Cadre de diagnostic de l'aptitude à la recherche à double usage (DURA)

Cible : Centres de recherche affiliés à des établissements d'enseignement supérieur (EES) (universités, collèges et instituts autochtones)

Date: 31 mars 2026 | Version: 2.5

1. Sommaire

Les EES financés par les fonds publics de l'Ontario font face à des attentes accrues en matière de sécurité de la recherche et de collaboration responsable, particulièrement lorsque les projets présentent un potentiel à double usage. Le DURA fournit un diagnostic pratique de l'état de préparation et une feuille de route qui aident les installations à déterminer les pratiques de gouvernance, de gestion du personnel, de contrôle de l'infrastructure et de contrôle des résultats nécessaires pour participer en toute sécurité à des collaborations à double usage par l'entremise de la plateforme d'innovation collaborative de l'Ontario (PICO). Il produit un niveau de préparation et des mesures recommandées, et fait référence à des programmes et à des normes faisant autorité lorsque cela est pertinent; il ne certifie pas la conformité et ne remplace pas ces autorités.

Le DURA est un cadre de maturité à **sept niveaux** (niveaux **0, 1, 2, 3, 4, 5 et 6**) conçu pour évaluer et guider les établissements d'enseignement supérieur (EES) canadiens dans leur capacité à mener des recherches à double usage (RDU), en évaluant leur aptitude organisationnelle et leur maturité en matière de gouvernance (mesures de contrôle, conformité, gestion des risques). Il n'évalue **pas** l'équipement de laboratoire, la qualité des résultats de recherche ou les compétences du personnel. Les établissements peuvent utiliser le cadre DURA pour l'autoévaluation, la production de rapports de gouvernance internes ou la validation par un tiers.

La nature délicate de cette initiative est en grande partie attribuable à l'équilibre entre la science ouverte et la nécessité de prévenir le transfert malveillant de connaissances, ainsi qu'aux conflits potentiels d'ordre éthique, moral ou politique.

Note importante sur la portée :

Le DURA fournit uniquement un **niveau de préparation** et des **orientations de mise en œuvre.** Il ne s'agit **pas** d'un programme d'accréditation, de certification ou de vérification de la conformité. Lorsque le DURA fait référence à la « validation » ou aux « preuves », il s'agit d'une attestation de l'installation de l'EES (veuillez consulter la section 7.3). Le DURA et la PICO n'effectuent **pas** de vérifications techniques, de vérifications de sécurité, de vérifications par les services de renseignement ou d'assurance formelle de la conformité, et renvoient plutôt à des normes et à des programmes faisant autorité (p. ex. orientations du gouvernement du Canada, ISO, OTAN), qui demeurent sous la responsabilité et l'administration de leurs autorités respectives.

2. Contexte stratégique

2.1. Contexte de la recherche à double usage

La recherche à double usage (RDU) désigne les travaux scientifiques et technologiques destinés à des fins civiles ou commerciales légitimes, mais qui peuvent également avoir des applications potentielles dans les domaines de la sécurité nationale, de la défense ou d'autres secteurs sensibles. De nombreuses technologies émergentes, telles que l'intelligence artificielle, les capacités cybernétiques, les technologies quantiques, les matériaux avancés, les systèmes spatiaux et les plateformes autonomes, entrent dans cette catégorie.

Au Canada et dans les pays alliés, une attention croissante est accordée à la gouvernance de la recherche à double usage menée dans les environnements de recherche financés par les fonds publics. Les établissements d'enseignement supérieur (EES) et les établissements de recherche jouent un rôle central dans les premières étapes de l'innovation, mais leur culture de recherche traditionnellement ouverte peut créer des défis lorsque les projets touchent à des technologies contrôlées, à des données sensibles ou à des considérations de sécurité nationale.

