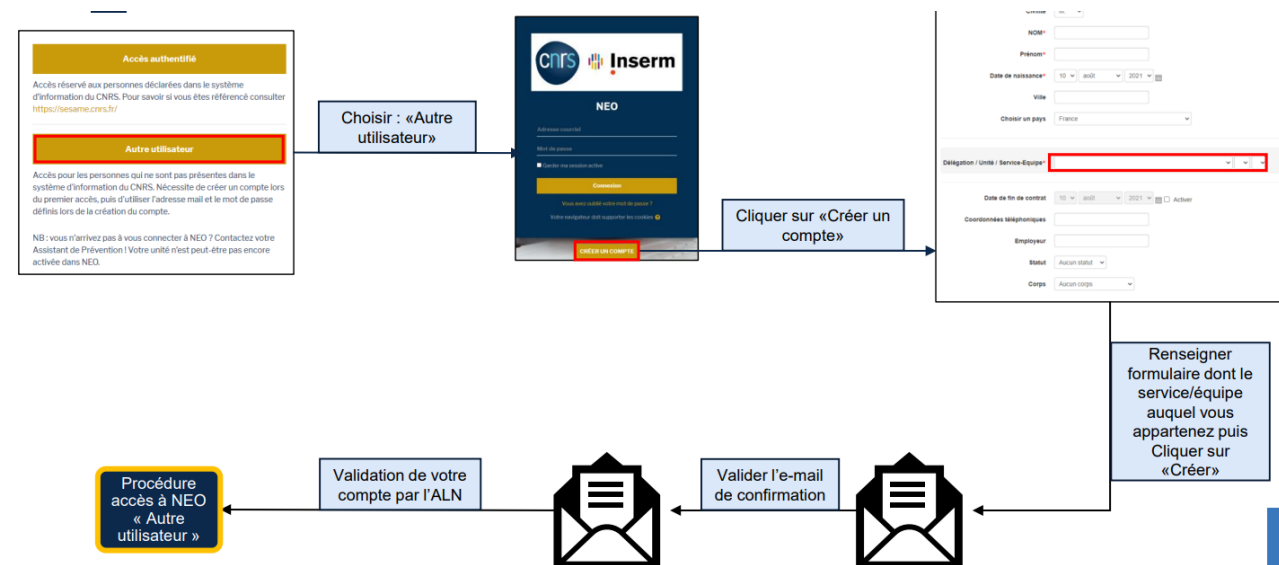


Figure 5 : Procédure de création d'un autre compte au CNRS

3.1.1.3 Les utilisateurs et leurs profils

Actuellement la déclaration des utilisateurs ayant des rôles de gestion dans NEO et l'attribution de leur profil s'effectue dans l'outil, manuellement, sans aucune mise à jour par un flux de données.

Il existe une exception au CNRS pour le Directeur d'unité qui crée directement avec le rôle dédié depuis le flux des structures.

Les profils selon leur rattachement sont associés à 3 périmètres de visibilité

- niveau établissement
- niveau régional
- niveau de l'unité

L'entrant : C'est celui qui intègre une unité ou structure et qui doit suivre un parcours de formation.

L'administrateur local de NEO (ALN) : il s'agit des assistants de prévention dans les unités. Ce sont les premiers interlocuteurs des nouveaux entrants. Ils administrent NEO au niveau de l'unité.

Le Consultant local de NEO (CLN) : il s'agit des directeurs d'unité qui ont des droits de consultation sur les données de leur unité, ou des acteurs partenaires de la prévention issus d'autres tutelles des unités.

L'administrateur régional de NEO (ARN) : Il s'agit du conseiller de prévention (Inserm) ou de l'IRPS (CNRS). C'est l'interlocuteurs des ALN. Il administre la plateforme au niveau régional. Il forme les ALN à NEO. Il active les structures de recherche désirant utiliser NEO et gère les comptes des ALN.

Le Consultant régional de NEO (CRN) : il s'agit des responsables formation en délégation qui ont des droits de consultation sur les données de leur délégation

L'administrateur National de NEO (ANN) : Il s'agit des acteurs de la Coordination nationale de Prévention et de Sécurité. C'est l'interlocuteurs des ARN. Il administre la plateforme au niveau national. Il forme les ARN à NEO et crée leurs comptes. Il définit les modules et l'offre de formation. Il administre le paramétrage de la plateforme et pilote l'assistance.

3.1.1.4 Présentation de NEO aux entrants

Extraits de plaquettes de présentation de l'application aux nouveaux entrants pour présenter et expliquer le contenu des modules et le mécanisme de validation des modules NEO :

Le bandeau de navigation

■ Présentation du bandeau de navigation

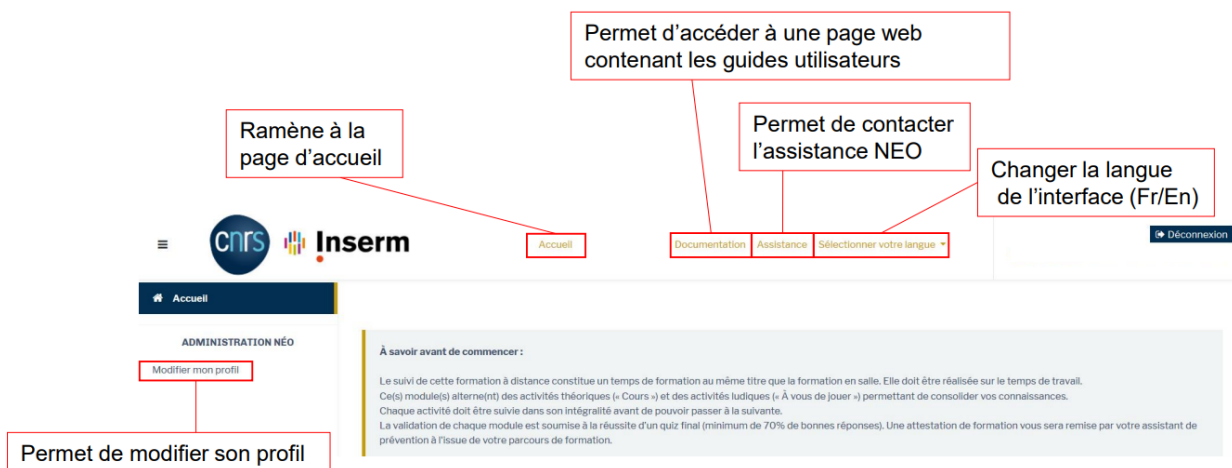


Figure 6 : Bandeau de navigation de NEO

La structuration des modules :

■ Module de formation

Composition du parcours :

- Alternance d'activités pédagogiques « cours » ① et d'activités ludiques « A vous de jouer » ②
- Un QCM ③

Principe de fonctionnement :

- Durée moyenne d'un module : 30 à 45 minutes.
- Les activités sont accessibles au fur et à mesure
- Le QCM n'est accessible qu'à la fin des cours et des activités ludiques.
- Vous avez 3 essais pour faire le QCM.
- Une note $\geq 70\%$ permet de valider le module.



Figure 7 : Structure des modules de NEO

■ Interface d'un cours :

Interface d'un cours

Chaque cours est composé de plusieurs slides, cliquer sur la barre de navigation pour changer de slide.

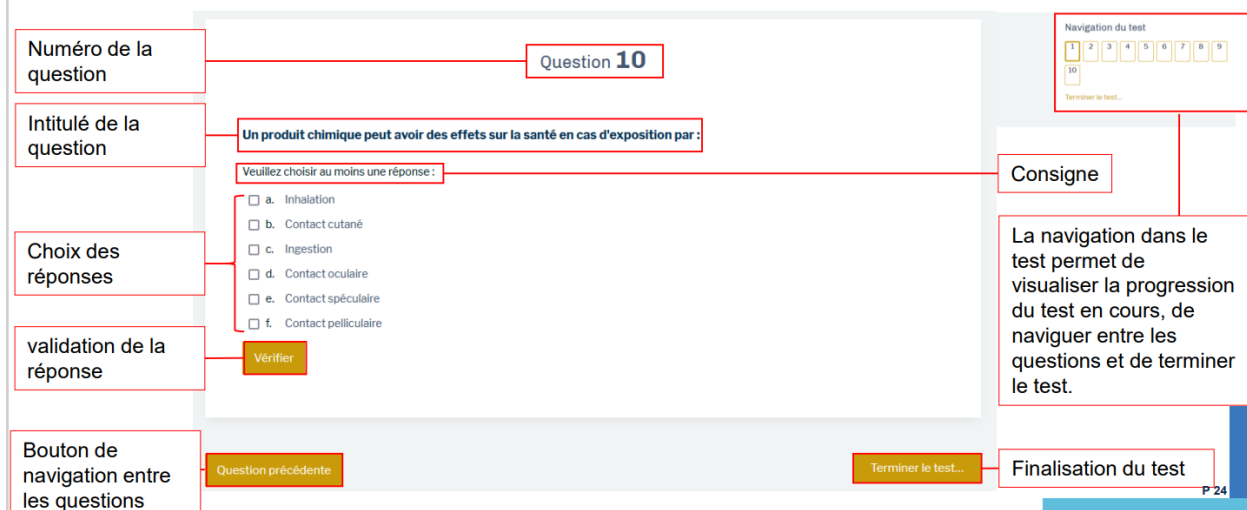


Figure 8 : Interface d'un cours de NEO

■ Interface du QCM de validation d'un module :

Interface du QCM

Chaque tests comportent 10 questions. Un score d'au moins 70% est requis pour valider le module. Vous bénéficiez de trois tentatives.



Interface du QCM

Après avoir répondu aux 10 questions, vous serez redirigé vers une page récapitulative, qui vous permet de vérifier que vous n'avez pas oublié de répondre à une question. Vous pouvez encore modifier la tentative à cet instant à l'aide du bouton « Retour à la tentative »

Si vous avez répondu à toutes les questions, cliquez sur « **Tout envoyer et terminer** ». Une fenêtre de confirmation va alors apparaître, il vous suffit de cliquer sur « **Tout envoyer et terminer** ».

Résumé de la tentative

Libellé de la question	État	Points
1	Incomplet	
2	Correct	1,00
3	Correct	1,00
4	Correct	1,00
5	Correct	1,00
6	Correct	1,00
7	Incorrect	0,00
8	Correct	1,00
9	Correct	1,00
10	Correct	1,00

Navigation du test

La navigation dans le test permet de visualiser les réponses non faites (blanc), bonnes (vert), fausses (rouge)

Absence de réponse/validation

Réponse correcte

Réponse fausse

Revenir au QCM

Envoi du QCM

Retour à la tentative

Tout envoyer et terminer

P 25

Score insuffisant au QCM - 3 tentatives sont épuisées

Si vous avez obtenu moins que 70% de bonnes réponses et que vous n'avez plus de tentative, contactez votre assistant de prévention qui fera le point avec vous.

Vous n'avez pas obtenu le score suffisant pour valider votre formation.

Il vous faut au moins 70% de bonnes réponses.

Attention vous n'avez que 3 tentatives. Si vous avez atteint le nombre de tentatives maximum, contactez votre Assistant de Prévention.

Aucune autre tentative n'est autorisée

[Retour au cours](#)

Obtenir mon attestation

Une fois que tous les modules accessibles ont été suivis (test compris), votre parcours de formation est considéré comme terminé.

Vous recevrez un message vous le confirmant la fin de votre parcours de formation.

Une attestation vous sera ensuite délivrée par votre Administrateur local NEO (assistant de prévention la plupart du temps) sur laquelle figurera des informations liées à l'entrant (nom, prénom, unité), les modules suivis, le temps consacré et la période sur laquelle a eu lieu cette formation.

Test
57 Avenue d'Azerex
65000

Attestation de formation / Training certificate

Je soussigné(e), Directeur du Test, atteste que / I, the undersigned, Director of Test, certify that:
a suivi le(s) module(s) de formation suivant(s) / has completed the following training course(s):

- Prévention
- Risque incendie
- Risque biologique
- Risque chimique

Cette formation équivaut à un volume horaire de 1h20min. / These courses represent 1h20min of training.

La formation réalisée sur l'application Neo s'est déroulée de 24/02/2016 à 24/02/2016. / The training was undertaken on the Neo application from 24/02/2016 to 24/02/2016.

Fait pour servir et valoir ce que de droit. / This certificate is issued for all legal purposes.

Directeur du Test /
Director of Test

Figure 9 : Interface du QCM de validation d'un module de NEO

3.1.1.5 Fonctionnalités disponibles aux ALN

Le Profil ALN est le principal acteur de NEO. L'application lui permet de piloter le suivi des formations dans NEO via le menu ci-dessous :



Figure 10 : Menu du profil ALN dans NEO

Les fonctionnalités suivantes sont mises à disposition :

- Gestion de l'arborescence des services/équipes de l'unité :

CONSULTATION SERVICES / EQUIPES			
Créer un service/équipe			
Services / Equipes	Membres	Date de création	Action
Equipe 1	3	jeudi 1 octobre 2020, 15:47	Action ▼
EQUIPE 2	3	jeudi 1 octobre 2020, 15:47	Action ▼
NEXS	0	vendredi 21 mai 2021, 15:40	Action ▼

Figure 11 : Gestion de l'arborescence des services/équipes de l'unité dans NEO

- Définition du parcours de formation par défaut de l'unité :

DÉFINITION DU PARCOURS PAR DÉFAUT

Sélection de l'unité / service

Délégation: DR14 - Occitanie Ouest (Ex Midi-Pyrenees) Unité: MOY1400 Service: Equipe 1 Sélectionner

Module	Actif
Prévention	<input checked="" type="checkbox"/>
Risque biologique	<input checked="" type="checkbox"/>
Risque incendie	<input type="checkbox"/>
Risque chimique	<input type="checkbox"/>
Bac a sable	<input type="checkbox"/>
Risque électrique 2	<input type="checkbox"/>

Figure 12 : Définition du parcours de formation par défaut de l'unité dans NEO

- Paramétrage du délai des relances envoyées aux nouveaux entrants

PARAMÈTRES DES MESSAGES DE RELANCE

▼ Relances de parcours à terminer pour les entrants

MOY1400 - Périodicité des relances ⓘ semaines ▼

Remarque : le paramètre de relance doit être supérieur à 1 jour. La définition des minutes et des secondes est inutile car non prise en compte par le traitement.

▼ Récapitulatif hebdomadaire ALN

☒ Recevoir un récapitulatif hebdomadaire par courriel

Modifier Annuler

Figure 13 : Paramétrage du délai des relances envoyées aux nouveaux entrants dans NEO

- Gestion des ressources documentaires locales associées à chaque module :

Module: Bac a sable


Langue: FR

Envoyer

Ajouter un document

Délégation / Unité: DR14 - Occitanie Ouest (Ex Midi-Pyrenees) --Sélectionner unité--

Choisir un fichier... Taille maximale des nouveaux fichiers : 600Mo



Plaqueette_Neo_ALN_oct2021.pdf - Vous pouvez glisser des fichiers ici pour les ajouter.

Envoyer

Documents

Fichier	Niveau	Action
Guide risques radioactifs et radioprotection v-01-2018.pdf	National	

Figure 14 : Gestion des ressources documentaires locales associées à chaque module dans NEO

■ Validation des comptes des entrants auto-inscrits

▼ Filtrer les entrants

Délégations

DR14 - Occitanie Ouest (Ex Midi-Pyrenees)

▼

MOY1400 -

▼

--Sélectionner service--

▼

Nom

Prénom

Adresse de courriel

État

--Sélectionner état--

▼

Afficher plus...

Actualiser la recherche

Remettre à zéro

Nombre de résultats : 9 / 9

Nombre de résultats par page : 20

Services / Equipes	Civilité	Nom	Prénom	Adresse courriel	Date de naissance	Date de création du compte	Date de fin de contrat	État ^	Action
EQUIPE 2	M.					22/02/2023		En attente	Action ▼
Equipe 1	M.	test	import	test.import@cnrs.fr	01/01/2000	24/03/2023	10/10/2024	Données confirmées	Action ▼

Figure 15 : Validation des comptes des entrants auto-inscrits dans NEO

■ Ajustement et suivi du parcours de formation de chaque entrant

CONSULTATION DES SESSIONS

Date de début :

Date de fin :

Nom :

Type de formation :

▼

État session :

▼

Statut session :

▼

Délégation :

--Sélectionner délégation--

▼

Unité :

--Sélectionner unité--

▼

Service :

--Sélectionner service--

▼

Statut unité :

▼

Envoyer

Remettre à zéro

Nombre de résultats : 10 / 10

Nombre de résultats par page : 20

Légende des modules

Module non commencé

Module débuté

Module terminé

Test non réalisé ou en cours

Test réussi

Score insuffisant au test

Validé par un ALN

Prénom	Adresse courriel	Date de création de la session	Date de fin de session	Type de formation	La prévention	Le risque biologique	Le risque incendie	Le risque chimique	Le risque électrique 2	Attestation	État session	Statut session	Langue	Statut unité
Colette		13/10/2022	27/10/2022	Individuel						Imprimer	Attestation	Activée	EN	Activée
Dzazira		30/05/2022		Individuel	À réaliser ▼						Créée	Activée	EN	Activée

Figure 16 : Ajustement et suivi du parcours de formation de chaque entrant dans NEO

- Impression des attestations pour signature du Directeur



Le 05/05/2023

import test

Délégation Occitanie Ouest (- MOY1400)

16 Av Edouard Belin
31055 TOULOUSE CEDEX 4**Attestation de formation / Training certificate**

Je soussigné(e), Directeur(trice) de la structure, atteste que / I, the undersigned, Director of structure, certify that:

import test a suivi le(s) module(s) de formation suivant(s) / has completed the following training course(s) :

- Prévention
- Risque chimique
- Risque électrique 2

Cette formation équivaut à un volume horaire de 2h15min. / These courses represent 2h15min of training.

La formation réalisée sur l'application Neo s'est déroulée du 24/03/2023 au 05/05/2023. / The training was undertaken on the Neo application from 24/03/2023 to 05/05/2023.

Fait pour servir et valoir ce que de droit. / This certificate is issued for all legal purposes.

Directeur(trice) / Director

Figure 17 : Attestation pour signature du Directeur dans NEO

- Export des données pour archivage annuel.
- Export CSV des sessions à effectuer

3.1.1.6 Fonctionnalités disponibles aux ARN

Les ARN disposent des mêmes fonctionnalités et peuvent aussi :

- Définir la mise à disposition des modules au sein de leur délégation pour certaines unités

GESTION DES MODULES

Remettre à zéro							
Page: 10							
	Nom du module	Id cours français	Id cours anglais	Date de fin	Durée	État	Action
<input type="checkbox"/>	Prévention	44	45		45	Activé	Action ▼
<input type="checkbox"/>	Risque biologique	36	35		45	Activé	Action ▼
<input type="checkbox"/>	Risque incendie	46	47		45	Activé	Action ▼
<input type="checkbox"/>	Risque chimique	38	37		45	Activé	Action ▼
<input type="checkbox"/>	Bac a sable	69	69		0	Activé	Action ▼
<input type="checkbox"/>	Aptilink	31	31		0	Désactivé	Action ▼
<input type="checkbox"/>	Risque électrique 2	81	81		45	Activé	Action ▼

Figure 18 : Gestion des modules pour une délégation dans NEO

■ Gérer les unités de leur délégation :

Créer une nouvelle unité

Réinitialiser les réglages du tableau

1

2

3

4

5

»

	Identifiant	Sigle de l'unité	Nom de l'unité	Nom du responsable	Courriel du responsable	Nombre d'ALN	Date de début	Date d'activation	Date de fin	État	Actions
<input type="checkbox"/>	GDR3762	THEOMODIVE	Théorie et Modélisation de la Biodiversité			0	01/01/2016	07/07/2021		Activée	Action
<input type="checkbox"/>	UMR5152	LPT	Laboratoire de physique théorique			1	01/01/2003	07/07/2021		Activée	Action
<input type="checkbox"/>	UMR5589	LCAR	Laboratoire Collisions Agrégats Réactivité			1	01/01/1995	07/07/2021		Activée	Action
<input type="checkbox"/>	EMR3649	TESTMPP	TEST de l'EMR3649			0	16/02/2018	07/07/2021	16/02/2023	En instance de fermeture	Action
<input type="checkbox"/>	UMR5626	LCPQ	Laboratoire de Chimie et Physique Quantiques			1	01/01/1995	07/07/2021	05/01/2023	En instance de fermeture	Action
<input type="checkbox"/>	UMR5100	LMGM	Laboratoire de Microbiologie et de Génétique Moléculaires			0	01/01/1999	07/07/2021		Activée	Action
<input type="checkbox"/>	UMR5219	IMT	Institut de Mathématiques de Toulouse			0	01/11/2006	07/07/2021		Activée	Action
<input type="checkbox"/>	GDR3070	CELLTISS	Physique de la cellule au tissu			0	01/01/2007	07/07/2021		Activée	Action
<input type="checkbox"/>	UMR5302	RAPSODEE	Centre de recherche d'Albi en génie des procédés des solides divisés, de l'énergie et de l'environnement			6	01/01/2012	07/07/2021		Activée	Action

Figure 19 : Gestion des unités d'une délégation dans NEO

3.1.1.7 Fonctionnalités disponibles aux ANN

Le profil ANN pilote l'administration de NEO via le menu ci-dessous qui reprend certaines fonctionnalités déjà citées et d'autres spécifiques à ce rôle.