Les initiatives fédérales telles que les orientations du gouvernement du Canada en matière de sécurité de la recherche, notamment la Recherche en technologies sensibles et affiliations préoccupantes (RTSAP), ainsi que les régimes connexes de contrôle des exportations et de marchandises contrôlées, soulignent l'importance de gérer ces risques tout en maintenant les avantages de la collaboration scientifique ouverte. Les établissements de recherche ont de plus en plus besoin de mécanismes de gouvernance leur permettant de déterminer, d'évaluer et de gérer les risques liés au double usage de manière structurée et proportionnée.

Le cadre DURA vise à répondre à ce besoin en fournissant un **modèle d'aptitude à la gouvernance** qui aide les installations de recherche à comprendre et à renforcer progressivement leurs mesures de contrôle et leurs processus internes liés à la collaboration à double usage. L'approche du Canada en matière de sécurité de la recherche s'harmonise avec les orientations des pays alliés sur le maintien d'une recherche sécurisée et ouverte, y compris les *Meilleures pratiques du G7 pour une recherche sécuritaire et ouverte*.

2.2. Collaboration recherche-industrie

La collaboration entre les établissements d'enseignement supérieur (EES), les partenaires de l'industrie et les organismes gouvernementaux est un élément central de l'écosystème d'innovation du Canada. Les centres de recherche au sein des EES contribuent fréquemment aux premières étapes du développement technologique, y compris la recherche appliquée, le prototypage et les activités de validation, qui peuvent ensuite passer au développement industriel et à la mise en marché.

Les programmes aux niveaux fédéral et provincial, y compris les initiatives d'innovation en matière de défense, les programmes de partenariat de recherche et les plateformes d'innovation collaborative, encouragent ces partenariats afin d'accélérer le développement de technologies avancées et de renforcer la capacité d'innovation du Canada.

Parallèlement, ces collaborations peuvent introduire des défis de gouvernance lorsque les projets impliquent des technologies sensibles, des partenaires étrangers, des renseignements contrôlés ou des exigences contractuelles en matière de sécurité. Les installations de recherche bénéficient donc de processus internes clairs pour gérer des questions telles que la sécurité de la recherche, les contrôles à l'exportation, la diligence raisonnable envers les partenaires, la gouvernance des données et la diffusion responsable des résultats de recherche.

Le cadre DURA fournit une méthode structurée pour aider les installations de recherche à évaluer leur état de préparation en matière de gouvernance pour ces types de collaborations et à déterminer les mesures pratiques qui favorisent une participation responsable aux écosystèmes d'innovation à double usage.

2.3. Stratégie industrielle de défense du Canada

La *Stratégie industrielle de défense (SID) du Canada : Sécurité, souveraineté et prospérité* met l'accent sur le renforcement de la base industrielle de défense du pays en soutenant le développement et la mise en marché de technologies avancées et à double usage grâce à la collaboration entre l'industrie, le gouvernement et les établissements de recherche.

Bon nombre des domaines technologiques mis en évidence dans la stratégie prennent naissance ou arrivent à maturité dans des environnements de recherche universitaires et financés par les fonds publics. À mesure que la collaboration entre ces installations et l'industrie liée à la défense s'élargit, les établissements ont besoin de structures de gouvernance capables de soutenir une recherche à double usage responsable tout en protégeant les intérêts en matière de sécurité nationale, la propriété intellectuelle et l'intégrité de la recherche.

La relation entre le cadre DURA et la Stratégie industrielle de défense est décrite plus en détail dans l'annexe intitulée « *Le cadre DURA dans le contexte de la Stratégie industrielle de défense (SID) du Canada* ». L'annexe explique comment le cadre DURA fonctionne au niveau institutionnel en fournissant un modèle de préparation à la gouvernance pour les installations de recherche participant à l'écosystème d'innovation en matière de défense au sens large.

La section suivante décrit la méthodologie utilisée pour appliquer le modèle DURA et évaluer la maturité de la gouvernance au sein des installations de recherche des EES.

3. Objet et portée du cadre DURA

3.1. Objectif

L'objet de la méthodologie DURA est de fournir une approche structurée pour évaluer l'aptitude en matière de gouvernance des installations de recherche des EES qui peuvent participer à des collaborations de recherche à double usage avec des partenaires de l'industrie ou du gouvernement.

La méthodologie soutient l'interprétation et l'application cohérentes du modèle DURA en définissant la portée de l'évaluation, le modèle de preuves utilisé pour étayer les déclarations d'aptitude et le processus par lequel les installations progressent à travers les niveaux de préparation.

L'évaluation DURA porte exclusivement sur l'aptitude en matière de gouvernance. Elle n'évalue **pas** le rendement de l'infrastructure de laboratoire, la qualité des résultats scientifiques ou les compétences des chercheurs individuels. Le cadre vise à aider les installations de recherche à comprendre et à renforcer progressivement leurs mécanismes de gouvernance interne liés à la sécurité de la recherche, à la gestion des risques de collaboration et au traitement responsable des technologies et des renseignements sensibles.

3.2. Portée et applicabilité

Cette section définit la portée institutionnelle et opérationnelle de la méthodologie DURA. Elle précise quels types d'installations de recherche le cadre vise à évaluer et établit les conditions d'applicabilité selon lesquelles des exigences de préparation particulières deviennent pertinentes.

La mise en œuvre initiale du cadre DURA se concentre sur les installations de recherche participant à la plateforme d'innovation collaborative de l'Ontario (PICO) exploitée par eCampusOntario. Bien que la mise en œuvre actuelle soit limitée aux établissements de l'Ontario, le cadre DURA et la

plateforme PICO sont conçus pour être applicables à l'échelle du Canada, étant donné que la sécurité de la recherche, les contrôles à l'exportation et les politiques de collaboration en matière de défense relèvent principalement du gouvernement fédéral.

3.2.1. Profil de portée (déclencheurs d'applicabilité)

Pour éviter un fardeau de conformité inutile et assurer des contrôles proportionnels, le DURA utilise un mécanisme de **profil de portée**. Le profil de portée définit l'environnement de risque des collaborations prévues et détermine quelles exigences en matière de préparation sont applicables.

Note sur la posture institutionnelle : Les installations intégrées à des universités militaires ou à des académies de défense, ou officiellement affiliées à celles-ci (p. ex. les établissements relevant d'une autorité de défense), devraient consigner cette posture dans le profil de portée, car elle peut avoir une incidence sur les clauses de sécurité applicables, les attentes en matière de surveillance et les exigences des partenaires, même lorsque l'activité de recherche demeure dirigée par des civils.

Avant d'attribuer un niveau DURA, l'installation devrait définir un profil de portée pour la ou les collaborations prévues. Le profil de portée est un document évolutif. Les installations devraient maintenir un **profil de portée de référence** représentant leur posture de collaboration habituelle, et documenter les **écarts** propres aux projets lorsqu'une collaboration proposée introduit une sensibilité plus élevée, des partenaires différents, une technologie réglementée ou contrôlée, ou des besoins en matière d'environnement séparé.

Le profil de portée détermine quelles exigences de préparation conditionnelles sont **applicables** ou **non**, ce qui évite d'imposer des mesures de contrôle excessives aux projets à faible risque. Le profil de portée devrait consigner ce qui suit, au minimum :