Figure 20 : Menu du profil ANN dans NEO

Les référentiels utilisés dans NEO portent sur :

- Les modules (en français et anglais)
- Les unités ou structures – mise à jour via un flux au CNRS
- Les délégations
- Les corps administratifs
- Les statuts de personnels

- Les entrants
- Les questionnaires

Chacun est éditable manuellement via ou peut faire l'objet de mise à jour via un import csv

Ce profil n'a pas accès à l'administration du site NEO, dédiée à un profil administrateur.

3.1.1.8 Fonctionnalités d'administration pilotées par le CNRS/Inserm

Le titulaire préétablit tous les paramétrages de la solution dans le cadre des prestations demandées et les met à disposition via des livraisons pour une installation par les soins du CNRS et de l'Inserm.

L'activation de nouvelles fonctionnalités relevant du paramétrage Moodle ne s'effectue pas de façon autonome par les établissements CNRS et Inserm qui n'ont pas alloué de compétences sur la technologie Moodle en vue d'une autonomie. Toutes ces opérations sont déléguées au titulaire.

Cependant le profil Administrateur tel qu'il est pratiqué au CNRS et à l'Inserm intervient sur certains paramétrages pour les aspects suivants :

- Le paramétrage du mode connexion et des informations de la page d'accueil
- La personnalisation de tous les emails émis en français et en anglais via un block dédié à NEO
- La conception de nouveaux modules en anglais et en français en lien avec le plugin H5P depuis charte graphique mise en place pour structurer la présentation des cours de façon homogène
- La mise à disposition de ces modules à tous avec la possibilité de définir un périmètre d'accessibilité de ces modules pour des accès restreints (cas des modules destinés à la formation des Assistants de prévention)
 - La planification des tâches (gestion des imports de flux des entrants et des structures ; batch de mise à jour des statuts des sessions ; purge annuelle avec un envoi de l'export csv à chaque ALN pour son unité).

3.1.2 Intégration dans le SI

3.1.2.1 Principes d'authentification

- **Authentification CNRS** : NEO est interfacé avec le SSO Shibboleth pour permettre une authentification des personnels référencés dans l'annuaire LDAP du CNRS afin de filtrer les connexions via le mode authentifié sur les populations autorisées. (cf. § 2.3.3.3).
- Au CNRS Une authentification par couple email/mot de passe interne à NEO est également possible pour permettre aux entrants des unités non référencés dans RESEDA de suivre leur parcours de formation dès leur arrivée dans les laboratoires. Cette modalité d'accès permet aussi à l'administrateur de NEO de se connecter .
- **Authentification Inserm** : NEO est interfacé avec un CAS (Central Authentication Service).

3.1.2.2 Flux échangés

- **Un flux des entrants au format .CSV** est déposé tous les matins sur le serveur de NEO et intégré par un batch dans les applications NEO du CNRS et de l'Inserm.

Au CNRS : ce flux est généré par un script python maintenu par le CNRS appelant le Webservice (WS) de la collection des personnels.

Ce WS est exposé par la brique des WS Mongo à partir du gestionnaire des données de référence du CNRS, RESEDA (cf. § 2.3.3.2).

Ce flux permet de récupérer uniquement les personnels récents selon un filtrage défini dans le script.

Ce flux quotidien ne récupère pas l'ensemble des personnels mais uniquement ceux mis à jour dans le SI du CNRS depuis la veille. Il s'agit d'un flux différentiel qui vient soit créer dans NEO de nouveaux entrants ; soit les mettre à jour si leurs données sont modifiées. Ce flux ne supprime aucun utilisateur dans NEO, cette action étant le fait de la purge annuelle.

A l'Inserm : ce flux est généré selon une autre solution locale.

- **Un flux des structures au format .CSV** est déposé tous les matins sur le serveur de NEO et intégré par un batch.

Ce flux est généré par un script python maintenu par le CNRS appelant le WS de la collection des structures.

Ce WS est aussi exposé par la brique des WS Mongo à partir du gestionnaire des données de référence du CNRS (cf. § 2.3.3.2). Il est également différentiel pour ne récupérer que les structures modifiées depuis la veille.

Il crée ou met à jour les unités modifiées ou restructurées.

NB : l'Inserm n'a pas mis en place un tel flux. Il s'agit d'une spécificité CNRS.

Au CNRS, un nouveau flux sera à mettre en place pour récupérer les profils AP (ALN dans NEO) dérivés des fonctions métiers (transmises via le WS des utilisateurs - cf. § 2.3.3.3) des Assistants de Prévention depuis le gestionnaire des accès et habilitations (IAM - cf. § 2.3.3.4) pour disposer d'une gestion automatisée de la création/gestion/suppression de ces profils dans les unités associées dans NEO.

3.1.3 Présentation technique

Le public visé est large et le parc machines est fortement hétérogène.

Neo est une plateforme Moodle comportant des développements spécifiques en PHP.

Elle est distribuée sous forme d'un site web afin d'être facilement utilisable par le plus grand nombre.

L'application respecte les normes HTML5 et CSS3, et doit prendre en compte le javascript et d'autres technologies côté navigateur.

L'application est supportée par les versions récentes des principaux navigateurs

3.1.3.1 Logiciels du serveur applicatif (VM)

Nature	composant	Version	Commentaire
OS	Redhat	9	
Logiciel	Apache	2.4.37	
Logiciel	PHP	8.1	
Logiciel	Moodle	4.1.15	

3.1.3.2 Logiciels du serveur de base de données (VM)

Nature	Logiciel	Version	Commentaire
OS	RedHat	9	
BD	PostgreSQL	16	

3.1.3.1 Logiciels des 2 serveurs proxy

Nature	Logiciel	Version	Commentaire
OS	RedHat	9	

3.1.3.1 Caractéristiques serveurs

3.1.3.1.1 Environnement de production

Fonction	CPU	RAM	DD	Divers
PROD – AS	Quadcore 2GHz minimum	2 Go	150 Go	VM
BDD	Dualcore 2GHz minimum	6 GO	20 GO	VM

3.1.3.1.2 Environnement de recette

Fonction	CPU	RAM	DD	Divers
REC – AS	Quadcore 2GHz minimum	2 Go	150 Go	VM
BDD	Dualcore 2GHz minimum	6 GO	20 GO	VM

3.2 VOLUMETRIE

3.2.1 Volumétrie des versions

L'application a atteint un stade de maturité et fait l'objet d'une moyenne de 3 versions livrées par an.

3.2.2 Volumétrie des anomalies

L'application a donné lieu à la gestion des anomalies³ correctives suivantes dans le cadre du MCO en production.

Les régressions ou anomalies émanant des itérations corrective d'une version livrée ne sont pas comptabilisées.

L'année considérée est l'année de résolution de l'anomalie.

	2021	2022	2023	2024
Anomalies bloquantes	1	3	1	
Anomalies majeures	4	4	1	1
Anomalies mineures	4	4	2	1
Tickets de support	5	4	2	2

3.2.3 Volumétrie des évolutions

L'application a donné lieu au nombre de version évolutives suivantes sur les 3 dernières années, sans compter les versions correctives ou les itérations associées à une version.

	2021	2022	2023	2024
Nombre de versions	4	3	2	2
Nombre de jours de réalisation	Environ 40	Environ 40	Environ 20	Environ 20

3.3 DIMENSIONNEMENT DE L'APPLICATION

Eléments	dimensionnement
Nombre de règles de gestion	<100
Nombre de tables	Environ 15
Nombre d'écrans	Environ 30
Nombre d'état	Environ 10
Nombre d'interfaces avec les autres applications	3
Maturité de l'application	mise en production en 2016

³ La définition et la typologie des anomalies sont décrites dans le glossaire du Livret 2 du CCTP.

3.4 EVOLUTIONS FUTURES IDENTIFIEES :

Les principales évolutions identifiées à ce jour portent sur les points suivants :

- Migrations techniques tous les 2 ans des composants trop anciens
- Amélioration de la gestion des actions récurrentes
- Amélioration continue des interfaces et fonctionnements de l'outil
- Mise en place d'un flux pour une gestion automatisée des AP
- Mise en place de fonctions de statistiques pour aider au pilotage des actions de formation en Prévention
- Amélioration/Intégration de nouveaux modules de formation de Prévention produits par le CNR/Inserm
- Réalisations graphiques pour valoriser les modules
- Rendre l'application Accessible

4 CADRE DE COHERENCE TECHNIQUE DE LA SOLUTION

Ce chapitre donne les exigences applicables à tout nouveau développement, que ce soit lors de la mise en œuvre d'une nouvelle application ou dans le cadre d'évolutions d'une application existante.

Ces exigences CNRS sont le plus souvent partagées avec l'Inserm

4.1 EXIGENCES D'INTEGRATION DANS LE SI

L'architecture de la solution est et sera compatible avec l'architecture générale du SI du CNRS et celle de l'Inserm.

4.1.1 Répartition fonctionnelle

Référence	Libellé exigence	Priorité
URB_003	Pour assurer que l'architecture des solutions nationales va dans le sens d'une répartition urbanisée des fonctionnalités entre les applications selon le principe de cohérence fonctionnelle et informationnelle forte, l'équipe projet doit faire valider son périmètre fonctionnel et informationnel par l'équipe urbanisation de la DSI.	1
URB_004	Lors de la conception et de la réalisation de la solution, les architectures transverses nationales et pilotées par la DSI sont privilégiées, entre autres par l'utilisation des plateformes mutualisées et la réutilisation des briques applicatives (notion de service, voire micro-service). Ceci afin de ne pas implémenter ou développer une fonction ou un contrôle métier déjà outillé dans une autre application ou service.	1
URB_005	Lors de la conception et de la réalisation de la solution, les fonctions restant à développer pour la solution sont prévues autant que possible pour être mutualisées, voire transformées en (micro-)services utilisables par d'autres applications.	1
URB_006	L'architecture de la solution découple les fonctionnalités « Etablissement » des fonctionnalités « Laboratoire » dans des modules applicatifs distincts qui proposent des services web (type REST) permettant une communication, entre ces fonctionnalités, par demi-flux via des formats pivots.	1

4.1.2 Echanges de données

4.1.2.1 Modalités générales

Les futures interfaces entrantes ou sortantes entre la solution et les autres applications du SI peuvent s'effectuer de plusieurs façons dont voici les principales : échanges de fichiers (XML, CSV, ...), échanges de messages (Broker), et services Web de type REST, tout en passant systématiquement par un des systèmes d'intermédiation du CNRS (cf. § 2.3.3.1).

L'objectif du CNRS et de l'Inserm est la mise en œuvre du principe de couplage faible entre les systèmes d'intermédiation et l'application.

Les échanges de données entre le gestionnaire d'échanges et de services CNRS ou Inserm et la solution NEO (flux entrants et flux sortants), se font au travers d'une couche d'abstraction (matérialisée par des services) pour permettre au gestionnaire d'échanges et de services CNRS ou Inserm d'assurer la gestion chronologique des échanges (quotidien, à la demande, ...) tout en disposant de services, portés par la solution NEO, appelables par le gestionnaire d'échanges et de services CNRS ou Inserm à tout moment (en journée, en traitement batch).

Dans le cas des flux par appel de services web, le passage par le gestionnaire d'échanges et de services du CNRS n'est pas obligatoire, toutefois, afin de garder un découplage des échanges, ces appels de services web passent à travers un proxy de service web (de manière transparente pour l'application appelante). Dans certains cas justifiés, la mise en œuvre des services web peut être réalisée via le gestionnaire d'échanges et de services du CNRS ou Inserm.

Au final, la solution d'échange pour chacun des flux est définie conjointement avec le CNRS et l'Inserm dans le cadre d'ateliers de travail dans la limite des règles prévalant au CNRS et à l'Inserm sur l'intégration des SI.

Pour les flux entrants, le CNRS et l'Inserm, qui appliquent les mêmes principes d'échange de données, déterminent et mettent à disposition, en fonction des besoins, les données échangées nécessaires à la solution NEO.

Cependant dans le cas où certains flux entrants sont à développer par le CNRS et par l'Inserm pour les besoins spécifiques de la solution, le titulaire doit déterminer son besoin au plus tôt, ajuster son planning le cas échéant, pour permettre au CNRS/Inserm la mise à disposition du nouveau flux avant la livraison de la solution. Une étude de faisabilité et des spécifications détaillées seront nécessaires.

Référence	Libellé exigence	Priorité
URB_007	<p>Le titulaire prévoit le bon fonctionnement et la continuité de service fonctionnel de la solution qu'il développe, y compris des éventuels outils d'intégration proposés, au regard de l'architecture générale du SI, et en particulier vis-à-vis des systèmes d'intermédiations retenus au CNRS.</p> <p>En particulier, la solution :</p> <ul style="list-style-type: none"> tient compte des arrêts de services de la solution, avec éventuellement l'émission d'un message de non disponibilité, afin de ne pas provoquer d'erreur (technique) pour les services appelants ; prend en compte et pallie la non réponse d'un service appelé en passant, par exemple, dans un mode dégradé non bloquant. 	1
URB_008	Si la solution fait appel à des services fonctionnels portés par un autre SI ou application, ou met à disposition des services fonctionnels, la gestion de ces communications passe par les systèmes d'intermédiation du CNRS, sauf exception justifiée et décidée conjointement entre le titulaire et le CNRS.	1
URB_009	La solution a la responsabilité de réaliser les services d'intégration des données et les services d'exposition des informations dont elle est propriétaire.	1
URB_010	Les échanges entre la solution et le reste du SI se font via des formats pivots.	1
URB_011	Les formats pivots non fournis par le CNRS sont de préférence basés sur des formats pivots existants et reconnus par la communauté.	1
URB_012	Les formats pivots sont facilement évolutifs en limitant les impacts sur leurs usages déjà en cours.	1
URB_013	Le formalisme de description des formats pivots est celui prescrit par la DSI du CNRS.	1
URB_014	<p>Si la mise en œuvre d'échange nécessite la transcodification de certaines données (nomenclatures par exemple), celle-ci est effectuée par les systèmes d'intermédiation au cours du flux, à partir de tables de transcodification administrées par le gestionnaire de données de référence (MDM) du CNRS.</p> <p>Les systèmes d'intermédiations prennent seulement en compte une transcodification simple, de type valeur ou groupe de valeur vers une autre valeur, sans application de règles métier. Celles-ci sont éventuellement mises en place dans le gestionnaire de données de référence du CNRS qui héberge les tables de transcodification.</p> <p>A noter que si les échanges se font via les services web, ces derniers ne réalisent aucune transcodification.</p>	2
URB_015	La solution va chercher les objets métiers, dont elle a besoin et en récupère, au moment où elle en a besoin, uniquement la population qui l'intéresse et uniquement le sous-ensemble des caractéristiques (partie du format pivot) qui lui est nécessaire. Autrement dit, seules les données / objets métiers nécessaires sont présents dans les flux entrants de la solution.	1
URB_016	En fonction des éléments d'analyse, le titulaire détermine l'ensemble des données strictement nécessaires dans le cadre de données personnelles (contrainte du règlement européen sur la protection des données – RGPD), au bon fonctionnement de la solution.	1
URB_017	<p>L'utilisation de données extérieures à la solution n'implique pas un stockage de ces données dans la solution.</p> <p>Aussi, la nécessité de stocker les données externes dans la solution doit être étudiée et validée entre le titulaire et le CNRS (équipes projet et transverses).</p>	1

Référence	Libellé exigence	Priorité
URB_018	Pour chaque objet métier dont la solution est propriétaire, un service d'exposition permet : <ul style="list-style-type: none"> ■ une diffusion au fil de l'eau des objets métier modifiés par la solution ; ■ et/ou, éventuellement, une diffusion sous forme de flux à la demande ; ■ un flux complet ou différentiel sur des critères à définir en conception détaillée (<i>par exemple, uniquement sur les objets modifiés depuis l'envoi précédent, uniquement un sous ensemble des objets métier, uniquement un objet métier donné</i>). ■ Une sélection des objets métier et/ou une partie de leurs caractéristiques, en fonction de critères à définir en conception détaillée 	1
URB_019	La solution expose toute la population des objets métiers dont elle est maître, avec le contenu complet du format pivot (FP), y compris les règles de diffusion, et/ou niveau de sensibilité. Autrement dit, la solution ne fait aucune restriction sur l'exposition des objets métiers qu'elle gère.	1
URB_021	Pour les objets métier dont la solution est propriétaire, et pour lesquels il y a une utilité, un service de recherche permet une recherche approchante, sur des caractéristiques à définir en conception détaillée.	2

4.1.2.2 Modalités d'implémentation

Les flux d'échange de données doivent techniquement adopter les règles d'implémentation suivantes :

Référence	Libellé exigence	Priorité
ECH_001	Les échanges inter-applicatifs passent par les systèmes d'intermédiation du CNRS. La solution ne communique qu'avec ces systèmes d'intermédiation, quel que soit le flux entrant ou sortant et propose des services permettant d'interagir avec eux.	1
ECH_002	La solution produit et reçoit des informations préformatées au format pivot défini par le CNRS. Les systèmes d'intermédiation ne portent pas les règles de gestion métier.	0
ECH_003	L'interfaçage avec les systèmes d'intermédiation est effectué via des services web du type REST. Pour la diffusion de ses données au reste du SI, la solution privilégie un appel à un service web CNRS de diffusion des données.	1
ECH_004	La fréquence de publication des données est faite au fil de l'eau, de façon quotidienne ou hebdomadaire.	1
ECH_005	L'encodage préconisé est UTF-8. Les formats utilisés pour les échanges de données sont XML, JSON et CSV, mais ces formats ne sont pas limitatifs. Le référentiel général d'interopérabilité (http://references.modernisation.gouv.fr/interopabilite) gouverne le choix des formats.	1
ECH_006	Seuls des protocoles de transport de données chiffrés sont utilisés comme par exemple les protocoles « SSH » (scp, sftp, etc). Se référer au RGS 2.0 annexes B1, B2 et B3 pour les versions des protocoles et algorithmes de chiffrement autorisés (https://cyber.gouv.fr/le-referentiel-general-de-securite-version-20-les-documents)	0
ECH_007-a	Pour tous les types de flux, la confidentialité des données transmises est garantie. Les moyens techniques utilisés sont décrits dans la documentation.	0
ECH_007-b	Pour tous les types de flux, l'intégrité des données transmises est garantie. Les moyens techniques utilisés sont décrits dans la documentation.	0
ECH_007-c	Pour tous les types de flux, l'unicité des requêtes est garantie pour éviter les rejeux. Les moyens techniques utilisés sont décrits dans la documentation.	0
ECH_007-d	Pour tous les types de flux, l'identité du client et du serveur de communication est garantie. Les moyens techniques utilisés sont décrits dans la documentation.	0

Référence	Libellé exigence	Priorité
ECH_008	Pour assurer la confidentialité et l'intégrité des données lors des échanges, le chiffrement des données en supplément du chiffrement des protocoles de transport (cf. ECH_006) est une mesure de protection dont l'opportunité est jugée au regard de la sensibilité. Ce chiffrement est réalisé à la source et le déchiffrement à la destination, sans possibilité d'interception par les systèmes d'intermédiation et de transport selon les normes de chiffrement en vigueur (cf. annexe B du RGS : https://cyber.gouv.fr/le-referentiel-general-de-securite-version-20-les-documents). Il est cependant toléré que le système d'intermédiation du CNRS assure le chiffrement en cas d'impossibilité de le réaliser à la source.	0
ECH_009	L'authentification des appels à un service web, de type REST, est réalisée soit par certificat, soit par identifiant/mot de passe stocké de manière confidentielle.	0
ECH_010	Lorsque que l'usage d'un broker est nécessaire, c'est celui du gestionnaire d'échange et de services du CNRS, via son API (JMS de préférence) qui est utilisé.	1

4.1.3 Authentification, **comptes** utilisateurs

Les services d'authentification CNRS (cf. § 2.3.3.3) sont disponibles sur plusieurs environnements :

- production : réservé à la production de la solution,
- recette : réservé à la recette de la solution,
- formation : réservé à la formation de la solution,
- test : seul environnement accessible au titulaire, ne contenant pas de données réelles et dont l'objectif est de permettre au titulaire de valider les aspects techniques liés aux briques d'authentification.

Le titulaire assure les développements applicatifs nécessaires pour s'interfacer avec le(s) fournisseur(s) d'identité du CNRS (cf. § 2.3.3.3). Si plusieurs fournisseurs peuvent être choisis, un WAYF doit être mis en place.

Pour les applications hébergées sur les infrastructures propres de la DSI du CNRS, le CNRS peut mettre en place un service intégré de service provider (SP) SAML 2.0 et de WAYF, de technologie Shibboleth3.

Le titulaire reste responsable de la solution mise en œuvre qui doit respecter les principes de fonctionnement suivants :

- L'application délègue l'authentification des utilisateurs au fournisseur d'identité du CNRS (cf. § 2.3.3.3).
- Une fois le client SAML intégré à l'application, ce sont les fournisseurs d'identité qui se chargent d'authentifier l'utilisateur CNRS.
- L'authentification des utilisateurs par les services d'authentification CNRS est possible soit par certificats (AC CNRS / TCS), soit par email/mot de passe (en se basant sur les informations contenues dans le référentiel des comptes utilisateurs du CNRS, soit avec une solution d'authentification multi-facteurs.
- Le navigateur est toujours redirigé vers le fournisseur d'identité CNRS et c'est ensuite, lors de l'authentification sur ce fournisseur d'identité, que l'utilisateur peut fournir ses identifiants et authentifiants.
- Une fois l'utilisateur authentifié auprès du fournisseur d'identité CNRS, le navigateur de l'utilisateur envoie à l'application l'identifiant opaque dans un message SAML. Ce jeton contient aussi des attributs de l'utilisateur authentifié. La liste des attributs diffusés est spécifique à chaque application et limitée à ses besoins.
- Le contrôle d'accès à l'application effectué par le fournisseur d'identité CNRS se limite à dire si les informations d'authentification de l'utilisateur sont correctes. Il atteste juste que l'utilisateur est référencé dans le SI du CNRS. L'application doit assurer elle-même son contrôle d'accès à partir des rôles et droits applicatifs gérés dans l'application. Si nécessaire, les droits et profils applicatifs associés sont stockés dans la base de l'application.
- Le service provider (SP) fourni par la DSI du CNRS peut restreindre l'accès à l'application sur la base d'attributs retournés par le fournisseur d'identité.
- Le critère d'accès est donc l'appartenance ou non de l'utilisateur au référentiel des comptes utilisateurs du CNRS.
- Dans le cas d'une gestion des droits déléguée à la brique de gestion des accès et habilitations du CNRS (cf. § 2.3.3.4), les rôles applicatifs peuvent être gérés et calculés de manière centralisée. Ces rôles applicatifs sont disponibles dans les services web des données des utilisateurs. Dans certains cas ils peuvent aussi être transmis à l'application lors de l'authentification. Les droits fins sont stockés et gérés dans la solution.

Référence	Libellé exigence	Priorité
AUTH_001-a	L'authentification à la solution se fait à partir du fournisseur d'identité CNRS pour les utilisateurs des unités CNRS et sinon au moyen de la fédération Renater.	1
AUTH_001-b	Pour les utilisateurs qui ne sont présents ni dans le fournisseur d'identité CNRS, ni dans la fédération Renater, le CNRS étudie les modalités de gestion des comptes. L'utilisation de comptes locaux n'est possible que sur autorisation expresse du CNRS.	1
AUTH_002-a	Dans le cas de comptes locaux, la solution comprend des fonctionnalités de gestion de ces comptes.	0
AUTH_002-b	Dans le cas de comptes locaux, les mots de passe ne sont jamais stockés en clair mais dans une forme transformée par une fonction cryptographique non réversible conforme au Référentiel Général de Sécurité (https://cyber.gouv.fr/le-referentiel-general-de-securite-rqs) et la transformation des mots de passe fait intervenir un sel aléatoire.	0
AUTH_003	Un service de découverte (WAYF) est mis en place lorsque le fournisseur d'identités CNRS n'est pas le seul fournisseur d'identité utilisé.	0
AUTH_004	La création d'un compte utilisateur pour accéder à la solution est effectuée par un mécanisme de provisioning et non par saisie manuelle. Le provisioning peut être effectué via l'utilisation du service web qui expose le référentiel des comptes utilisateurs (annuaire référentiel du CNRS), à la demande ou au fil de l'eau ou encore via les informations issues de l'authentification. La création automatique de compte sur demande de l'utilisateur directement dans l'application est interdite.	1
AUTH_005	Pour les personnels présents dans les unités du CNRS, l'origine des données pour la création et la modification des comptes utilisateurs est l'annuaire référentiel du CNRS.	0
AUTH_006	Un mécanisme de gestion du cycle de vie des comptes utilisateurs de la solution est mis en place.	1
AUTH_007	La modification d'un compte utilisateur dans la solution est effectuée via des services web ou via les systèmes d'intermédiation du CNRS.	1
AUTH_008	Les phases d'identification et d'authentification sont séparées de l'ensemble des actions applicatives de l'utilisateur dès la conception de la solution afin de permettre la plus grande modularité possible, et donc une facilité, quant au choix du mécanisme d'identification et d'authentification.	1
AUTH_009	Le contrôle d'accès à l'application est renforcé directement sur le reverse proxy hébergeant le Service Provider par la vérification d'un attribut spécifique exposé par le référentiel des comptes pour refuser l'accès aux utilisateurs authentifiés qui n'auraient pas de droits sur l'application. Dans ce cas, une page d'erreur spécifique est à prévoir pour indiquer de manière claire à l'utilisateur qu'il n'a pas les droits nécessaires pour accéder au service/à l'application. Ce contrôle s'ajoute mais ne se substitue pas aux contrôles de droits des utilisateurs réalisés par l'application.	1

Référence	Libellé exigence	Priorité
HAB_001	La solution permet de définir différents rôles applicatifs selon les fonctions métier et les responsabilités des utilisateurs.	0
HAB_002	La solution permet de définir des rôles applicatifs en fonction des fonctions métier et du domaine d'appartenance, ainsi que des accès associés (lecture, écriture, etc.). Ces rôles sont associés à des périmètres correspondant au besoin et/ou au droit d'en connaître pour les populations considérées.	1
HAB_003	La solution permet de définir ou provisionner des comptes d'accès permanents et temporaires (définition d'une date de début et une date de fin de la validité du compte).	1
HAB_004	La solution permet la désactivation des comptes utilisateurs.	0
HAB_005	Lorsque des comptes par défaut existent, il doit être possible de les désactiver, les renommer, modifier le mot de passe ou les supprimer sans impact sur l'application.	1

4.1.4 Stockage des documents

La règle ci-dessous n'est pas actuellement en place mais pourrait devenir un objectif d'évolution

Référence	Libellé exigence	Priorité
DOC_001	Les documents gérés par la solution sont stockés sur la plateforme de GED du CNRS. Dès lors, les fonctionnalités d'ajout/modification/lecture/suppression de documents invoquées depuis la solution sont réalisées à travers des services web proposés par la GED du CNRS par l'intermédiaire des systèmes d'intermédiation.	1

4.2 EXIGENCES TECHNIQUES

4.2.1 Eléments techniques structurants

L'application est une application ouverte sur Internet avec des utilisateurs y accédant pour certains par une authentification. Actuellement l'application est ouverte à des utilisateurs non authentifiés via une gestion des comptes interne à NEO.

Au CNRS, où la volumétrie est la plus conséquente, l'application est ouverte à un potentiel de 5000 utilisateurs authentifiés.

On estime cependant que, toutes populations confondues, la fréquentation de l'application est de l'ordre de 50 à 300 utilisateurs par jour. Suite aux campagnes de recrutement l'accès simultané des utilisateurs peut monter à 1000 personnes.

4.2.2 Services d'infrastructure

4.2.2.1 Architecture générale

La solution est construite sur une architecture logicielle intégrée, c'est-à-dire :

- s'appuyant sur une gestion des données unique,
- s'appuyant sur des mécanismes d'accès, d'authentification et de gestion de la confidentialité proposant une ergonomie homogène pour l'ensemble des fonctionnalités,
- disposant d'un outillage d'administration dédié.

Référence	Libellé exigence	Priorité
INF_001	Partout où cela est possible, les privilèges accordés aux comptes de service utilisés par la solution sont minimisés au strict nécessaire. <i>Exemple: accès BDD, accès au système de fichiers, ...</i>	0
INF_002	L'exploitation et l'administration « fonctionnelle » de la solution est réalisée par une IHM spécifique, si possible dédiée, avec des comptes nominatifs dédiés. Elle ne nécessite pas de connexions en SSH ou d'actions nécessitant une console (<i>ex : récupération de logs récurrente, édition de fichiers de paramétrage pour lancer une campagne, etc.</i>).	0
INF_003	La solution ne peut pas être proposée en mode SaaS.	0

4.2.2.2 Caractéristiques système

Les exigences système suivantes doivent être respectées :

Référence	Libellé exigence	Priorité
INF_004	Le serveur HTTP de référence est Apache sur Linux. L'autre plateforme acceptée est la solution IIS sous Windows.	0
INF_005	Dans le cas où la solution nécessite un serveur d'application Java préinstallé, la référence est Tomcat. Une autre solution peut être acceptée sur dérogation.	1
INF_006	Le système d'exploitation serveur de référence est Red Hat Enterprise Linux, le système d'exploitation Windows serveur est toléré.	0

Référence	Libellé exigence	Priorité
INF_007	La configuration d'un serveur PHP exécute uniquement les modules nécessaires à la solution, qui sont les seuls actifs. Cette liste est définie et communiquée par le titulaire. Certains modules sont explicitement interdits (notamment ceux permettant un appel direct au SE). Certaines fonctions sont interdites : disable_functions = system, exec, shell_exec, passthru, phpinfo, show_source, highlight_file, popen, proc_open, fopen_with_path, dbmopen, dbase_open, putenv, move_uploaded_file, chdir, mkdir, rmdir, chmod, rename, filepro, filepro_rowcount, filepro_retrieve, posix_mkfifo.	0
INF_008	Toutes les montées de versions mineures pour les OS serveurs (de type Linux), les modules serveurs applicatifs et bases de données, sont effectuées avec un déclenchement automatique, pour tout ce qui a été installé par le gestionnaire de paquets.	0

De plus, le titulaire a pris en compte dans son offre les exigences sur la sécurité des applications définies au chapitre 4.3.

4.2.2.3 Caractéristiques réseau

La solution mise en œuvre s'appuie impérativement sur l'infrastructure réseau existante et intègre les aspects suivants :

- tous les échanges sont compatibles avec les protocoles IPv4 et IPv6 ;
- tous les flux du système d'information sont recensés et maîtrisables, en terme de capacité à appréhender le mode de fonctionnement protocolaire associé, et à assurer le filtrage par des équipements de type « pare-feu » ; le titulaire fournit une matrice des flux de l'application, indiquant clairement les protocoles, ports et sens de communication utilisés par ces flux ;
- le serveur applicatif n'est pas directement visible des navigateurs clients, des éléments de type « reverse-proxy » étant intercalés dans le flux (Navigateur ⇄ [HTTPS] ⇒ Reverse Proxy ⇄ [HTTP] ⇒ Serveur applicatif) ;
- le fonctionnement de l'application intègre la mise en œuvre de composantes techniques souvent déployées dont notamment les réseaux privés virtuels (VLAN), la translation d'adresses IP (NAT), l'utilisation de serveurs de type Reverse Proxy, les « pare-feux », le chiffrement (via une technologie de type VPN ou autre) ;
- la solution est parfaitement inter opérante avec les principaux services Internet (DNS, SMTP, NTP, SNMP, etc.), dans leurs versions chiffrées quand elles existent. Elle respecte en particulier les principaux RFC associés à chacun des protocoles, et les règles en usage dans la communauté Internet.

Référence	Libellé exigence	Priorité
INF_009	Les flux entre les postes clients et le(s) serveur(s) applicatif(s) passent par une DMZ avec rupture de flux effectuée par des reverse proxy.	1
INF_010	Les seuls flux « réseau » (hors flux techniques comme "DNS", "EAI", ...) légitimes sont les suivants : <ul style="list-style-type: none"> ■ reverse proxy → serveur d'application ■ serveur d'application → serveur de base de données 	1
INF_011	Les flux entrants de systèmes externes sont soumis à autorisation de la sécurité. Dans le cas où ils sont autorisés, ils passent par des services en DMZ.	0
INF_012	Les flux sortants sont chiffrés conformément aux dispositions réglementaires (cf. RGS Annexe B1, B2, B3 https://cyber.gouv.fr/le-referentiel-general-de-securite-version-20-les-documents), passent un proxy HTTP et sont initiés par le CNRS	1
INF_013	La compatibilité IPv6 est assurée de façon native. En production, les communications se font en IPv4 sauf décision expresse du CNRS.	2
INF_014	Les connexions VPN doivent obligatoirement être effectuée en site à site IPSEC IKEv2, le roaming user SSL avec chiffrement au niveau réglementaire requis est toléré avec identification du terminal et de l'utilisateur	0

Référence	Libellé exigence	Priorité
INF_015	Un filtrage protocolaire L4 au minimum est mis en service sur les systèmes d'exploitation, s'appuyant sur une matrice de flux documentée, permettant de limiter au strict nécessaire : <ul style="list-style-type: none"> les ports d'écoute les sources pouvant joindre chaque port (exemple : un port d'écoute destiné à un échange interapplicatif ne doit être joignable que par l'autre pair de communication) les destinations légitimes lorsqu'il s'agit de flux sortants. Par défaut, un serveur n'initie pas de trafic réseau, en dehors du trafic nécessaire à sa mise à jour. Le titulaire fournit la matrice des flux en tant que livrable.	0
INF_016	L'administration de la solution doit être compatible avec des solutions d'administration de type bastion.	0
INF_017	La prise de main depuis l'extérieur passe par un VPN puis un bastion.	0

4.2.2.4 Exploitabilité de la solution

L'application doit être techniquement paramétrable à souhait, et elle doit être facilement exploitable par les équipes qui la maintiennent en condition opérationnelle. En particulier, les exigences suivantes sont à respecter par l'application :

Référence	Libellé exigence	Priorité
INF_018	Les solutions applicatives permettant d'assurer la continuité d'activité (<i>ex. serveurs d'application redondants</i>) sont nécessaires lorsque le besoin est confirmé par les besoins de continuité de la solution. Dans ce cas, la scalabilité du service doit pouvoir se faire par l'ajout de nœud(s) sur les différentes couches (tiers) de la solution (hors base de données).	0
INF_019	L'hébergement en production bénéficie d'une politique de sauvegarde définie en fonction des besoins de reprise d'activité de la solution. Les sauvegardes sont déportées pour être suffisamment isolées du site de production.	0
INF_020	Les technologies à base de containers (de type Docker) ne sont pas préconisées tant que le CNRS ne s'est pas doté de l'outillage adapté.	1
INF_021	L'application doit être compatible avec un environnement d'exécution durci selon les règles définies par le CNRS, ces règles sont issues des profils SCAP 1.3 publiés par le NIST pour les systèmes d'exploitation.	1

4.2.2.5 Caractéristiques d'observabilité

Le CNRS effectue la supervision de ses applications en collectant les informations suivantes :

- métriques techniques du système d'exploitation et composants,
- logs des composants de bas niveau (système d'exploitation, base de données, serveur web, ...),
- logs applicatifs issus de fichiers de logs fournis par l'application avec un format facilitant leur analyse.