- **Pertinence pour la RTSAP :** si les travaux portent sur des **domaines de recherche en technologies sensibles** et déclenchent donc des mesures de sécurité de la recherche renforcées.
- **Sécurité de la recherche (SR) dans le cadre du financement de la recherche de l'Ontario** (par projet) : si les collaborations sont susceptibles d'être soumises dans le cadre de programmes de financement de la recherche du ministère de l'Ontario qui appliquent le processus de sécurité de la recherche de l'Ontario (p. ex. attestations de chercheurs désignés, liste de vérification des risques, plan d'atténuation). Si déclenché, inclure les artéfacts de SR de l'Ontario du projet et identifier le responsable interne de l'installation chargé de leur administration.
- **Marchandises contrôlées/contrôles à l'exportation :** si les travaux impliquent des **marchandises contrôlées, des technologies contrôlées ou des articles ou des données soumis à des contrôles à l'exportation,** ce qui peut déclencher des programmes fédéraux particuliers et des exigences contractuelles.
- **Classification de la sensibilité des données :** la classe de sensibilité la plus élevée des données attendues (p. ex. publiques, protégées, contrôlées, réglementées, soumises à des contrôles à l'exportation).
- **Déclencheur lié aux données autochtones et aux partenariats :** si le projet implique des partenaires ou des communautés autochtones, de la recherche dirigée par des Autochtones, des données pouvant être identifiées comme autochtones, ou de la recherche menée sur des terres ou dans des contextes autochtones. Si déclenché, le dossier de preuves doit inclure des artéfacts de gouvernance des données autochtones propres au projet (p. ex. plan de gestion conforme aux principes de propriété, de contrôle, d'accès et de possession [PCAP®]), s'il y a lieu, des protocoles propres à la communauté,

des approbations et des dossiers de décision, et des conditions de partage, d'accès et de conservation des données). Les exigences en matière de gouvernance des données autochtones sont propres à chaque communauté et doivent être confirmées projet par projet.

- **Profil du partenaire :** PME nationale, maître d'œuvre de programmes de défense, ministère ou organisme gouvernemental, centre de recherche affilié au gouvernement ou rattaché au ministère de la Défense, ou partenaire étranger (et si le partenaire impose des clauses de sécurité particulières).
- **Posture de l'installation :** si les travaux nécessitent des **environnements séparés** (physiques ou numériques) au-delà des contrôles standards du campus.
- **Modèle de mobilisation :** projet concurrentiel unique, collaboration commanditée par l'industrie, réseau multi-institutionnel, ou centre financé par la défense ou structure de recherche affiliée à la défense (selon le cas).

Lorsqu'une exigence n'est pas applicable selon le profil de portée, l'installation doit fournir une brève **justification de non-applicabilité** dans le cadre du dossier de preuves pour la revendication du niveau du DURA.

3.3. Principes d'évaluation

La méthodologie DURA est conçue pour s'harmoniser avec les principes canadiens de protection de la recherche couramment utilisés par les universités à forte intensité de recherche du U15 (p. ex. la transparence, la prévisibilité, l'engagement et l'inclusivité, ainsi que la responsabilité partagée), tout en demeurant proportionnelle au profil de portée de l'installation.

Le cadre DURA est guidé par les principes suivants pour assurer une application cohérente et proportionnée dans les installations de recherche participantes :

- **Proportionnalité :** les exigences sont appliquées en fonction du profil de portée de l'installation et du contexte de risque associé.
- **Évaluation fondée sur des preuves :** l'avancement nécessite des preuves documentaires ou procédurales démontrant que les mécanismes de gouvernance sont mis en œuvre.
- **Seuils d'étape clairs :** chaque niveau de préparation contient des capacités obligatoires qui doivent être satisfaites avant la progression.
- **Accent sur la gouvernance :** l'évaluation porte sur l'état de préparation en matière de gouvernance, et non sur la qualité de la recherche, les capacités techniques ou la compétence du personnel.
- **Amélioration continue :** les niveaux de préparation supérieurs exigent une surveillance et un examen périodique pour maintenir les pratiques de gouvernance.
- **Équité et non-profilage :** la mise en œuvre du DURA et les communications sur la sécurité de la recherche doivent être appliquées de manière antiraciste et inclusive, en évitant les préjugés et le profilage tout en gérant les risques légitimes liés à la sécurité de la recherche.