4.2.3 Architecture applicative

4.2.3.1 Normes d'architecture

Les exigences et recommandations techniques concernant l'architecture applicative sont les suivantes :

Référence	Libellé exigence	Priorité
DEV_001	L'architecture doit bien séparer les aspects essentiels de la solution (présentation, aspects métiers, accès aux données) afin de faciliter la testabilité et l'extensibilité de la solution. Une attention particulière est portée à l'abstraction de la base de données, afin de permettre la mise en place de l'intégration continue du code et faciliter les éventuels changements de base de données.	0
DEV_002	La haute disponibilité est mise en place pour les solutions identifiées comme ayant le besoin de disponibilité attendu le plus élevé.	0

Référence	Libellé exigence	Priorité
DEV_003	L'architecture est de type client léger, les clients lourds ou riches basés sur des technologies de plugins dans les navigateurs (tels que les applets, Flash, ActiveX, ...) sont interdits. Tous les traitements et vérifications sont réalisés au moins du côté serveur : aucune entrée cliente n'est considérée comme fiable par défaut.	0
DEV_004	L'usage de Java WebStart est temporairement toléré lorsqu'il n'existe aucune alternative (par exemple si besoin de signature numérique)	1
DEV_005	Il est interdit de déployer sur les postes de travail des logiciels créant des adhérences autres que le navigateur, en dehors de certaines exceptions à justifier.	1
DEV_006	La solution est utilisable à partir d'un navigateur Web sur un protocole de transport TLS aussi bien pour les solutions à visibilité internet que les solutions internes. Le CNRS impose les technologies Web natives (HTML5, CSS3...) limitant les interactions avec le système d'exploitation et le respect des standards du W3C.	1
DEV_007	L'architecture n'est pas monoposte.	0
DEV_008	En plus du français, la gestion d'au moins une langue étrangère (l'anglais) est fournie.	1
DEV_009	Les libellés (messages d'erreur, champs, texte, ...) sont externalisés, soit en base soit via un fichier de propriétés. <i>Par exemple, les nomenclatures ne sont pas stockées dans le code applicatif mais sont externalisées.</i>	1
DEV_010	Tous les envois de mails sont effectués depuis le domaine cnrs.fr avec un expéditeur existant dédié, ils sont gérés par la solution selon les règles suivantes : 1. Ces envois passent par les relais SMTP mutualisés de la DSI 2. Le code ne tente pas d'envoyer directement via le port 25 (notamment sous Java ou PHP qui embarquent des bibliothèques dédiées au lieu de s'appuyer sur l'OS) pour éviter que les mails envoyés soient considérés comme spam 3. Le domaine de sortie est choisi parmi ceux autorisés par les relais de la DSI 4. La solution n'utilise pas l'adresse mail des utilisateurs comme clause FROM sous peine d'usurpation d'identité et blacklistage pour les domaines non gérés par la DSI 5. La solution respecte un formalisme de message imposé par le CNRS 6. La solution supporte l'envoi de messages numériquement signés 7. Il est recommandé de ne pas envoyer de pièces jointes, dans le cas où ce serait nécessaire, la solution permet le paramétrage de la limite la taille des pièces jointes 7. La solution prévoit des envois par lots en cas de besoin, et limite le nombre de destinataires par lot et la fréquence d'envoi. En cas de besoin d'envoi de messages aux utilisateurs de la solution, un serveur SMTP dédié (fourni par la DSI si la solution est hébergée par la DSI) est utilisé	0

4.2.3.2 Langages

Les exigences et recommandations techniques concernant les langages utilisés sont les suivantes :

Référence	Libellé exigence	Priorité
DEV_011	L'ensemble des langages et des composants nécessaires à la solution sont utilisés dans les versions mentionnées dans le document CCT_Versions-cibles (ce document est mis à jour régulièrement). Le document, dans sa version courante est applicable à tout moment, ce qui implique des mises à jour régulières des applicatifs en conséquence.	0
DEV_012	Sauf contrainte contractuelle, le choix du langage et des frameworks est le résultat d'un consensus entre la DSI et le titulaire en charge de la réalisation de la solution.	0
DEV_013	Les frameworks de développement doivent être ouverts, éprouvés, avec une large communauté active, maîtrisés par le titulaire en charge de la réalisation solution, et permettre d'automatiser les tests unitaires. Leur choix est justifié en regard des gains attendus en termes de développement et d'évolutivité. Les versions utilisées sont systématiquement celles qui sont les plus récentes et qui présentent la durée de support la plus longue.	1

Référence	Libellé exigence	Priorité
DEV_014	Pour une solution Java, le framework utilisé est Spring Boot avec le serveur web embarqué (la solution ne requiert donc pas d'être installée dans un conteneur de servlets).	N/A
DEV_015	Pour une solution PHP, le framework utilisé est Symfony.	1
DEV_016	Le nombre de composants externes complémentaires est limité au strict minimum. L'utilisation de composants externes, progiciels, logiciels tiers respecte les règles suivantes : 1. Son fournisseur est engagé sur le maintien dans la durée d'une réelle API de communication 2. Les évolutions de la solution peuvent être menées sans avoir systématiquement recours à des consultants experts de ces composants tiers. 3. Les développements spécifiques n'ont pas d'impact sur les montées de version, ou bien ces impacts sont intégrés comme un coût additionnel en début de projet 4. Le code tiers utilisé dispose d'une licence d'utilisation bien identifiée, n'induisant pas pour le CNRS de contraintes d'acquisition ou d'aliénation de ses droits. Les licences libres sont recommandées.	0

4.2.3.3 Normes de développement

En fonction de la technologie retenue, des préconisations concernant les méthodologies et règles de développement sont applicables et s'appliquent notamment pour le code spécifique développé pour le CNRS.

Les recommandations ci-après s'appliquent de manière plus générale à l'ensemble des technologies.

Le CNRS/Inserm est attentif à la qualité logicielle de l'application et à ses capacités d'évolution.

D'une manière générale, le titulaire doit utiliser autant que possible des standards pérennes normalisés ou reconnus du marché.

Les exigences et recommandations techniques concernant les normes de développement sont les suivantes :

Référence	Libellé exigence	Priorité
DEV_017	Les développements sont modulaires afin de faciliter la maintenance et l'évolutivité du code.	0
DEV_018	Les erreurs sont traitées de manière à assurer la sécurité dans les développements (toutes les erreurs levées lors de l'exécution doivent être traitées en conséquence).	0
DEV_019	Les bibliothèques de logs utilisées sont ouvertes, éprouvées, avec une large communauté active, et maîtrisées par le titulaire. Les logs sont paramétrables et gèrent a minima les niveaux suivants : ERROR : une erreur technique non récupérable est survenue dans la solution ; en général, la solution n'est plus opérationnelle ensuite WARN : un point d'attention a été soulevé, ou une erreur récupérable est survenue INFO : permet de suivre le fonctionnement métier de l'application, plus les étapes importantes de la vie de l'application DEBUG : permet de voir le fonctionnement technique de la solution.	0
DEV_020-a	La solution journalise des événements permettant l'audit des connexions effectuées à la solution, et le suivi des opérations importantes. Les opérations à tracer ainsi que le format du contenu de ces journaux sont définis conjointement entre le titulaire et le CNRS, les logs issus de l'application sont dans des fichiers textes dans un format permettant leur analyse.	0
DEV_020-b	L'application utilise une bibliothèque de logs qui permet de paramétrer la destination des événements de logs (par exemple syslog).	0
DEV_022	La solution ne récupère pas de code externe (en dehors sa phase de construction), sauf si la dépendance a été définie explicitement, intégralement et statiquement dans son code.	0
DEV_023	Le paramétrage technique de la solution est réalisé au travers de fichiers de configurations qui doivent être stockés de manière indépendante du code applicatif.	0

Référence	Libellé exigence	Priorité
DEV_024	Afin de lutter contre les risques d'injection de code, les requêtes SQL adressées à la base de données sont faites au moyen de requêtes préparées fortement typées ou par l'intermédiaire d'une couche d'abstraction assurant le contrôle des paramètres.	0
DEV_025	Les tests unitaires sont automatisés, avec un taux de couverture minimum défini d'un commun accord entre tous les acteurs du projet. Ces tests doivent s'exécuter sans erreur dans la forge du CNRS (les cas d'erreurs résiduels devront être justifiés par le titulaire).	0
DEV_026	Des frameworks sont utilisés pour développer les tests unitaires, dans les versions mentionnées dans le document CCT_Versions-cibles (ce document est mis à jour régulièrement). Les tests unitaires livrés en même temps que les fonctionnalités couvertes servent aux tests de non régression et peuvent fournir à travers des outils de couverture de tests un indicateur de qualité.	1
DEV_027	Les codes doivent être documentés et lisibles. Les composants (modules, classes, méthodes) doivent reposer sur une nomenclature de nommage normalisée et cohérente.	0
DEV_028	Les packages sont préfixés en utilisant fr.cnrs	0
DEV_029	Au niveau OS, le jeu de caractères pour la solution est UTF-8.	1
DEV_030	<p>Les solutions sont compatibles avec la liste des navigateurs/OS et versions associées dans le document CCT-Versions-cibles (ce document est mis à jour régulièrement).</p> <p>La notion de support d'une plate-forme cliente impose que l'ensemble des fonctionnalités attendues soit disponible dans des conditions de complétude, d'ergonomie et de performance tout à fait normales.</p> <p>Les niveaux de prises en charge possibles sont les suivants :</p> <p>Maximal : Les navigateurs dans cette catégorie doivent offrir aux visiteurs toutes les performances techniques, visuelles et fonctionnelles définies par le cahier des charges et la maquette graphique,</p> <p>Dégradé : Les navigateurs doivent permettre une expérience utilisateur équivalente au niveau précédent mais qui peut toutefois présenter des différences considérées comme négligeables (décalages minimes, arrondis, ombrages...),</p> <p>Minimal : L'intégration HTML/CSS est accessible et agencée convenablement, mais aucun effort n'est porté sur la compatibilité visuelle avec les niveaux précédents.</p>	0
DEV_031	L'utilisation de Javascript est autorisée notamment pour fluidifier les échanges avec la solution, <i>par exemple en effectuant des contrôles côté client</i> . Cependant, ces contrôles côté client ne se substituent pas aux contrôles côté serveur qu'il faut impérativement réaliser.	0
DEV_032	Il est interdit de construire un framework Javascript.	0
DEV_033	L'architecture de services web recommandée est l'architecture de type REST.	1
DEV_034	Le CNRS n'impose pas d'outil de génération de PDF particulier dans la mesure où l'outil choisi est ouvert, éprouvé, avec une large communauté active, et maîtrisé par le titulaire.	0
DEV_035	Les outils de requêtage mis à disposition sont paramétrés de manière à limiter les risques de dégradation des performances de la plate-forme en cas d'utilisation malavisée par certains utilisateurs. Les outils de requêtage doivent garantir le respect des droits d'accès de l'utilisateur.	0
DEV_036	Les éléments d'architecture critiques, complexes ou difficiles à appréhender doivent faire l'objet de paragraphes spécifiques dans la documentation permettant leur bonne compréhension.	0
DEV_037	Les dossiers d'architecture technique, spécifications techniques détaillées (STD) ainsi que les manuels d'exploitation (MEX) et d'installation (MINS) sont actualisés par le titulaire autant que de besoin. Ils sont réputés être à jour à tout moment.	0
DEV_038	La gestion des types d'environnements (développement, recette, production, ...) est prise en charge dans la solution pour adapter automatiquement le niveau de fonctionnalité de la solution (<i>exemple : activation du debug, paramétrages d'envoi de mails, etc.</i>). Les propriétés de l'environnement sont renseignées sur l'instance déployée et facilement modifiables (<i>exemple : fichier unique à modifier au moment du déploiement</i>)	2

Référence	Libellé exigence	Priorité
DEV_039	L'ensemble des éléments du bandeau, l'ensemble des couleurs, des polices de caractères, des espaces, filets, comportements au passage de la souris, aplats couleurs, paramétrages de tableaux, gestion des menus et onglets, sont gérés par une feuille de style CSS (pas de code couleur ni de mise en page en dur dans le code de la page).	1
DEV_040	Eviter au maximum l'utilisation de tables pour gérer la mise en forme dans le code HTML.	2
DEV_041	<p>Les configurations des systèmes et des logiciels utilisés par la solution (notamment Java, PHP) sont obligatoirement durcies à l'état de l'art (cf. https://cyber.gouv.fr/publications/securiser-un-site-web), afin de limiter la surface d'attaque et la fuite d'informations par trop grande verbosité. On citera en particulier et sans exhaustivité :</p> <ul style="list-style-type: none"> ■ la suppression des balises « meta » dans l'entête HTML lorsque celles-ci indiquent le logiciel ayant généré la page ; ■ la suppression des éléments visibles sur la page indiquant les outils (CMS, éditeur, etc.) utilisés ; ■ la limitation en production des informations de débogage dans les messages d'erreur (en évitant par exemple de fournir la requête SQL qui a généré une erreur) ; ■ l'utilisation de pages d'erreurs personnalisées pour ne pas reposer sur les pages par défaut facilement reconnaissables ; ■ dans certains cas, l'utilisation de l'erreur 404 générique plutôt que d'une erreur 401, 403, 405, etc. pour éviter de révéler trop d'informations sur le fonctionnement ou le contenu en accès limité du site ; ■ la banalisation des entêtes HTTP qui peuvent fournir des informations de version trop précises sur le serveur ou le système d'exploitation employés ; ■ le rejet, en production, des requêtes HTTP TRACE qui n'ont d'intérêt qu'en phase de débogage. 	0

4.2.3.4 *Outillage de développement*

Le CNRS opère une forge logicielle afin de favoriser la qualité logicielle, la réduction de la dette technique et l'intégration continue.

Cette forge est composée des éléments suivants :

- un service de gestion de configuration et de dépôt interne : Gitlab
- un service d'intégration continue : Gitlab CI et Gitlab runners
- un analyseur de code : Sonar
- un gestionnaire d'artéfacts : Artifactory

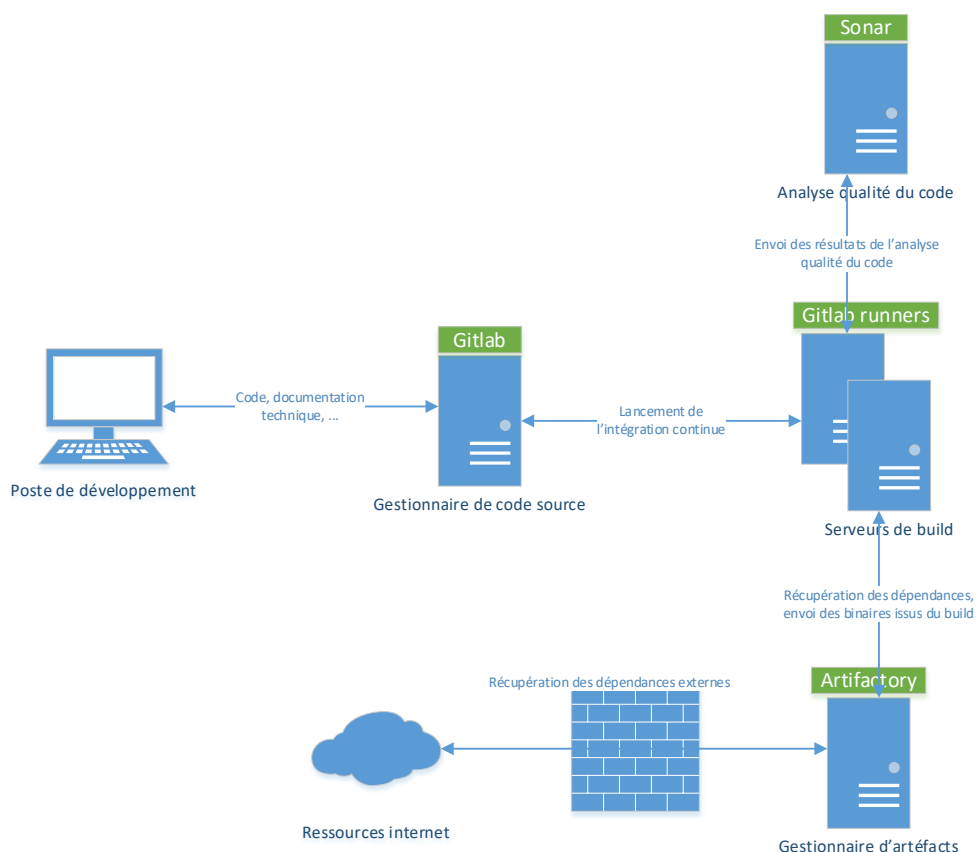


Figure 21 : Présentation de la forge logicielle

Le titulaire doit utiliser la forge de développement de la DSI du CNRS dans l'objectif d'améliorer la qualité.

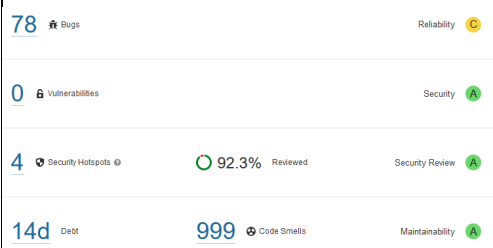

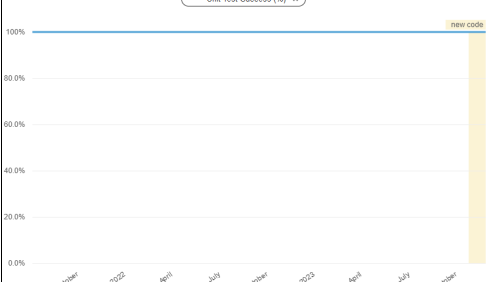
Le CNRS utilise les outils Ansible et Tower pour automatiser autant que possible le déploiement de ses applications.

L'outil de vérification de la qualité du code utilisé à la DSI est SonarQube (<https://www.sonarsource.com/products/sonarqube/>).

Au démarrage de l'accord-cadre, les équipes CNRS et titulaire se mettent d'accord sur le profil SONAR à utiliser afin d'évaluer la qualité du code source.

Les métriques particulièrement suivies par le CNRS sont les suivantes :

Métrique SonarQube	Description métrique	Cible CNRS
	Taux de commentaires	à <i>ajuster/justifier</i> en fonction des applications
	Duplication de code	à <i>ajuster/justifier</i> en fonction des applications

Métrique SonarQube	Description métrique	Cible CNRS
	Respect des règles de codage, problèmes potentiels de sécurité	Pas d'anomalies de niveau « blocker » et « critical ». Analyser les majeures. Pas de vulnérabilités.
	La couverture de tests unitaires (pourcentage de lignes de code du projet qui est appelé pendant la phase de test)	Supérieur à 50%
	Le taux de succès des tests unitaires	égal à 100%

Le niveau de conformité à atteindre fait l'objet d'une concertation entre le titulaire et le CNRS/Inserm.

Plus que l'atteinte de seuils définis, le CNRS est attentif à l'évolution des métriques au cours du temps (lors de chaque livraison majeure de l'application).

Les exigences concernant les outils de développement du titulaire sont les suivantes :

Référence	Libellé exigence	Priorité
DEV_042	Le CNRS n'impose pas de contrainte sur l'outil de développement intégré (IDE) dans la mesure où l'outil choisi est maîtrisé par le titulaire.	2
DEV_043	Pour les cas qui nécessitent des interactions avec des éléments externes (tests, environnement d'intégration ou de recette, ...), des mocks/bouchons sont utilisés. L'usage de bibliothèques de mocks est possible. Le CNRS n'impose pas d'outil particulier dans la mesure où celui choisi est ouvert, éprouvé, avec une large communauté active, et maîtrisé par le titulaire.	0
DEV_044	JMeter est l'outil préconisé pour les tests de charge, si un autre outil est proposé il doit être ouvert, éprouvé, avec une large communauté active, et maîtrisé par l'équipe en charge de son utilisation.	1
DEV_045	Un moteur de production est utilisé afin de gérer les dépendances de la solution, le lancement des tests automatisés, sa construction, la publication des artefacts sur un gestionnaire d'artefacts, ... Pour les projets Java, Maven ou Gradle est utilisé. Pour les projets PHP sous Symfony, Composer est utilisé.	1
DEV_046	Le nommage des artefacts générés par la phase de construction de la solution suivent les normes de nommage standard (<i>par exemple Maven pour les projets Java, Composer pour les projets PHP</i>).	1
DEV_047	Le gestionnaire de source Git est utilisé pour la gestion des codes sources. Le CNRS dispose d'un outil de gestion de code source Gitlab dans lequel se trouve le code source de la solution (soit en posant les commits directement dans le Gitlab du CNRS, soit avec un mécanisme de synchronisation - à la charge du titulaire - dans le cas où le titulaire souhaite utiliser des dépôts Git qui ne sont pas ceux du CNRS).	0
DEV_048	La notion de tag (au sens Git) est utilisée pour faire le lien entre les modifications de code source et la version de la livraison.	0

Référence	Libellé exigence	Priorité
DEV_049	Un modèle de gestion des branches Git est utilisé (<i>par exemple Gitflow</i>) en accord avec le CNRS.	1
DEV_050	Le CNRS dispose d'un outil d'analyse statique de code source, SonarQube, utilisé pour analyser le code de la solution. Le titulaire a la possibilité d'utiliser également un outil d'analyse de qualité du code, qui peut ne pas être SonarQube. Des indicateurs et des métriques de qualité logicielle reposant sur ces outils sont proposés par le titulaire. Les éléments de qualité remontés par l'outil SonarQube du CNRS et analysés ensuite, sont définis au démarrage du projet.	1
DEV_051	Le CNRS dispose d'un outil d'intégration continue, Gitlab CI, utilisé a minima pour lancer l'analyse Sonar. De manière générale, la solution est construite par cet outil. Le code source contient un fichier ".gitlab-ci.yml" indiquant la marche à suivre pour construire le projet (ce qui inclut au minimum la récupération des dépendances, le lancement des tests automatisés, la construction de la solution et la publication des artéfacts). Tout autre mode de construction est à discuter au démarrage du projet.	1
DEV_052	Le titulaire exécute une tâche de construction automatique avant toute livraison au CNRS afin de valider la bonne réalisation des opérations de compilation, de réussite des tests unitaires ainsi que de vérifications des éventuelles licences.	1
DEV_053	La livraison et l'installation de la solution est réalisée de façon outillée et automatisée en évitant toute opération manuelle (sauvegarde système, rollback, ...). Il n'y a pas de recommandation particulière pour le choix de l'outil d'installation, mais l'outillage écrit pour réaliser cette tâche est également géré dans l'outil de gestion de code Gitlab du CNRS.	1
DEV_054	Le titulaire se synchronise avec le gestionnaire de version (Git) du CNRS à chaque livraison pour le code spécifique développé pour le CNRS afin que le CNRS ait une visibilité sur le code, les tests unitaires et les tests d'intégration associés.	0
DEV_055	La réussite de l'ensemble des tests unitaires est une condition nécessaire à l'acceptation d'une livraison majeure. Le niveau de réussite des tests unitaires à atteindre peut cependant faire l'objet d'une concertation en cas de forte contrainte au cas par cas.	1
DEV_56	Les modifications de schémas de base de données sont automatisées par l'application soit par le lancement de commandes de migration fournies par le framework, soit lors du démarrage de l'application.	1

4.2.4 Base de données

Les exigences et recommandations techniques concernant les bases de données sont les suivantes :

Référence	Libellé exigence	Priorité
BDD_001	Une base de données (relationnelle ou non relationnelle si c'est pertinent) est utilisée pour gérer la persistance des données.	0
BDD_002	Les solutions de SGBD de référence sont PostGreSQL et MongoDB.	1
BDD_003	La non adhérence au SGBD est assurée, les requêtes ne doivent pas être implémentées directement dans le code. Dans le cas des langages orientés objet, un ORM (mapping entre le modèle relationnel et le modèle objet) est utilisé. Dans les autres cas, une couche d'abstraction de la base de données est utilisée. Lorsque des requêtes SQL sont implémentées, elles le sont en respectant le standard SQL ANSI.	1
BDD_004	Au niveau SGBD, le jeu de caractères utilisé est UTF-8	1
BDD_005	Tous les objets de la base de données sont documentés.	1

4.2.5 Engagements de qualité de service pour l'application

4.2.5.1 Disponibilité

Dans le cas d'une phase de migration en production (portage), une interruption de service de 5 jours maximum est envisageable.

Dans le cas d'un déploiement d'une nouvelle version (mise en production), l'interruption de service acceptable est de 4h en continu une fois par mois ; que ce soit en cas de panne de l'application, ou en cas de maintenance programmée.

Les périodes de maintenance programmée se font à des périodes décidées en commun accord entre le CNRS et le titulaire.

Il est à noter qu'étant donné le caractère particulier d'une application fonctionnant selon un calendrier de campagne, l'application doit rester disponible et performante, en particulier pendant les pics d'utilisation de fin de période.

4.2.5.2 Intégrité

La solution doit permettre un contrôle de l'intégrité des données (intégrité structurelle et intégrité du contenu).

En cas de corruption de données, la perte de données acceptable est de 24h. Si nécessaire, l'application doit avoir la possibilité de reprendre les flux ou les batch qui auront été générés lors de la période de perte de données.

Le CNRS doit parfaitement maîtriser la nature des données utilisées par l'application et les mécanismes permettant de restaurer un jeu de données cohérent et exhaustif en cas de nécessité.

Le titulaire est tenu de fournir un descriptif exhaustif des données utilisées et des contraintes techniques associées à une restauration. L'usage des contraintes référentielles est fortement conseillé.

4.2.5.3 Performances

Le CNRS/Inserm définit comme suit les caractéristiques de performances attendues de l'application :

- Connexion au serveur (contrôle des accès compris) et affichage de la page d'accueil en moins de 5 secondes.
- Temps d'affichage d'une IHM de saisie / consultation inférieur à 3s dans 80% des cas.
- Temps d'exécution d'une requête de recherche inférieur à 10 secondes,
- Temps de génération d'un état inférieur à 20 secondes.

Ces chiffres correspondent à des transactions simples et largement utilisées dont le temps de réponse est mesuré sur le poste client hébergé sur le même réseau.

Certaines fonctionnalités peuvent déroger à ces règles. Toutefois elles doivent :

- faire l'objet d'un accord explicite du chef de projet DSI-CNRS,
- afficher à l'utilisateur des éléments permettant de juger de leur avancement.

Le titulaire fournit au CNRS/Inserm :

- des éléments de dimensionnement de la plate-forme de production pour garantir un niveau de performance conforme au besoin en regard des éléments de volumétrie disponibles ;
- des éléments de tuning de la plate-forme permettant d'optimiser les performances (système, base de données, ...).

Le titulaire fournit au CNRS/Inserm en même temps que chaque version stable de l'application le rapport des tests de performances qui auront été menés.

Ce rapport met particulièrement en avant les éléments chiffrés concrets qui permettent de valider les temps de réponses exigés par le CNRS/Inserm en condition de forte charge applicative. Il met aussi en évidence les composantes techniques de l'application nécessitant le plus de ressources techniques et induisant des temps de réponses significatifs.

4.3 EXIGENCES D'ERGONOMIE-GRAPHISME

NEO étant mutualisé avec l'Inserm, la charte graphique du CNRS n'est pas applicable à la solution. Toutefois, elle doit répondre à des exigences d'identité et d'ergonomie, et également suivre des recommandations techniques pour leur intégration (cf. § 4.2.3.3) afin de satisfaire au mieux les exigences d'accessibilité auxquelles tous les services Web d'un établissement public doivent se conformer.

Les éléments concernant l'ergonomie et le graphisme pourront être ajustés en cours de réalisation, de manière concertée entre le titulaire et l'équipe projet CNRS.

Référence	Libellé exigence	Priorité
ERG_001	Les règles d'ergonomie et de graphisme mises en œuvre dans la solution sont formalisées dans les spécifications fonctionnelles détaillées. Elles sont réputées être à jour à tout moment.	1

4.3.1 Charte graphique

Référence	Libellé exigence	Priorité
ERG_002	Un bandeau est positionné en haut de la page sur l'ensemble de la solution. Le bandeau est composé du logo du CNRS et de celui de l'Inserm situés à gauche de la page. A droite il y a le nom de la solution. Si le nom de la solution n'est pas explicite pour les utilisateurs, le titre est accompagné d'un sous-titre qui décrit ce que fait la solution. Le bandeau peut intégrer également les liens institutionnels une zone de connexion et éventuellement d'accès au profil en haut à droite au-dessus du titre ainsi qu'une barre d'outils (« Aide », « Documentation », etc.) à droite en dessous du titre (sauf solution responsive smartphone).	1
ERG_003	L'ensemble de la solution utilise les mêmes éléments de la feuille de style de manière logique et uniforme : police de caractère, liens de navigation, intitulés de champ, titres de différents niveaux, messages informatifs et d'aides à la saisie, messages d'alerte, etc. Il en est de même pour la sémologie des pictogrammes.	0
ERG_004	La solution utilise une gamme de codes couleurs et de polices préconisées par le CNRS/Inserm pour NEO. Si besoin est, cette gamme peut être enrichie avec la contribution du CNRS.	1
ERG_005	Dans le cas d'une solution responsive, l'organisation des écrans peut s'appuyer sur des grilles (grid). Toutes les fonctionnalités essentielles de la solution sont accessibles quel que soit le média. L'apparence du bandeau et la disposition des éléments de barre d'outils sont optimisés pour apparaître sur une interface de smartphone.	1

4.3.2 Règles d'ergonomie

L'application doit être ergonomique c'est-à-dire qu'elle doit être facilement utilisable, fonctionnelle et compréhensible par l'ensemble des utilisateurs, ce de manière aisée, déductible et conviviale.

L'application doit accompagner l'utilisateur qui doit savoir ce qu'il doit faire sur la page active. Il doit également pouvoir naviguer et se repérer dans l'ensemble de l'application. Pour cela, l'application doit utiliser les systèmes de navigation les plus adaptés, *par exemple : menus, onglets, enchaînements d'étapes, etc.*

Les éléments fonctionnels du cœur de page doivent être disposés de manière à permettre une lecture facile, avec des éléments regroupés et structurés.

La conception de l'IHM peut faire appel à des composants d'IHM innovants, *par exemple : effets de transition, de transparence, mouvements, auto complétion, etc.*

L'application doit être conçue de manière globale et homogène.

Référence	Libellé exigence	Priorité
ERG_006	La taille des fenêtres est adaptable à différentes tailles et résolutions d'écrans. Aucune fenêtre de la solution ne comporte d'ascenseur horizontal.	1
ERG_007	Les tableaux sont conçus de manière optimisée (utilisation de formules synthétiques, de pictogrammes, interlignages valorisés par des couleurs de fond, mise en valeur des entêtes, des liens, ordre des colonnes pertinent, système de navigation pour les tableaux longs).	1
ERG_008	Les titrailes et entêtes sont explicites et clairement structurées et hiérarchisées (utilisation de la feuille de style CSS et des balises h1, h2, etc.).	0
ERG_009	Les éléments de navigation sont clairs et explicites. Dans le cas d'arborescences complexes, un chemin de navigation apparaît.	1
ERG_010	Dans le cas de solution responsive, l'interface est adaptée au pilotage de l'ihm via un doigt (zone cliquable agrandie, survol impossible, navigation par balayage de l'écran, etc.). Les textes sont agrandis.	1

4.4 EXIGENCES DE SECURITE

Le référentiel des exigences sécurité est présenté dans le tableau ci-dessous. Lorsque nécessaire, il est complété par des éléments détaillés dans les paragraphes suivants.

Référence	Libellé exigence	Priorité
SSI_001	Un dossier de sécurité pour la solution détaillant les mesures de sécurité opérationnelle mises en application, ainsi que tous les éléments de preuve de la réelle application de ces mesures (captures d'écran, fichiers de configuration, compte rendus...) est créé et maintenu. Il indique également comment ces mesures sont régulièrement vérifiées et le dossier comprend le CR des vérifications, le compte-rendu des audits. Ce même dossier constitue une preuve de mise en œuvre des mesures de sécurité conformément au RGPD.	0
SSI_002	Le framework utilisé dispose d'un historique clair et vérifiable de ses vulnérabilités. A date d'implémentation, il ne présente pas de faille non corrigée. L'historique permet d'évaluer la réactivité de correction et la fréquence des failles, et est un argument du choix.	0
SSI_004	Lorsque l'analyse de risque en détermine la nécessité, le chiffrement des données est à mettre en place. Les outils et/ou protocoles de chiffrement utilisés doivent être qualifiés et certifiés par l'ANSSI..	1
SSI_005	Validation des entrées utilisateur : toute saisie utilisateur est vérifiée côté serveur en conformité avec le format, la taille, la sémantique et le type de données attendu.	0
SSI_006	Audit statique de code : le cycle de développement inclut des phases régulières d'audit statique de code, par l'utilisation d'outils d'aide à l'analyse et/ou par revue de code par un pair. Le titulaire fournit au CNRS les états réguliers de cette analyse.	1
SSI_007	Déconnexion à temps contraint paramétrable : l'utilisateur de la solution est déconnecté de sa session après un temps paramétrable dans la solution. Cette durée est implémentée de manière cohérente dans l'ensemble des modules techniques nécessaires à la solution.	0
SSI_008-a	Les identifiants de session utilisateur sont aléatoires avec entropie d'au moins 128 bits.	0
SSI_008-b	L'attribut Secure est associé au cookie de l'identifiant de session utilisateur.	0
SSI_008-c	L'attribut HttpOnly est associé au cookie de l'identifiant de session utilisateur.	0
SSI_009	Les informations liées aux habilitations des utilisateurs ne sont jamais passées en paramètres de URL.	0
SSI_010	Gestion des erreurs applicatives : les messages d'erreur applicatifs sont présentés à l'utilisateur en masquant toute information technique divulguant les composants de la solution et leurs versions.	0
SSI_011-a	Lors de la mise en œuvre d'un téléchargement montant (upload) de fichiers, le téléversement est effectué dans une zone disque tampon, puis le fichier est déplacé hors de l'arborescence d'hébergement web.	1
SSI_011-b	Lors de la mise en œuvre d'un téléchargement montant (upload) de fichiers, la vérification du fichier repose sur le type MIME (sans faire confiance ni à l'extension du fichier ni aux entêtes HTTP reçues) et la taille du fichier. En cas de discordance le fichier est refusé.	1
SSI_011-c	Lors de la mise en œuvre d'un téléchargement montant (upload) de fichiers, la vérification de la présence de logiciels malveillants est réalisée par l'antivirus installé sur le système d'exploitation.	1
SSI_011-d	Lors de la mise en œuvre d'un téléchargement montant (upload) de fichiers, le nom du fichier téléchargé est anonymisé.	1
SSI_012	Gestion des vulnérabilités : une surveillance des vulnérabilités applicatives est mise en place pendant la durée de la vie de la solution, et à la correction <i>pro bono</i> de celles-ci. Ces vulnérabilités peuvent toucher toutes les briques applicatives nécessaires à la solution.	1
SSI_013	Dans le cadre d'un développement spécifique, une licence logicielle est choisie par le CNRS conformément à ses besoins. Une référence à cette licence apparaît dans chaque fichier source produit.	0

Référence	Libellé exigence	Priorité
SSI_014	Lorsque des fonctions de visa ou de signature électronique sont mises en œuvre, elles respectent les dispositions du règlement eIDAS (https://cyber.gouv.fr/le-reglement-eidas-n9102014) et du RGS (https://cyber.gouv.fr/le-referentiel-general-de-securite-rgs). La mise en œuvre est obligatoirement discutée avec le département Sécurité.	0
SSI_015	En fonction des résultats de l'analyse de risques et/ou de l'étude d'impact vie privée (EIVP) menées, les données stockées sont chiffrées au repos (at rest) selon les dispositions du RGS Annexe B2(https://cyber.gouv.fr/le-referentiel-general-de-securite-version-20-les-documents). Les clés de chiffrement sont stockées de manière à n'être disponibles que pour les personnels ayant besoin d'en connaître. Dans certains cas, les administrateurs techniques et fonctionnels peuvent ne pas avoir accès aux données.	1
SSI_016	La solution prend en compte les besoins d'archivage numérique pérenne de ses données, selon les durées d'utilité spécifiées par la MOA/Archiviste. Quand cela est possible, elle implémente un connecteur vers le SAE intermédiaire transverse du CNRS.	1
SSI_019	Conformément au RGPD, quand le traitement réalisé par la solution relève d'un consentement de l'utilisateur, la solution se charge de vérifier l'existence de ce consentement.	0
SSI_020	Pour protéger les données, les environnements hors production n'utilisent pas les informations des données de production sauf dérogation expresse du CNRS.	0
SSI_021	Les journaux générés par la solution, les logiciels intermédiaires, les serveurs web et d'application, le système d'exploitation, les équipements réseaux et de sécurité couvrent au niveau de détail requis par la réglementation les activités de connexions et les opérations importantes menées sur ces systèmes quelle que soit la source (utilisateur, administrateur, scripts ou processus particulier) afin d'identifier l'auteur et la substance d'une action illicite, délictueuse, ou criminelle.	0
SSI_022	Les journaux générés par la solution, les logiciels intermédiaires, les serveurs web et d'application, le système d'exploitation, les équipements réseaux et de sécurité sont établis dans un format structuré dont les champs couvrent a minima pour chaque événement, requête ou action : <ul style="list-style-type: none"> ■ l'horodatage ■ le compte utilisateur ou processus associé ■ l'adresse IP ou la source à l'origine [en cas d'interaction distante] ■ le libellé intelligible de l'événement ou l'action ■ le code retour de l'action [option] ■ un identifiant unique de corrélation [option] ■ la taille de la requête [option] 	0
SSI_023	Les journaux générés par la solution, les logiciels intermédiaires, les serveurs web et d'application, le système d'exploitation, les équipements réseaux et de sécurité sont tous horodatés de manière fiable et synchronisés sur une même source temps en indiquant notamment le fuseau horaire si les journaux ne sont pas établis en heure UTC.	0
SSI_024	Les journaux générés par la solution, les logiciels intermédiaires, les serveurs web et d'application, le système d'exploitation, les équipements réseaux et de sécurité sont exportés en temps réel hors du système générateur, de manière fiable et intégrée vers un système central de collecte spécifié par le CNRS.	0

4.4.1 Auditabilité

Niveau de traçabilité

La solution met en œuvre obligatoirement la politique de traçabilité de l'ensemble des accès (autorisés et refusés) et des opérations réalisées. Ces traces doivent contenir à minima les informations suivantes :

- Date et heure de l'accès (avec une information d'horodatage fiable) : connexion et déconnexion ;
- Compte d'accès ;
- Etat de l'accès : autorisé ou refusé (et la raison en cas d'échec) ;
- Opérations réalisées ;
- Adresse IP source et protocole d'accès.

De plus, la solution doit implémenter ces fonctions autour de la gestion des traces :

- Durée de rétention des traces (mécanisme de rotation des traces, capacité de rétention maximale) ;
- Centralisation des traces (le CNRS dispose de la solution Elastic) ;
- Sauvegarde des traces ;
- Archivage des traces ;
- Protection des traces (pour assurer leur disponibilité, intégrité et confidentialité) ;
- Supervision des traces.

Gestion des traces

La solution doit permettre un reporting sur les :

- Opérations en général ;
- Accès et les opérations qualifiées comme sensibles réalisées ;
- Sortie d'information (ou exports de données);
- Données non intègres.

L'accès à ces rapports doit être réservé aux personnes clairement identifiées et habilitées.

4.4.2 Protection des applications web

L'application se doit de réduire au maximum les risques d'intrusion et de prévenir les stratégies d'attaques potentielles venant du web.

L'application ne doit pas être sensible à ce type de risques connus (liste non-exhaustive) :

- les injections de codes (de tous types : SQL, XML, Null Byte, LDAP, Mail Command, OS Command, XQuery...);
- les attaques par XSS (Cross Site Scripting) ;
- les attaques par des faiblesses dans la gestion des droits et des sessions ;
- les attaques par références directes aux objets ;
- les attaques par « Cross-Site Request Forgery » ;
- les attaques basées sur des erreurs de configuration ;
- les attaques sur des failles de restriction d'URL ;
- les attaques sur des URL d'accès aux objets prévisibles ;
- les attaques sur des redirections abusives.

Pour cela, l'application intègre, au moins, les dispositifs suivants :

- en cas d'utilisation d'espace privé (identifiant de session, etc.) dans les cookies, privilégier les cookies SSL (attribut secure), associer obligatoirement l'attribut HTTPOnly et associer systématiquement les attributs « Path, Domain et Expire » ;
- prévoir une déconnexion au bout de 20 minutes sans saisie ;
- prévoir une possibilité de déconnexion explicite pour l'utilisateur ;
- l'identifiant de session est à initier par le serveur ;
- l'identifiant de session doit être de type aléatoire et non-prédictible et d'une entropie d'au moins 128 bits ;
- l'identifiant de session doit être forgé après l'authentification ;
- lier l'identifiant de session à l'ID utilisateur, mais aussi à son adresse physique (adresse IP) ;
- interdire le passage d'informations sur les habilitations en paramètre ;
- interdire le passage de commandes (SQL, interpréteur..) directement dans les paramètres ;
- contrôler systématiquement les paramètres (formulaires et requêtes), au niveau du serveur ;
- préférer les POST au GET ;
- interdire les références directes aux objets dans les paramètres ;

- systématiser les contrôles d'accès aux objets et aux ressources ;
- gérer les accès multiples aux ressources ;
- durcir les paramètres et possibilités de redirections et de forward ;
- restreindre les accès aux URL d'administration ;
- gérer les erreurs applicatives pour les masquer à l'utilisateur ;
- un système de token par action serait un plus.