3.4. Rôles clés dans le processus DURA

Le processus DURA est conçu pour être appliqué de manière simple et reproductible au sein des EES. Pour ce faire, il s'appuie sur trois rôles complémentaires : un responsable institutionnel, une fonction institutionnelle de sécurité de la recherche (lorsqu'elle existe) et un responsable au niveau de l'installation chargé de l'exécution quotidienne. Les titres varient d'un EES à l'autre; les responsabilités ci-dessous définissent les rôles aux fins du DURA.

- **Responsable institutionnel** (p. ex. VP/VPA Recherche ou l'équivalent). Le responsable institutionnel est le dirigeant de l'établissement responsable de la gouvernance de l'aptitude à la recherche à double usage. Il possède le pouvoir décisionnel, résout les recours hiérarchiques et veille à ce que le responsable au niveau de l'installation puisse mobiliser les fonctions institutionnelles (p. ex. le bureau de la recherche, les services juridiques, les TI, la gestion des risques, la mobilisation autochtone) lorsque le profil de portée d'un projet l'exige. Le responsable institutionnel approuve l'établissement de pratiques de préparation au double usage au niveau institutionnel, soutient les attentes en matière de ressources et constitue le point de responsabilité principal lorsqu'une collaboration proposée introduit un risque élevé.
- **Agent de sécurité de la recherche (ASR)**/ Bureau de la sécurité de la recherche (fonction institutionnelle). L'ASR est la fonction institutionnelle qui soutient des pratiques cohérentes en matière de sécurité de la recherche dans l'ensemble de l'EES. Lorsqu'il est présent, l'ASR fournit des orientations sur la politique de sécurité de la recherche, les pratiques de diligence raisonnable envers les partenaires, les voies de signalement et de recours hiérarchique en cas d'incident, et l'harmonisation avec les orientations fédérales applicables (p. ex. attentes liées à la RTSAP, s'il y a lieu) et les exigences en matière de gouvernance institutionnelle. Il peut conseiller les installations sur les mesures de contrôle appropriées en fonction du profil de portée, coordonner la formation et la sensibilisation, et servir de point de liaison avec les unités institutionnelles responsables de la cybersécurité, des services juridiques et contractuels, de la protection de la vie privée et de l'éthique. L'ASR ne certifie pas l'aptitude de l'installation; il soutient la gouvernance et la cohérence.
- **Responsable de la sécurité du centre de recherche (RSCR)**. Le RSCR est le responsable désigné de l'installation chargé de coordonner les activités DURA au sein d'un laboratoire, d'un établissement, d'un centre ou d'une installation. Il maintient le profil de portée de référence de l'installation, coordonne l'achèvement des listes de vérification du DURA pour les mises à niveau et veille à ce que les artéfacts internes requis existent et soient à jour (p. ex., politiques, plans, dossiers de formation, approbations de gouvernance). Il coordonne également les intervenants au niveau de l'installation (chercheurs principaux, gestion du laboratoire, soutien informatique, gestionnaires de données) et transmet les enjeux à l'ASR et au responsable institutionnel lorsqu'un projet nécessite des décisions ou des ressources institutionnelles supplémentaires. Dans le contexte du DURA, « RSCR » est une définition de rôle; la personne peut détenir un autre titre officiel à l'EES (p. ex., gestionnaire de laboratoire, directeur des opérations, administrateur de centre).

Note sur la PICO : Les niveaux DURA consignés dans la PICO sont auto-attestés par les installations. La PICO consigne les sélections de la liste de vérification et les changements de niveau (identifiant d'utilisateur et horodatage) et envoie des notifications au gestionnaire de la PICO, à l'ASR de l'EES et au RSCR de l'installation. La PICO ne valide pas, ne certifie pas, n'examine pas et ne vérifie pas les déclarations des installations.

3.5. Processus d'évaluation

La méthode d'évaluation est intentionnellement simple et évite la notation ou la pondération; elle se concentre sur les preuves documentaires requises à chaque niveau.