5 CADRE D'ORGANISATION DES PRESTATIONS

5.1 SYSTEME QUALITE

En ce qui concerne la qualité, le CNRS/Inserm préconise de s'appuyer sur la norme ISO 9001 (Systèmes de management de la qualité) et sur des référentiels de bonnes pratiques tels que :

- ITIL® : Bibliothèque pour l'infrastructure des technologies de l'information (Information Technology Infrastructure Library)
- Agile : Manifeste pour le développement agile de logiciels.

Le CNRS/Inserm est particulièrement attentif à la forte orientation utilisateur, l'approche processus et l'amélioration continue.

Le plan assurance qualité (PAQ) explicite les dispositions qualité (organisation, méthodes, outillage...) nécessaires à la bonne exécution du projet pour toutes les prestations définies dans l'accord-cadre. Il définit les procédures applicables à l'ensemble du périmètre de l'accord-cadre.

Le CNRS/Inserm peut effectuer des audits de l'application du PAQ. Dans ce cas, le CNRS/Inserm prévient le titulaire dans les formes mentionnées au CCAP en précisant la nature, le déroulement et le calendrier souhaité.

Côté CNRS, le responsable d'application de la DSI est garant de l'application des dispositions qualité pour le périmètre de son projet. Il est accompagné dans cette activité par la cellule qualité de la DSI, en particulier lors du démarrage de l'accord-cadre. La cellule qualité DSI s'assure du partage des dispositions qualité entre les différents projets et veille à l'homogénéisation des pratiques.

Référence	Libellé exigence	Priorité
QUA_001	Le titulaire fournit au CNRS un plan assurance qualité. Le PAQ est ajusté d'un commun accord avec le CNRS lors du démarrage de l'accord-cadre. Il est mis à jour tant que de besoin tout au long de l'accord-cadre avec l'accord des deux parties.	0
QUA_002	Le titulaire respecte les normes, méthodes et standards qualité du plan assurance qualité. Chaque non-respect d'une exigence du plan qualité est justifié par le titulaire et approuvé par le CNRS avant d'être mis en œuvre.	0
QUA_003	Le titulaire identifie dans son équipe projet les rôles de rédaction et mise à jour du plan assurance qualité, de mise en œuvre opérationnelle des dispositions d'assurance et contrôle qualité.	1
QUA_062	Le titulaire définit dans le PAQ et met en œuvre les contrôles, revues ou audits qualité qu'il juge nécessaires et suffisants dans le contexte du projet, afin de garantir au CNRS la qualité de la prestation et du produit fourni.	1
QUA_004	Le titulaire définit une démarche d'amélioration continue décrivant les dispositions générales mises en œuvre pour faire progresser la qualité de la prestation et du produit fourni (chapitre du PAQ ou document à part). Il met en œuvre cette démarche tout au long de l'accord cadre. Il livre et présente au CNRS un bilan et un plan de progrès à la fin de chaque version majeure mise en production. En phase de maintenance, il livre et présente annuellement au CNRS un bilan de l'année passée et un plan de progrès pour l'année à venir.	1

5.2 ORGANISATION DES EQUIPES PROJET

5.2.1 Organisation de l'équipe CNRS/Inserm

La composition de l'équipe CNRS/Inserm pour le suivi de l'application NEO est la suivante :

Equipe CNRS :

- **un responsable métier** (MOA) appartenant à la Coordination Nationale de Prévention et Sécurité du CNRS et s'appuyant sur les représentants des différentes MOA, des experts métier et des utilisateurs, pour définir les besoins métier, les prioriser, valider l'application fonctionnellement et mettre en œuvre la conduite du changement.
- **un chef de projet informatique** (MOE), appartenant à la DSI du CNRS ; ce responsable est garant de l'intégration dans le SI CNRS. Il s'appuie sur une **équipe projet maîtrise d'œuvre** (MOE) dédiée au projet avec un responsable

technique pour la partie infrastructure système et réseau et sur des équipes transverses à la DSI (urbanisation, outils d'intermédiation, architecture applicative, sécurité, qualité-méthodes, graphisme...).

Equipe Inserm :

- un **responsable informatique (MOE)**, appartenant à l'Inserm et en charge du suivi de l'application pour le compte de l'Inserm.
- un **responsable métier (MOA)** appartenant à l'Inserm ; ce responsable est garant de la solution fonctionnelle NEO pour l'Inserm. Il participe aux expressions de besoins avec la MOA du CNRS, gère l'assistance des utilisateurs Inserm et effectue les recettes pour le compte de l'Inserm.

Groupe d'utilisateurs CNRS/Inserm :

- Il est composé d'IRPS, d'AP, d'acteurs de la CNPS, de conseillers prévention dans des universités contribuant à exprimer des besoins et pouvant participer à des recettes.

Responsable de la TMA :

L'interlocuteur privilégié du titulaire pour les relations contractuelles est le **chef de projet informatique** de la DSI du CNRS, responsable du suivi de l'accord-cadre pour le CNRS/Inserm.

5.2.2 Organisation et gestion des compétences de l'équipe projet du titulaire

Le titulaire met en œuvre une organisation et une gouvernance pour piloter l'accord-cadre. Il identifie les compétences nécessaires et s'assure du maintien de ces compétences tout au long de l'accord-cadre.

Référence	Libellé exigence	Priorité
QUA_005	Le titulaire définit dans le PAQ et met en œuvre une organisation et une gouvernance pour piloter l'accord-cadre, en regard de celle du CNRS. Il identifie les profils types (a minima : chef de projet - interlocuteur privilégié du CNRS, responsable technique - architecte, responsable sécurité, responsable qualité et développeur). Il précise pour chaque profil les compétences associées et le taux de disponibilité minimal.	1
QUA_006	Le titulaire propose dans le PAQ et met en œuvre une organisation des équipes adaptée aux différentes prestations de l'accord-cadre et aux phases de la méthode de développement du projet.	1
QUA_008	Le titulaire communique au CNRS une matrice de couverture des profils types et compétences par l'équipe projet ainsi que l'identité et le CV de chaque membre de l'équipe dès la notification de l'accord-cadre et à chaque changement d'un membre de l'équipe projet.	1
QUA_009	Le titulaire s'engage sur une équipe ferme pour le démarrage de l'accord-cadre, a minima pour les profils types de chef de projet et responsable technique.	1
QUA_010	Le titulaire assure tout au long de la durée de l'accord-cadre : <ul style="list-style-type: none"> ■ le maintien de la qualité : respect des profils types déposés dans l'offre du titulaire pour chacun des intervenants ; ■ le maintien de la continuité : pas plus d'un changement au cours d'une période de six (6) mois glissants parmi les profils clés du titulaire, sauf en cas de force majeure. 	1
QUA_011	En cas de nécessité de remplacement d'un membre de l'équipe, la période de recouvrement est comprise a minima entre deux (2) semaines et un (1) mois en fonction du profil. Ce délai de transfert de compétences et de connaissances du contexte du CNRS et du projet est défini en accord avec le CNRS et strictement respecté.	1
QUA_012	Le titulaire informe le CNRS par écrit de tout changement concernant l'équipe projet avec un préavis de trois (3) mois pour les profils clefs ou un (1) mois sinon.	1
QUA_013	Le titulaire met en œuvre des dispositions pour gérer la variation de charges de son équipe afin de garantir sa flexibilité et sa réactivité en fonction de l'activité du projet.	1

5.3 DISPOSITIFS DE CONDUITE DE PROJET

5.3.1 Structures de pilotage projet

Les principales structures à mettre en place entre le CNRS/Inserm et le titulaire pour assurer le bon déroulement du projet sont décrites ci-dessous :

- **Comité contractuel (MOA/MOE/titulaire) :**
 - il a pour objet le pilotage global des activités du titulaire (y compris qualité et sécurité), ainsi que le suivi de l'avancement des activités (risques, indicateurs, planning global, ressources, suivi financier). Il décide du lancement d'une nouvelle prestation et dans ce cadre, valide la commande ;
 - il est composé pour le CNRS/Inserm du responsable de l'accord-cadre, des responsables d'application et métier, du responsable du département SIRHSPSD, de membres des équipes projet en fonction de l'ordre du jour, d'un éventuel représentant des départements qualité et sécurité et de la direction de la DSI, et pour le titulaire, a minima, du chef de projet ;
 - pour chaque réunion de comité, un ordre du jour systématique et un document support sont diffusés au préalable, aux participants et un compte-rendu est rédigé et envoyé à son issue. Le CNRS/Inserm valide le compte-rendu dans les cinq jours. A défaut de réponse, le compte-rendu est réputé approuvé par le CNRS/Inserm.
- **Comité opérationnel (MOE/titulaire) :**
 - il a pour objet le pilotage régulier des activités du titulaire, ainsi que le suivi opérationnel du projet (suivi des actions, des versions et livraisons...) ;
 - il est composé pour le CNRS/Inserm des responsables d'application, des responsables métier, de membres des équipes projet en fonction de l'ordre du jour et pour le titulaire, a minima, du chef de projet ;
 - pour chaque réunion de comité, l'ordre du jour est systématique ainsi qu'un compte-rendu diffusé aux participants. Le CNRS/Inserm valide le compte-rendu dans les cinq jours. A défaut de réponse, le compte-rendu est réputé approuvé par le CNRS/Inserm.

Référence	Libellé exigence	Priorité
QUA_014	Le titulaire met en œuvre et participe aux comités contractuel selon une fréquence trimestrielle ou définie en accord avec le CNRS.	1
QUA_015	Le titulaire met en œuvre et participe aux comités opérationnels selon une fréquence mensuelle au départ, puis bimensuelle en fonction de l'activité en cours, ou définie en accord avec le CNRS.	1
QUA_016	Le titulaire fournit aux participants des comités un document support dans les deux jours ouvrés précédant la réunion.	1
QUA_017	Le titulaire rédige et adresse le compte-rendu des comités aux participants dans les deux jours ouvrés consécutifs au comité.	1
QUA_018	Le titulaire propose dans le PAQ et met en œuvre toute autre structure de pilotage adaptée aux différentes prestations de l'accord-cadre.	1

5.3.2 Pratiques de gestion de projet

Le CNRS/Inserm souhaite qu'a minima le titulaire mette en œuvre les pratiques de gestion de projet suivantes :

Référence	Libellé exigence	Priorité
QUA_020	Chaque réunion ou point téléphonique entre le titulaire et le CNRS fait l'objet d'une trace écrite (courriel, compte-rendu de réunion) rédigée par le titulaire et à valider par l'ensemble des participants dans un délai fixé par les 2 parties.	1
QUA_021	Chaque courriel envoyé suit les préconisations suivantes : <ul style="list-style-type: none"> ■ préfixer l'objet du message avec le nom du projet : « [Nom projet] sujet » ; ■ si nécessaire, indiquer l'urgence attendue pour la réponse en précisant URGENT dans l'objet du message « [nom-projet] URGENT sujet » ; ■ dans le corps du message, préciser ce qui est attendu du destinataire : simple information, avis, décision, action... Si nécessaire, indiquer la date d'échéance attendue pour la réponse ; ■ éviter les pièces jointes, les remplacer par des liens vers l'outil collaboratif du CNRS. 	1

Référence	Libellé exigence	Priorité
QUA_022	Le titulaire suit et informe le CNRS des actions identifiées lors des comités ou réunions diverses avec le CNRS.	1
QUA_023	Le titulaire tient à jour et diffuse au CNRS un planning du projet, global pour l'ensemble du projet et détaillé pour la phase à venir.	1
QUA_024	Le titulaire gère les risques du projet qui ont été formalisés dans son offre et ajustés lors du démarrage et tout au long de l'accord-cadre.	1
QUA_025	Le titulaire définit les procédures d'alertes et d'arbitrage.	1
QUA_026	Le titulaire met en œuvre une procédure de gestion de crise en cas d'alerte avérée. Il précise le processus d'escalade suivi pour le traitement et la résolution de ces problèmes.	1

La gestion de crise s'impose dans le cas d'incident persistant (délai de résolution indéterminable, correction impossible ou inefficace), d'incident de sécurité de grande envergure (attaque virale), d'incidents multiples, de risque d'altération de données (perte de sauvegarde, ...), de risque avéré sur le fonctionnement et les missions du CNRS ou de l'Inserm (atteinte à l'image de marque), et de l'occurrence de tout événement à caractère improbable ou de criticité catastrophique (atteinte à la sauvegarde des personnes ou des biens).

5.3.3 Indicateurs de pilotage et qualité du projet

Des indicateurs pertinents sont définis pour permettre de suivre l'avancement du projet et d'anticiper la survenance des difficultés. Ces indicateurs sont mesurés régulièrement et présentés par le titulaire lors des différents comités.

Les indicateurs que le CNRS souhaite suivre sont notamment les suivants :

- indicateurs de pilotage :
 - état d'avancement des prestations en cours (livrées, recettées, facturées)
 - coûts et ressources prévues, affectées, consommées
 - turnover de l'équipe projet
 - respect des délais de diffusion des documents pour les comités
 - taux de satisfaction client
- indicateurs de qualité du code :
 - taux de couverture des tests unitaires automatisés
 - taux de commentaires
 - convention de nommage
 - complexité du code, couplage
 - mesures de performance
- indicateurs de qualité des livraisons :
 - respect des délais de livraison
 - nombre d'anomalies ⁴ (bloquantes, majeures, mineures) en recette et en production, ratio nombre anomalies/charge commandée, nombre d'anomalies imputables à des régressions
 - nombre de livraisons nécessaires au prononcé de la validation (documents et logiciels)

Le titulaire peut proposer de nouveaux indicateurs, dans la mesure où ils permettent de piloter efficacement le projet.

Le plan de mesure explicite les indicateurs, leurs modalités de calculs (formule, période retenue, outillage), leurs objectifs à atteindre et leurs modalités de suivi.

Référence	Libellé exigence	Priorité
QUA_027	Le titulaire fournit au CNRS un plan de mesure (chapitre du plan assurance qualité ou document à part) adapté à la méthode de développement du projet. Le plan de mesure est ajusté d'un commun accord avec le CNRS lors du démarrage de l'accord-cadre. Il est mis à jour tant que de besoin tout au long de l'accord-cadre avec l'accord des deux parties.	1
QUA_028	Le titulaire élabore, maintient et livre lors des différents comités les tableaux de bord conformes au plan de mesure comprenant les indicateurs adaptés au niveau du comité concerné.	1

⁴ La définition et la typologie des anomalies sont décrites dans le glossaire du Livret 2 du CCTP.

5.4 METHODE DE DEVELOPPEMENT

5.4.1 Cycle de vie

Les activités à mener tout au long du projet se répartissent de la manière suivante :

- expression des besoins (à la charge du CNRS/Inserm) ;
- réalisation (à la charge du titulaire) : spécifications fonctionnelles et techniques détaillées, conception, paramétrage ou développements spécifiques, tests unitaires, d'intégration, de validation, de non-régression, de performance et de sécurité ;
- recette (à la charge du CNRS/Inserm, avec assistance éventuelle du titulaire) : validation des développements en environnement de recette ;
- mise en production (à la charge du CNRS/Inserm, avec assistance éventuelle du titulaire) : initialisation du système, mise en production ;
- en parallèle, conduite du changement (à la charge du CNRS/Inserm, avec assistance éventuelle du titulaire) : communication, formation des utilisateurs, documentations utilisateurs, organisation de l'assistance.

Pour l'enchaînement de ces activités, le CNRS préconise un cycle de vie itératif et incrémental⁵, découpé en plusieurs versions mises en production sur décision du CNRS/Inserm. Chaque version suit globalement un cycle en cascade.

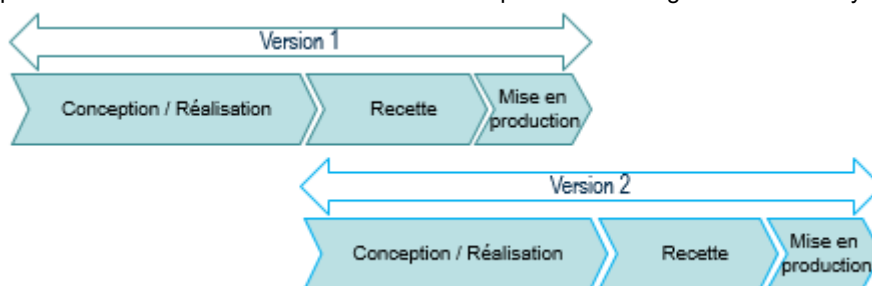


Figure 22 : Cycle de vie en cascade itératif et incrémental

Toutes les dispositions mises en œuvre par le titulaire pour donner visibilité sur la réalisation d'une version en cours sont appréciées par le CNRS/Inserm.

Afin de vérifier l'avancement régulier des travaux et de détecter en amont les problèmes, le titulaire peut planifier, en accord avec le CNRS/Inserm, une ou plusieurs mises à disposition intermédiaires des produits de la commande. Elles donnent lieu, le cas échéant et selon le livrable, à des remarques pour les documents ou des déclarations d'anomalies (pour l'application). Elles ne donnent pas lieu à des opérations de réception au sens du CCAP.

Référence	Libellé exigence	Priorité
QUA_029	Le titulaire définit dans le PAQ et met en œuvre une méthode de développement itérative-incrémentale, adaptée au contexte du projet ou de l'évolution. Il identifie les phases, entrées attendues, activités, rôles et livrables fournis.	1
QUA_031	Le titulaire, en accord avec le CNRS, définit le périmètre des versions et des itérations en fonction des exigences fonctionnelles (priorités des utilisateurs), ergonomiques, techniques et dans un objectif de réduction des risques.	1
QUA_030	Dans le cas où le CNRS demande une méthode de développement orientée agile, Scrum est préconisé (cf. https://www.scrum.org). Le titulaire définit dans le PAQ les modalités de sa mise en œuvre opérationnelle. Le cycle de développement de l'application est découpé en versions mises en production, elles-mêmes composées d'itérations (sprints de durée fixe) permettant de disposer rapidement de nouvelles fonctionnalités. Les activités à réaliser, les livrables attendus et l'outillage de suivi et pilotage du projet demeurent les mêmes qu'en mode non orienté agile. L'ensemble de la documentation est créée, mise à jour et livrée de façon itérative et incrémentale.	1

⁵ La notion d'incrémental sous-entend ici qu'une première itération de la mise en œuvre d'une fonctionnalité peut être suivie d'une deuxième itération visant à la compléter ou la modifier au vu de ce qu'a matérialisé la première itération mais également au vu de ce que l'ajout d'autres fonctionnalités a pu mettre en évidence pour l'utilisateur.

Référence	Libellé exigence	Priorité
QUA_007	Dans le cas où le CNRS demande une méthode de développement orientée agile, le titulaire définit dans le PAQ les rôles spécifiques liés au mode agile (<i>par exemple</i> : product owner, proxy product owner, scrum master, équipe de développement). L'attribution des rôles aux membres des équipes CNRS et titulaire se fait en concertation avec le CNRS.	1
QUA_019	Dans le cas où le CNRS demande une méthode de développement orientée agile, le titulaire définit dans le PAQ les objectifs, la fréquence ainsi que les participants du titulaire et du CNRS pour chaque rituel mis en place (<i>par exemple</i> : <i>sprint planning</i> , <i>daily scrum</i> , <i>sprint review</i> , <i>sprint retrospective</i>).	1

5.4.2 Activités de réalisation (à la charge du Titulaire)

Le titulaire conduit les travaux de réalisation en respectant les exigences applicables.

Afin de minimiser les phases de recette du CNRS (nombre d'anomalies⁶ minimal et période réduite de tests de recette), le titulaire maximise la qualité des documents de conception et du code produit et propose une organisation pertinente quant à ses propres tests (organisation, outillage...).

Référence	Libellé exigence	Priorité
QUA_032	Le titulaire décrit dans le PAQ le déroulement des ateliers de travail avec le CNRS : leur déclenchement en lien avec le cycle de vie du projet, leurs modalités de déroulement, les supports produits (avant, après et dans quels délais).	1
QUA_033	Le titulaire intègre dans sa démarche de conception de la solution une méthode d'analyse de l'expérience utilisateur (UX) afin de prendre en compte les critères de satisfaction de l'utilisateur.	2
QUA_034	Le titulaire s'appuie sur une maquette pour faire valider au CNRS, avant codage, les règles d'ergonomie, de présentation des écrans et de navigation dans l'application.	1
QUA_035	Les spécifications fonctionnelles détaillées sont formalisées sous forme de cas d'utilisation et de diagrammes UML.	1
QUA_036	Le titulaire définit dans le PAQ la stratégie de tests qu'il met en place pour le projet, en couverture des exigences fonctionnelles, techniques et d'interface. Il en précise également les différents niveaux (unitaire automatisé ou manuel, d'intégration, de validation, de non-régression, de performance unitaire et/ou plus global, de sécurité) et l'outillage associé.	1
QUA_037	Le titulaire adapte l'activité de test à la méthode de développement du projet.	1
QUA_038	Dans le cas où le CNRS demande une méthode de développement orientée agile, le titulaire définit dans le PAQ et met en œuvre : <ul style="list-style-type: none"> - l'utilisation de user stories permettant de spécifier le contenu du backlog de chaque itération (tout en assurant la rédaction finale des spécifications fonctionnelles détaillées sous forme de cas d'utilisation), - des techniques de tests adaptées (tels que Test Driven Development, Acceptance Test-Driven Development...). 	1

5.4.3 Activités de recette (à la charge du CNRS / Inserm)

Le CNRS rédige son cahier de recette pour ses propres tests. En aucun cas, ce cahier ne peut être utilisé par le titulaire pour passer ses tests d'intégration ou de validation.

La recette CNRS est composée de différents types de tests :

- fonctionnels, techniques, intégration dans le SI, sécurité (par la maîtrise d'œuvre DSI) ,
- métier (par les maîtrises d'ouvrage).

Une analyse de la qualité du code et de l'architecture logicielle peut également être réalisée par la DSI (en plus des comptes rendus et indicateurs fournis par le titulaire).

Le CNRS passe des scénarios de tests en environnement de recette à chaque livraison logicielle ou évolution du paramétrage.

⁶ La définition d'une anomalie est décrite dans le glossaire du Livret 2 du CCTP.

Les résultats des tests du CNRS sont consignés dans des dossiers de tests ou dans l'outil de gestion des tests de recette du CNRS.

Les anomalies détectées par le CNRS sont formalisées et classifiées selon 3 niveaux de gravité (cf. glossaire du Livret 2 du CCTP) dans l'outil de gestion des anomalies et évolutions du CNRS.

Référence	Libellé exigence	Priorité
QUA_039	Le titulaire s'engage à corriger la totalité des anomalies issues de la recette avant mise en production, sauf dérogation explicite du CNRS.	0

5.5 GESTION DES ENVIRONNEMENTS

5.5.1 Postes de travail du titulaire

Le titulaire respecte les contraintes suivantes pour les postes de travail de tous les membres de son équipe :

Référence	Libellé exigence	Priorité
ENV_001	Le titulaire fournit pour ses équipes, les postes de travail, imprimantes, scanner... et les logiciels, ainsi que les fournitures bureautiques, y compris lorsque la réalisation s'effectue dans les locaux du CNRS.	0
ENV_002	Le titulaire respecte les contraintes du cadre de cohérence technique (CCT) au niveau de la connectivité SSL, et regroupe dans un réseau dédié tous les postes de travail non hébergés dans les locaux du CNRS et devant accéder aux ressources serveurs et bureautiques du CNRS.	0

5.5.2 Environnement de développement

La plate-forme de développement et de tests unitaires mise en œuvre par le titulaire doit respecter les contraintes suivantes :

Référence	Libellé exigence	Priorité
ENV_003	Le titulaire met en œuvre une plate-forme de développement et tests pour son besoin propre, compatible avec l'environnement cible de production qui fait référence.	0
ENV_004	Le titulaire implémente sur la plate-forme de développement des « bouchons » afin de simuler des connexions aux services d'infrastructures qui seront utilisés sur les autres environnements (en particulier l'EAI/ESB et le service d'authentification).	0

5.5.3 Environnements CNRS

Le CNRS/Inserm fournit et administre l'ensemble des plates-formes serveurs du projet à l'exception de la plate-forme de développement et de tests du titulaire :

- Un environnement d'Intégration si fourni par le CNRS (actuellement non existant) : cet environnement permet au titulaire de tester le déploiement et l'intégration de l'application dans le SI du point de vue technique uniquement (authentification et flux EAI/ESB compris).
- Un environnement de Recette : cet environnement permet au CNRS et à l'Inserm de réaliser les tests de recette (Vérification d'Aptitude) de l'application avant mise en production.
- Un environnement de Production : cet environnement héberge l'application accessible aux utilisateurs et permet au CNRS de réaliser la Vérification de Service Régulier.

Le CNRS/Inserm est responsable des briques mutualisées comme les frontaux web, le SSO (Single Sign-On) et les serveurs de base de données.

Le CNRS/Inserm est responsable (installation et exploitation) des composants d'infrastructures, OS, stockage, réseau, sur tous les environnements (intégration, recette et production). La configuration logicielle des environnements de recette est la même que celle de production, alors que la configuration de l'infrastructure sous-jacente (CPU, RAM, ...) est équivalente ou proportionnelle (selon les projets) à celle de l'environnement de production.

Le CNRS/Inserm assure l'exploitation applicative des environnements de recette et production.

Le CNRS utilise l'outil Ansible Tower pour automatiser les déploiements des applications lorsque cela est possible.

Les exigences suivantes s'appliquent au paysage applicatif précité :

Référence	Libellé exigence	Priorité
ENV_005	Un environnement d'intégration est préparé par le CNRS. Il est ensuite à la charge du titulaire de procéder aux installations applicatives sur cet environnement. Le titulaire est autonome sur cet environnement.	1
ENV_006	Les environnements de recette, de formation et de production ne sont pas accessibles au titulaire. Cependant, en cas de besoin, le CNRS demande au titulaire d'y accéder, sur site CNRS uniquement.	0

5.6 GESTION DES LIVRAISONS

La réalisation d'une commande par le titulaire donne lieu par celui-ci à la mise à disposition des livrables mentionnés dans chaque prestation (cf. Livret 2). La procédure de livraison s'effectue selon les modalités suivantes :

Référence	Libellé exigence	Priorité
QUA_040	Chaque livraison d'un produit fini effectuée par le titulaire est accompagnée d'un bon de livraison, précisant la version des composants livrés (application ou document), la liste des exigences et des modifications implémentées, en particulier la liste des fiches de relecture prises en comptes ou la liste des anomalies corrigées dans la version. Ce bon de livraison est déposé par le titulaire dans l'outil collaboratif du CNRS.	1
QUA_041	Un courriel est adressé à l'équipe projet CNRS l'informant de la mise à disposition de la livraison et contenant un lien vers le bon de livraison.	1
QUA_042	Pour les livraisons documentaires, le titulaire utilise l'outil collaboratif du CNRS.	1
QUA_043	Pour les livraisons applicatives, le titulaire utilise la forge DSI, pour y déposer l'ensemble des composants de l'application et les manuels d'installation et d'exploitation (cf. « Description des livrables documentaires » en annexe du Livret 2) qui permettent au CNRS de mettre en œuvre et d'exploiter l'application livrée.	1
QUA_044	Tous les éléments fournis lors d'une livraison applicative (y compris le code source) permettent d'identifier l'application concernée et sa version livrée. Toute version de l'application est identifiée par un numéro de version unique : version.sous-version.état technique[-rcN] : <ul style="list-style-type: none"> le numéro de version est incrémenté à chaque évolution fonctionnelle importante, le numéro de sous-version : lors d'une évolution fonctionnelle minime, l'état technique : lors d'une correction logicielle (par rapport à la version en production), [-rcN] : (optionnel) numéro de Release Candidate pour les livraisons en recette ; ce numéro de Release Candidate n'est pas présent dans la version finale (pour la production) 	1
QUA_045	En cas de livraison d'un delta, le titulaire procède à une re-livraison totale une fois la version stabilisée.	1
QUA_046	En accord avec le CNRS, les livraisons applicatives peuvent être accompagnées d'une démonstration de l'application par le titulaire, en présence du titulaire et de l'équipe CNRS.	2

5.7 GESTION DE LA DOCUMENTATION

La documentation produite par le titulaire doit être de qualité et permettre une bonne compréhension des mécanismes développés à des fins d'exploitation et de maintenabilité.

Référence	Libellé exigence	Priorité
QUA_047	Tous les documents produits dans le cadre du présent accord-cadre sont livrés sous format électronique modifiable (donc pas uniquement en pdf).	1

Référence	Libellé exigence	Priorité
QUA_048	Les documents du projet sont déposés et partagés par le CNRS et le titulaire dans l'outil collaboratif du CNRS.	1
QUA_049	Le titulaire remet à l'issue de l'accord-cadre l'ensemble de la documentation fonctionnelle et technique de l'application à jour (créée et modifiée tout au long de l'accord-cadre).	0

L'objectif du CNRS est de tendre vers l'application de dispositions communes pour la documentation des différentes applications. Dans le cas de l'application NEO où il existe des principes de gestion de la documentation spécifiques, ils sont appliqués tels quels ou évoluent sur demande du CNRS/Inserm.

Les principes de gestion de la documentation préconisés au CNRS sont les suivants :

Référence	Libellé exigence	Priorité
QUA_050	Tout document produit contient : le nom du document, une référence, la date de dernière mise à jour, la version, l'historique des versions (si besoin), le sommaire, les pages numérotées, les marques de révision apparentes d'une version à l'autre (si besoin).	1
QUA_051	<p>Chaque document reçoit une référence unique au sein du projet (nom du fichier) :</p> <p style="text-align: center;">Nom-du-projet_Identification-du-document_[Confidentialité_]Vx.y ou Nom-du-projet_Identification-du-document_[Confidentialité_]Date-evenement</p> <p>avec :</p> <ul style="list-style-type: none"> ■ Identification-du-document = nom représentatif du contenu, de la forme : Type-document_[Code-domaine]_Libelle-libre ■ Confidentialité : code indiquant le niveau de confidentialité du document, DL, DC ou DR ■ Vx.y : version du document pour les documents de référence ■ Date-evenement au format AAAAMMJJ pour les documents événementiels (CR de réunion...). <p>La référence du document ne contient aucun caractère accentué ni espace (à remplacer par « - »).</p>	1
QUA_052	<p>Chaque document mentionne dans sa référence le code de confidentialité. Seuls les documents de niveau classification PUBLIC (cible de diffusion non contrôlée : la publication de l'information présente un impact nul pour l'organisme) n'ont pas de code de classification. Les différents codes et niveaux de classification sont les suivants :</p> <ul style="list-style-type: none"> ■ DL : DIFFUSION LIMITEE + Mention pour une information dont la cible n'est pas nominative mais dont la mention précise les structures ou entités destinataires de l'information ou des personnes es-qualité. La mention spécifique associée au niveau de classification peut être suffisante pour définir la liste de diffusion. Une divulgation non autorisée de l'information aurait un impact modéré ; ■ DC : DIFFUSION CONFIDENTIELLE pour une information dont la cible n'est pas nominative mais précise les structures ou entités destinataires de l'information, des personnes es-qualité et qui doit être diffusée via un canal dont l'accès est strictement contrôlé. Une divulgation non autorisée de l'information aurait un impact important ; ■ DR : DIFFUSION RESTREINTE conformément à l'II901 pour une information dont la cible est nominative ou précise les structures ou entités destinataires de l'information, des personnes es-qualité ayant besoin d'en connaître et qui doit être diffusée via un canal dont l'accès est strictement contrôlé. Une divulgation non autorisée de l'information aurait un impact catastrophique. 	1
QUA_053	Pour chaque document, un marquage est apposé afin de signifier le niveau de protection et les mesures réglementaires à appliquer en ce qui concerne la communication, la diffusion, la reproduction, la conservation et la destruction de ceux-ci : le niveau de classification (DIFFUSION LIMITEE, DIFFUSION CONFIDENTIELLE ou DIFFUSION RESTREINTE) est apposé en haut de chaque page en caractères gras, rouge et en capitales.	1

Référence	Libellé exigence	Priorité
QUA_054	Le numéro de version du document est incrémenté à chaque modification du contenu du document devant faire l'objet d'une diffusion (il n'est pas incrémenté pour des corrections portant sur la forme du document - fautes de frappe, d'orthographe, ...). Le numéro de version est de la forme : x.y, avec : <ul style="list-style-type: none"> x : incrémenté à chaque évolution majeure du document (<i>par exemple</i>, ajout de chapitres, changement de version de l'application, refonte du document...) y : incrémenté à chaque évolution mineure (<i>par exemple, prise en compte de remarques de relecture, ajout de précisions...</i>). 	1
QUA_055	Les documents du projet sont initiés à partir de modèles. Ces modèles sont définis au démarrage de l'accord-cadre et référencés dans le plan assurance qualité. Ils peuvent être issus soit du fonds documentaire du CNRS soit de celui du titulaire.	1

Le CNRS/Inserm formalise ses remarques au travers d'une fiche de relecture pour les documents qui ont fait l'objet d'une livraison, par marques de révision dans le document pour les comptes rendus et les mises à dispositions intermédiaires.

Une partie de la documentation peut éventuellement être gérée dans le Wiki du CNRS.

Les règles et pratiques à mettre en œuvre autour de la gestion documentaire sont ajustées d'un commun accord au démarrage de l'accord-cadre.

5.8 CAPITALISATION DES CONNAISSANCES

La capitalisation des connaissances acquises lors de l'exécution des prestations est un facteur clés de succès, tant pendant la durée d'exécution de l'accord-cadre que lors de la phase de réversibilité éventuelle en fin d'accord-cadre. A ce titre, le titulaire met en œuvre les pratiques suivantes :

Référence	Libellé exigence	Priorité
QUA_056	Le titulaire identifie les informations ne relevant pas de la documentation, nécessaires à ses équipes pour exécuter correctement les prestations objet de l'accord-cadre. Il peut s'agir, sans que la liste ne soit exhaustive, de procédures, de guides opératoires, d'une base de connaissance, ... Il s'assure également de leur suivi, de leur mise à jour et de la gestion de leur obsolescence.	1
QUA_057	Le titulaire rend compte de l'avancement de la mise en œuvre du système de capitalisation pendant le comité opérationnel du projet.	1
QUA_058	Le titulaire livre annuellement ou à la demande les informations relevant de la capitalisation des connaissances dans les formats compatibles avec les outils du CNRS.	1

5.9 OUTILLAGE DE SUIVI ET PILOTAGE DU PROJET

Le CNRS utilise les outils suivants :

- gestion des anomalies et des évolutions : Mantis (<https://www.mantisbt.org/>)
- assistance : e-dem, basé sur JIRA Service Desk (désormais Jira Service Management <https://www.atlassian.com/fr/software/jira/service-management>)
- base de connaissance, wiki : Confluence (<https://fr.atlassian.com/software/confluence>)
- gestion documentaire, collaboratif : CoRe, basé sur Microsoft SharePoint (<https://www.microsoft.com/fr-fr/>)
- modélisation : PowerAMC (<https://www.sap.com/france/products/powerdesigner-data-modeling-tools.html>)
- gestion des tests de recette : TestLink (<http://www.testlink.org/>)

Référence	Libellé exigence	Priorité
QUA_059	Le titulaire utilise les outils ci-dessous, fournis par le CNRS : <ul style="list-style-type: none"> l'outil libre Mantis, pour le suivi des anomalies et du portefeuille de demandes d'évolution, <i>si demandé par le CNRS</i>, l'outil e-dem, basé sur JIRA Service management, pour le suivi des incidents, problèmes et demandes, associé à une base de connaissance dans le wiki Confluence l'outil CoRe, basé sur la plate-forme collaborative MS SharePoint, pour le partage des documents, livraisons documentaires, calendriers, annuaires, suivi d'actions... 	1
QUA_060	Le CNRS se réserve la possibilité de changer l'un ou l'autre des outils présentés ci-dessus, au cours de la durée de vie de l'accord-cadre. Dans ce cas, le titulaire en est informé suffisamment à l'avance et procède également au changement d'outillage dans ses relations avec le CNRS. Ce changement est réputé n'avoir aucun impact financier quant à l'exécution du présent accord-cadre.	1

Ces outils sont mis en œuvre et paramétrés par le CNRS. Ils sont accessibles par les équipes maîtrise d'œuvre et maîtrise d'ouvrage CNRS, et le sont également par le titulaire (avec des profils différents). Les pratiques mises en place autour de ces outils sont préconisées par la cellule qualité de la DSI du CNRS, elles sont communiquées au titulaire et ajustées d'un commun accord au démarrage de l'accord-cadre.

Référence	Libellé exigence	Priorité
QUA_061	Le titulaire met en œuvre des outils bureautiques et de gestion de projet qui supportent des formats compatibles avec les outils utilisés ou préconisés par le CNRS, mais non fournis au titulaire : <ul style="list-style-type: none"> suite bureautique : MS Office, gestion de projet : MS Project, modélisation des données : PowerAMC, dossiers et suivi des tests : TestLink, wiki : Confluence. 	1

Le titulaire peut le cas échéant proposer d'autres outils pour compléter ceux proposés par le CNRS. Toutefois, ceux-ci seront soumis à acceptation par celui-ci.

5.10 MESURES ET CLAUSES DE SECURITE

5.10.1 Gestion de la Sécurité par le titulaire

Responsabilité

Référence	Libellé exigence	Priorité
SECU_001	L'organisation de la sécurité des systèmes d'information du titulaire pour le projet est décrite dans le PAS. L'équipe comporte a minima : <ul style="list-style-type: none"> Une personne de niveau hiérarchique supérieur formée et compétente en SSI capable de prendre des décisions dans la conduite du projet, responsable du respect des dispositions du PAS Une personne intégrée ou proche des équipes de MOE du titulaire en charge du projet responsable de la mise en œuvre du PAS La rédaction, la mise à jour et le suivi du PAS sont à la charge du titulaire 	0

Dans l'exercice de leurs activités, les intervenants sont liés par un devoir de réserve et astreints au secret professionnel.