Les artéfacts de preuves sont vérifiés à l'interne par le responsable de la sécurité du centre de recherche de l'installation (le RSCR ou son délégué) pour confirmer leur présence, leur exhaustivité, leur actualité et leur cohérence interne.

Note propre aux projets (SR de l'Ontario) : Les exigences en matière de sécurité de la recherche du ministère de l'Ontario sont évaluées projet par projet dans le cadre d'un processus de financement. Dans le DURA, ces exigences sont traitées comme un déclencheur du profil de portée : les installations ne sont pas tenues de conserver les formulaires de SR de l'Ontario comme artéfacts permanents de laboratoire, sauf si elles anticipent un financement du ministère de l'Ontario, auquel cas l'installation devrait démontrer l'existence d'un processus interne pour recueillir, conserver et transmettre les attestations et les artéfacts d'atténuation requis au niveau du projet.

Pour soutenir l'effort d'évaluation au fil du temps pour les installations aux niveaux 5 et 6, le RSCR est responsable de coordonner des bilans périodiques avec les intervenants concernés (p. ex. la direction, les TI, le bureau de la recherche, la gestion du laboratoire) et d'assurer le suivi de l'achèvement des artéfacts requis.

Règle en matière de changement de portée : Lorsque le profil de portée change de façon à rendre des exigences supplémentaires applicables, le RSCR de l'installation doit revérifier les seuils de niveau touchés par les exigences nouvellement applicables avant de revendiquer ou de maintenir le niveau supérieur pour cette collaboration, et consigner la date d'entrée en vigueur et la version du profil de portée mis à jour.

3.6. Guide de traitement des preuves (interne à l'installation)

Cette section décrit le traitement interne des preuves par l'installation; la PICO ne valide pas et n'examine pas les preuves.

Le responsable de la sécurité du centre de recherche (RSCR) désigné déterminera si, avec la liste de vérification des capacités obligatoires comme guide, le seuil d'un niveau a été franchi pour passer au niveau suivant, en s'assurant que tous les services du centre de recherche ont effectué leur propre autoévaluation.

- **Niveaux 2-3 :** auto-attestation appuyée par le téléversement de preuves de base (artéfacts minimaux viables).
- **Niveau 4 :** examen interne structuré (RSCR plus fonctions institutionnelles pertinentes, comme les TI et le bureau de la recherche) appuyé par un registre de preuves et des notes d'examen documentées.
- **Niveaux 5-6 :** la validation indépendante par un tiers est **facultative et dépend de la portée** (encouragée lorsque requise par les contrats des partenaires, les données ou technologies réglementées, ou les profils de portée à risque plus élevé). La validation indépendante peut comprendre des fonctions de vérification institutionnelle, des experts-conseils externes ou des programmes de certification requis par les contrats des partenaires.

Pour éviter toute partialité liée à l'« auto-notation » dans le processus d'autoévaluation, le responsable de la sécurité du centre de recherche (RSCR) désigné devrait être une personne ayant une connaissance et une expérience des exigences du centre de recherche.

3.7. Terminologie et définitions

Un langage commun est nécessaire pour assurer une compréhension commune par les centres de recherche, l'industrie et l'établissement de défense. À cette fin, nous avons compilé un glossaire des termes, qui est joint au présent document et qui est également intégré à la page d'accueil sur le double usage d'eCampusOntario (https://aka.pe/eCO/dur/ [en anglais seulement]).

4. Modèle de préparation du DURA

4.1. Aperçu de l'échelle de préparation

L'échelle de préparation du DURA comprend sept niveaux **(niveaux 0 à 6)** qui représentent une maturité croissante en matière de gouvernance.

L'échelle trace la progression de la sensibilisation initiale au double usage jusqu'à la mise en œuvre complète des exigences fédérales et du contexte stratégique canadien ainsi que des pratiques de gouvernance institutionnelle applicables. Elle couvre quatre **piliers fonctionnels** clés : la gouvernance, le personnel, l'infrastructure et le contrôle des résultats. Ces piliers sont décrits en détail aux sections 4.4 et 5 ci-dessous.

Le modèle met également l'accent sur la nécessité d'une **surveillance et d'une amélioration continues** comme meilleures pratiques opérationnelles. Aux niveaux de préparation supérieurs, ces mécanismes devraient être **institutionnalisés** (c.-à-d. intégrés aux activités courantes, examinés périodiquement et améliorés en fonction des leçons apprises) pour maintenir la gouvernance de la sécurité de la recherche au fil du temps.

L'échelle de préparation est résumée à la section 4.2; les règles d'interprétation et les références canoniques sont fournies à la section 4.3.

4.2. Tableau de l'échelle de préparation

Niveau	État	Objectif
0	**Retrait**	Décision explicite d'exclure la RDU du mandat de l'installation.
1	**Neutre**	Aucun intérêt actuel ni considération formelle de la RDU.
2	**Intérêt**	Repérage du potentiel à double usage dans la recherche existante.
3	**Élaboration**	Élaboration de politiques et d'infrastructures de sécurité internes.
4	**Validation**	Préparation appuyée par des preuves : les contrôles et la gouvernance sont documentés et peuvent être examinés pour en vérifier l'exhaustivité et la cohérence.
5	**Prêt**	La gouvernance et les contrôles de sécurité sont actifs et suffisants pour l'exécution conforme des ententes de partenariat qui imposent des exigences élevées en matière de sécurité, de données ou de souveraineté (selon le profil de portée).
6	**Engagé**	Système de gouvernance institutionnalisé et démontré par l'exécution soutenue et conforme de multiples collaborations à double usage, avec une amélioration continue mesurable.

4.3. Définitions des niveaux

L'échelle de maturité du DURA se divise en sept états (niveaux 0, 1, 2, 3, 4, 5 et 6). Les objectifs des niveaux et les attentes en matière de préparation sont résumés dans le tableau de l'échelle de préparation ci-dessus (section 4.2).

Les définitions canoniques des niveaux (état, objectif, actions et références faisant autorité) sont maintenues dans le document complémentaire, *Cadre de l'échelle de maturité* DURA.

Le présent document de méthodologie définit comment les niveaux sont appliqués :

- **Profil de portée en premier :** Avant de revendiquer un niveau DURA, l'installation définit un profil de portée, comme décrit à la section 3.2.1. Le profil de portée détermine quelles exigences sont applicables par rapport à celles qui ne le sont pas.
- **Responsable de la gouvernance :** Aux niveaux 3 et supérieurs, les installations doivent nommer un responsable institutionnel désigné (p. ex. VP/VPA Recherche ou l'équivalent) pour conférer une autorité en matière de recours hiérarchique et veiller à ce que le RSCR puisse mobiliser les fonctions institutionnelles (TI, services juridiques, bureau de la recherche) lorsque les profils de portée déclenchent des exigences élevées.
- **Obligatoire, conditionnel et souhaitable :** Les éléments « obligatoires » définissent le seuil à atteindre pour revendiquer un niveau; les éléments « conditionnels » dépendent du profil de portée applicable; les éléments « souhaitables » reflètent une maturité supérieure au sein d'un niveau, sans pour autant hausser ce dernier.
- **Pas de crédit partiel pour les seuils :** L'avancement exige l'achèvement à 100 % des éléments obligatoires applicables au profil de portée. Si un élément n'est pas applicable, l'installation doit fournir une brève justification de non-applicabilité dans le cadre du dossier de preuves.
- **Modèle de preuves :** La « validation » désigne un examen administratif de la présence, de l'exhaustivité, de l'actualité et de la cohérence interne des preuves, et non une certification ou une assurance de conformité technique.