Sensibilisation, qualification et formation

Référence	Libellé exigence	Priorité
SECU_002	Le titulaire indique au CNRS la fréquence et le contenu des actions de formation et de sensibilisation de ses personnels aux enjeux et aux méthodes de Sécurité.	0

5.10.2 Protection des biens

Protection des sites

Référence	Libellé exigence	Priorité
SECU_003	Si le titulaire exécute les prestations à partir de ses propres locaux ou en télétravail, il opère en « <i>site sûr</i> » dont les caractéristiques sont à évaluer avec le département Sécurité de la DSI. Cette disposition est également valable pour le support ou la maintenance à distance. Le titulaire ne détient à aucun moment de données de production significatives sur ses infrastructures. Le cas échéant, le titulaire réalise un dossier de type « <i>site sûr</i> » incluant les modalités d'accès aux ressources de la DSI et les mesures de sécurité nécessaires à l'accomplissement des prestations. Si un Plan d'Assurance Sécurité existe, le dossier « <i>site sûr</i> » lui sera annexé. En cas de télétravail, aucun accès aux environnements ou aux données de production n'est autorisé.	0
SECU_004	Le titulaire fournit un dossier de site sûr décrivant les mesures de sécurité physique en place dans les locaux qu'il utilise pour l'accomplissement des prestations. Ce dossier traite des thématiques suivantes sous les angles technique et organisationnel : <ul style="list-style-type: none"> ■ Infrastructures informatiques (réseaux et systèmes) ■ Contrôle d'accès physique aux locaux ■ Contrôle d'accès logique aux systèmes ■ Postes de travail ■ Liaisons réseaux externes (WAN, réseaux privés avec le CNRS) ■ Plan de reprise/de continuité d'activité ■ Télétravail ordinaire et télétravail exceptionnel ■ Gestion de crise 	0

Protection du système d'information

Référence	Libellé exigence	Priorité
SECU_005	Le titulaire dispose de dispositifs, de procédures et de moyens qu'il met en œuvre afin protéger les actifs du CNRS. Ces moyens permettent en particulier de : <ul style="list-style-type: none"> ■ contrer les virus et codes malveillants ■ protéger son réseau contre les intrusions. Il décrit les mesures mises en œuvre.	0

Politique de contrôle d'accès

Référence	Libellé exigence	Priorité
SECU_006	Le titulaire dispose d'une politique, de mesures et de dispositifs pour gérer le contrôle d'accès à ses locaux et à ses systèmes d'information. Cette politique concerne notamment : <ul style="list-style-type: none"> ■ la politique d'attributions des droits ■ les méthodes d'accès (authentification et autorisation) ■ la gestion des identifiants uniques ■ la politique de mots de passe et de gestion de l'authentification forte ■ les processus d'autorisation pour l'accès et les privilèges des utilisateurs ■ les processus de gestion des listes de personnes autorisées à participer aux activités de TMA ■ les processus de révocation des droits ■ la politique et les processus de révision des droits d'accès ■ le contenu de la charte interne utilisateur et/ou de la charte interne administrateur Le titulaire décrit les mesures en place. Il fournit en particulier sa PSSI d'entreprise.	0

Gestion des vulnérabilités

Référence	Libellé exigence	Priorité
SECU_007	Le titulaire dispose de procédures de gestion interne des vulnérabilités sur le système d'information qu'il met en œuvre pour assurer les activités de développement, de maintenance et de support. Il décrit les méthodes et outils en place pour la découverte et le suivi de la correction de ces vulnérabilités.	0

Gestion des incidents

Référence	Libellé exigence	Priorité
SECU_008	Le titulaire dispose de procédures de gestion des incidents internes de sécurité sur le système d'information qu'il met en œuvre pour assurer les activités de développement, de maintenance et de support.	0

Exigences de Sécurité concernant les personnels extérieurs

Référence	Libellé exigence	Priorité
SECU_009	Le titulaire met en œuvre des moyens de contrôle pour s'assurer du respect des exigences de sécurité du CNRS par ses sous-traitants éventuels, ainsi que des consultants ou techniciens amenés à intervenir dans le cadre des prestations. Il fournit les éléments contractuels le liant avec ses partenaires prouvant les obligations qui leur incombent dans ce domaine.	0

Travail dans les zones sécurisées

Référence	Libellé exigence	Priorité
SECU_010	<p>Le titulaire ne doit jamais intervenir physiquement sur un site du CNRS ou géré par le CNRS sans être mandaté et surveillé par du personnel du CNRS ou mandaté par le CNRS. Il doit refuser d'assurer sa prestation, si le personnel encadrant du CNRS ou mandaté par le CNRS ne respecte pas son obligation de surveillance. Il notifie l'incident à sa direction et au RSSI de la DSI. Le délai d'exécution de la prestation est suspendu jusqu'à ce que le personnel encadrant du CNRS ait pris les mesures nécessaires à cette surveillance.</p> <p>Le titulaire n'est pas autorisé, sauf autorisation expresse du CNRS, à photographier, faire des enregistrements audio ou vidéo des locaux ou des équipements du CNRS.</p> <p>De même, il est interdit au titulaire d'introduire du matériel photographique, vidéo, audio ou d'autres matériels d'enregistrement dans les locaux du CNRS ou géré par le CNRS, sauf autorisation expresse du CNRS.</p>	0

Stockage et échange d'informations

Référence	Libellé exigence	Priorité
SECU_011	<p>Le titulaire met en œuvre des moyens techniques conformes aux recommandations de l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) afin de protéger de toutes divulgations indésirables volontaires ou accidentelles, toutes les informations relatives au CNRS :</p> <ul style="list-style-type: none"> ■ lors du stockage de celles-ci en dehors des sites physiques du CNRS, pendant et après les prestations. ■ lors des échanges avec le CNRS, quel qu'en soit le moyen (e-mail, partage de fichier, etc.). <p>De plus le titulaire effacera les informations qu'il aura en sa possession, immédiatement et en fournissant au CNRS un quitus formel :</p> <ul style="list-style-type: none"> ■ sur simple demande du CNRS ■ en fin de prestation 	0

Gestion des sauvegardes

Référence	Libellé exigence	Priorité
SECU_012	Le titulaire donne au CNRS l'ensemble des éléments techniques concourant à une sauvegarde intégrale et régulière des données du CNRS qui lui sont confiées et des données nécessaires à l'exécution des prestations (plan de sauvegarde, procédures, script d'arrêt/démarrage, objets à sauvegarder, intégrité temporelle des données, etc.). La solution du titulaire doit permettre au CNRS de mettre en place des tests réguliers de restauration des sauvegardes.	0

Rétrocession des informations du CNRS

Référence	Libellé exigence	Priorité
SECU_013	Le titulaire précise les mesures et dispositifs qui garantissent le retour au CNRS et la destruction des informations du CNRS qu'il a en sa possession à l'expiration ou à la résiliation du marché. Le titulaire fournit au CNRS l'ensemble de la documentation nécessaire et une description précises des éléments techniques permettant au CNRS d'extraire les données de la solution dans un format compréhensible (<i>par exemple fichier csv et schéma relationnel des données</i>). Ces éléments doivent permettre au CNRS de reprendre ces données dans une autre solution le cas échéant.	0

5.10.3 Obligations du titulaire

Référence	Libellé exigence	Priorité
SECU_014	Le titulaire reconnaît être tenu à une obligation de conseil, de mise en garde et de recommandations en termes de sécurité et de mise à l'état de l'art. En particulier, il s'engage à informer le CNRS des risques d'une opération envisagée, des incidents éventuels ou potentiels, et de la mise en œuvre éventuelle d'actions correctives ou de prévention. Le titulaire est responsable du maintien en condition de sécurité des systèmes nécessaires à la réalisation des prestations jusqu'à leur échéance. Le titulaire ne peut se dégager de cette responsabilité que si, après qu'il ait informé le CNRS de failles dans la sécurité du système, de manière circonstanciée, précise et détaillée, et qu'il ait proposé une ou des solutions de nature à pallier la faille, le CNRS a choisi de ne pas mettre en œuvre ces préconisations.	0

5.10.4 Localisation des données

Référence	Libellé exigence	Priorité
SECU_015	Les lieux d'hébergement des données du CNRS, dont les journaux, les jeux d'essai pour les environnements de développement (liste non-exhaustive), satisfont aux exigences de sécurité du donneur d'ordres (CNRS) et aux dispositions de la loi informatique et libertés en vigueur. Tout transfert de données en dehors des Etats de l'UE est soumis à avis, et autorisation préalable du CNRS, après avis de son Délégué à la Protection des Données. Le titulaire communique la liste de tous les lieux de stockage de données (site d'hébergement principal, site(s) de secours, etc.). Si la faisabilité technique de cette exigence s'avère délicate dans le cadre d'architectures distribuées, il est demandé au titulaire d'être en mesure de localiser, a posteriori, et non en permanence, le lieu de stockage des données, en particulier suite à un incident. Enfin, le titulaire doit fournir au CNRS tous les éléments attestant qu'il satisfait bien aux exigences réglementaires ci-dessus, quel que soit la localisation.	0

5.10.5 Audit

Référence	Libellé exigence	Priorité
SECU_016	<p>Le titulaire est informé de la volonté du CNRS de conduire ou organiser des audits réguliers des systèmes d'information. Ces audits techniques et organisationnels ont pour objectifs de vérifier le respect par le titulaire de ses engagements initiaux en termes d'organisation et de moyens mis en œuvre concernant la SSI.</p> <p>Le CNRS peut, à tout moment, à son initiative, par ses propres équipes ou par celles de tiers désignés par lui (sélectionnés sur la liste des prestataires qualifiés en audit SSI publiée sur le site de l'ANSSI à la date de commande de l'audit https://cyber.gouv.fr/produits-services-qualifies?field_type_service_value[passi]=passi), procéder à des audits des prestations confiées au titulaire, afin de :</p> <ul style="list-style-type: none"> ■ vérifier les engagements de niveaux de service, de qualité, de sécurité des prestations réalisées ; ■ vérifier la mise en application des règles d'organisation, des méthodes, des pratiques mises en œuvre pour réaliser les prestations. <p>A cet effet, le CNRS ou son mandataire désigné met en œuvre tous les moyens qu'il juge nécessaire pour s'assurer du parfait achèvement des prestations. Ceci inclut, sans volonté d'exhaustivité :</p> <ul style="list-style-type: none"> ■ la communication de documents tenus à jour par le Titulaire (plans, documentations, contrats, certifications, rapports...) ; ■ l'audition orale d'équipes de maîtrise d'œuvre (techniciens, ingénieurs, responsables techniques, opérationnels, responsables de la sécurité, équipes de direction...) ; ■ la conduite de tout audit organisationnel ou technique, en boîte blanche, noire ou grise. <p>Le CNRS s'engage à respecter un préavis raisonnable conforme aux dispositions du CCAP avant tout déclenchement d'audit.</p> <p>Le résultat des audits est présenté au titulaire, et conduit à la rédaction d'un plan d'action. Les actions inscrites ne conduisent pas à facturation supplémentaire de la part du titulaire si elles découlent directement d'un constat de non-conformité par rapport :</p> <ul style="list-style-type: none"> ■ à ses engagements initiaux ou ■ à la réglementation en vigueur à la date de notification de l'appel d'offres. <p>Dans tous les autres cas (évolution de la réglementation, évolution de la PSSI du CNRS, évolution d'une application modifiant son profil de risque...), le titulaire peut proposer une cotation pour la réalisation des prestations de mise en conformité.</p> <p>Le résultat des audits de conformité aboutit à un avis formel du CNRS</p> <ul style="list-style-type: none"> ■ conforme : l'audit n'a pas révélé de dysfonctionnements majeurs, et les engagements qui ont été audités sont tenus ; ■ conforme avec réserves : des dysfonctionnements mineurs ont été relevés ou des objectifs ne sont pas remplis au niveau de l'engagement de service attendu. Dans ce cas, le titulaire propose un plan de remédiation aux dysfonctionnements à court terme : le plan est soumis au CNRS dans les huit jours après communication de l'avis formel, et l'engagement de remédiation ne peut dépasser six mois. Le titulaire démontre à ses frais que les engagements sont tenus à l'issue du plan d'action ; ■ non conforme : tout ou partie des engagements ne sont pas tenus, ou des dysfonctionnements majeurs ont été constatés. Dans ce cas, le titulaire engage des actions selon les modalités décrites supra, sous astreinte journalière de remise en conformité. 	0

5.10.6 Application des plans gouvernementaux

Référence	Libellé exigence	Priorité
SECU_017	<p>Dans le cadre de l'application de plans gouvernementaux, les autorités françaises peuvent décider la mise en œuvre d'un ensemble de mesures spécifiques destinées à lutter contre des attaques notamment terroristes visant les systèmes d'information de l'État ou les systèmes d'information et réseaux de télécommunications. Il peut également s'agir de mesures d'entraînement à la réaction en cas d'incident.</p> <p>Dans le cadre du marché, le titulaire peut être concerné par ces alertes décidées au niveau gouvernemental, et s'engage à appliquer les consignes de sécurité données par le CNRS. Ces mesures sont susceptibles d'évoluer. Les modifications sont régulièrement transmises durant l'exécution du marché.</p> <p>Le titulaire est tenu de mettre immédiatement en œuvre lesdites dispositions, quand bien même elles auraient un impact significatif sur le coût de la prestation. Dans ce dernier cas, les conséquences financières de ces dispositions sont tirées soit par voie d'avenant, soit, en cas de désaccord persistant entre le CNRS et le titulaire, par les tribunaux compétents. Sans impact significatif sur les coûts, le respect de cette exigence est réputé réalisé pro bono.</p>	0

6 ANNEXES

6.1 DOCUMENTS JOINTS

Les documents suivants sont joints au présent CCTP. Ils sont applicables tout le long de l'accord cadre.

Le CNRS/Inserm pourra faire évoluer ces documents au cours de l'accord cadre en fonction des évolutions technologiques rendues nécessaires par l'état de l'art. Ces évolutions pourront faire l'objet de commandes au titulaire le cas échéant.

Nom	Description	Type ⁷
Annexe 1 : Tableau des exigences	Ce document présente : <ul style="list-style-type: none"> les exigences applicables dans le cadre des développements et de la maintenance de la solution (onglet « cadre de cohérence technique ») les exigences applicables à l'organisation des prestations (onglet « organisation des prestations ») 	[A]
Annexe 2 : CCT_Versions-cibles	Ce document présente à un instant t (ce document évolue régulièrement dans le temps et n'est donc pas figé en termes d'engagement) les versions cibles des composants applicatifs et les éléments de compatibilité navigateurs requis dans le cadre des développements et de la maintenance d'applications	[A]

6.2 REFERENCE DES EXIGENCES

Référence	Groupe d'exigence
AUTH	Authentification
BDD	Base de données
DEV	Développement
DOC	Stockage des documents
ECH	Echange de données
ENV	Environnements
ERG	Ergonomie, graphisme
HAB	Habilitations
INF	Infrastructure
QUA	Qualité
REGL	Conformité réglementaire
SECU	Mesure et clauses de sécurité
SSI	Sécurité des systèmes d'information
URB	Urbanisation

6.3 ABREVIATIONS ET GLOSSAIRE

6.3.1 Abréviations

Le tableau suivant présente la liste des abréviations utilisées dans ce document.

Sigle	Description
ANSSI	Agence Nationale de la Sécurité des Systèmes d'Information

⁷ [A] = document applicable

[R] = document de référence (cf. dans le glossaire au § 6.3.2)

Sigle	Description
AP	Assistant de Prévention
API	Application Programming Interface (interface de programmation applicative)
BDD	Base De Données
CAS	Central Authentication Service
CCAP	Cahier des Clauses Administratives Particulières
CCTP	Cahier des Clauses Techniques Particulières
CNIL	Commission nationale de l'informatique et des libertés
CNPS	Coordination Nationale de Prévention et de Sécurité
CNRS	Centre National de la Recherche Scientifique
CSS	Cascading Style Sheets
CSV	Comma-separated values
DCP	Donnée à caractère personnel
DEV	plate-forme de DEVeloppement
DGD-I	Direction Générale Déléguée à l'Innovation
DGD-R	Direction Générale Déléguée aux Ressources
DGD-S	Direction Générale Déléguée à la Science
DNS	Domain Name System (système de noms de domaine)
DR	Délégation Régionale
DSI	Direction des Systèmes d'Information
EAI/ESB	Enterprise Application Integration (intégration d'applications d'entreprise) / Enterprise Service Bus
ETPT	Equivalent Temps Plein Travaillé
GED	Gestion Electronique de Documents
GIP	Groupement d'Intérêt Public
HTML	HyperText Markup Language (langage de balisage d'hypertexte)
HTTP	HyperText Transfer Protocol (protocole de transfert hypertexte)
HTTPS	HyperText Transfer Protocol Secure (protocole de transfert hypertexte sécurisé)
IAM	Identity and Access Management : Gestion et gouvernance des identités et des accès
IdP	Identity Provider (fournisseur d'identité)
IHM	Interface Homme Machine
IPsec	Internet Protocol Security (protocole de sécurité internet)
IPv4	Internet Protocol version 4 (protocole internet version 4)
IRPS	Inspecteur Régional de Prévention et Sécurité
JMS	Java Message Service
JSON	JavaScript Object Notation (format de données textuelles dérivé de la notation des objets du langage JavaScript)
LAN	Local Architecture Network (réseau local)
LDAP	Lightweight Directory Access Protocol (protocole d'accès aux annuaires)
MESRI	Ministère de l'Enseignement Supérieur et de la Recherche et de l'Innovation
MCO	Maintien en Condition Opérationnelle
MDM	Master Data Management (gestion des données de référence)
MOA	Maîtrise d'ouvrage

Sigle	Description
MOE	Maîtrise d'œuvre
NAT	Network Address Translation (mécanisme de translation d'adresses)
NTP	Network Time Protocol (protocole d'heure réseau)
OS	Operating System
PGSI	Politique Générale de Sécurité de l'Information
PAQ	Plan Assurance Qualité
PAS	Plan Assurance Sécurité
PSSI	Politique de Sécurité des Systèmes d'Information
PSST	Pôle Santé et Sécurité au Travail
REC	plate-forme de RECette
RENATER	REseau NATIONAL de télécommunications pour la Technologie, l'Enseignement et la Recherche
REST	REpresentational State Transfer
RFC	Requests For Comments (demande de commentaires)
RGAA	Référentiel général d'Accessibilité pour les Administrations
RGI	Référentiel Général d'Interopérabilité
RGPD	Règlement Général sur la Protection des Données
RGS	Référentiel Général de Sécurité
RH	Ressources Humaines
RSSIC	Responsable de la Sécurité des Systèmes d'Information du CNRS
SAE	Service d'archivage électronique
SAML	Security Assertion Markup Language (langage de balisage d'informations d'authentification)
SGBD	Système de Gestion de Base de Données
SGCN	Secrétariat Général du Comité national
SI	Système d'Information
SMTP	Simple Mail Transfer Protocol (protocole simple de transfert de courrier)
SNMP	Simple Network Management Protocol (protocole simple de gestion de réseau)
SP	Service Provider (fournisseur de services)
SQL	Structured Query Language (langage de requête structurée)
SSH	Secure SHell
SSI	Sécurité des Systèmes d'Information
SSI	Service des Systèmes d'Information
SSL	Secure Socket Layer
SSO	Single Sign-On (authentification unique)
TLS	Transport Layer Security
VLAN	Virtual Local Area Network (réseau local virtuel)
VPN	Virtual Private Network (réseau privé virtuel)
W3C	World Wide Web Consortium
WCAG	Web Content Accessibility Guidelines (règles pour l'accessibilité des contenus Web)
XML	eXtensible Markup Language (langage de balisage extensible)
XSS	Cross Site Scripting

6.3.2 Glossaire

Le tableau suivant présente le glossaire des termes utilisés dans ce document.

Terme	Description
Document applicable	Document devant être obligatoirement appliqué par le Titulaire
Document de référence	Document pouvant être utilement consulté par le Titulaire
EAI/ESB	Plateforme d'intermédiation des flux de données
Flux	Tout échange de données ou d'information entre deux briques applicatives (y compris services d'intermédiation), quelle que soit la modalité et forme de cet échange. Un flux peut être entièrement manuel, ou peut faire appel à des services web, ou peut passer par l'EAI/ESB, ou
LDAP	Protocole permettant l'interrogation et la modification des services d'annuaire.
REST	Style d'architecture d'échange de données autour de services web basés sur le protocole HTTP
Shibboleth	Mécanisme de propagation d'identités, développé par le consortium Internet2 , qui regroupe 207 universités et centres de recherche. Pour toute information complémentaire se référer au site suivant : http://shibboleth.net/
Téléservice	Application destinée à la communication interadministration ou destinée à réaliser des téléprocédures ouvertes à des usagers, c'est-à-dire application grand public.