Pour l'interprétation opérationnelle par domaine de capacité (gouvernance, personnel, infrastructure, contrôle des résultats), consultez la section sur les piliers d'évaluation fonctionnelle qui suit.

4.4. Piliers d'évaluation fonctionnelle

Le cadre DURA évalue l'état de préparation en matière de gouvernance selon quatre piliers d'évaluation fonctionnelle. Ces piliers représentent les principaux domaines de capacité institutionnelle requis pour gérer les risques liés à la recherche à double usage de manière structurée et durable.

- **Gouvernance :** Politiques institutionnelles, structures de surveillance et processus décisionnels qui définissent comment les risques liés à la recherche à double usage sont déterminés, gérés et surveillés.
- **Personnel :** Pratiques de ressources humaines liées à la sensibilisation, à la formation, au contrôle de l'accès et aux responsabilités fondées sur les rôles pour les personnes participant aux activités de recherche à double usage.
- **Infrastructure :** Environnements physiques et numériques utilisés pour stocker, traiter et transmettre les données et les technologies de recherche, y compris la cybersécurité et les mesures de protection au niveau de l'installation adaptées au profil de portée.
- **Contrôle des résultats :** Mécanismes régissant la diffusion, le transfert et la protection des résultats de recherche, y compris les publications, la propriété intellectuelle, les ensembles de données et les artéfacts de collaboration.

5. Interprétation illustrative des piliers fonctionnels

Le tableau suivant fournit une interprétation de haut niveau de la façon dont les piliers d'évaluation fonctionnelle évoluent généralement à travers les niveaux de préparation DURA **au-dessus du niveau 1 (Neutre)**. Les définitions faisant autorité des exigences, des actions et des références des niveaux sont maintenues dans le document complémentaire *Échelle de maturité DURA (Cadre)*.

Capacité fonctionnelle	Niveau 2 : Intérêt	Niveau 3 : Élaboration	Niveau 4 : Validation	Niveau 5 : Prêt	Niveau 6 : Engagé
Gouvernance	Repérage formel du potentiel à double usage dans la recherche existante.	Nomination d'un responsable de la sécurité du centre de recherche (RSCR) et d'un responsable institutionnel désigné (p. ex., VP/VPA Recherche ou l'équivalent) pour fournir le pouvoir décisionnel et le soutien au recours hiérarchique pour la gouvernance de l'aptitude à la recherche à double usage.	Si applicable (marchandises ou technologies contrôlées impliquées) : Inscription au Programme des marchandises contrôlées (PMC) amorcée ou achevée ou justification documentée de non-applicabilité selon le profil de portée; dossier de preuves de gouvernance examiné pour son exhaustivité et sa cohérence interne (pas de certification).	L'autorité contractuelle institutionnelle et le processus permettant de conclure des ententes assorties des clauses requises en matière de sécurité de la recherche et de gestion des données sont actifs (selon le profil de portée et les exigences des partenaires).	Boucle établie de surveillance continue et d'amélioration continue pour les risques de sécurité et les contrôles de gouvernance.
Personnel	Sensibilisation de base aux enjeux en matière de sensibilité de la recherche parmi les chercheurs principaux.	Déterminer la pertinence pour la RTSAP et recenser les activités visées par la portée (lorsque applicable selon le profil de portée); définir les exigences de formation et d'intégration fondées sur les rôles pour le personnel soutenant les projets à double usage.	Pour les travaux visés par la RTSAP : attestations requises achevées et processus documenté d'examen, de recours hiérarchique et de conservation des dossiers pour les risques d'affiliations préoccupantes (le DURA et la PICO n'effectuent pas de vérification de sécurité par les services de renseignement).	Accès restreint par des zones réservées aux personnes qui ont besoin de savoir et des contrôles d'accès appropriés au profil de portée (physiques ou numériques).	Capacité soutenue et mesurable : cycles de mise à jour de la formation, contrôles de dotation et leçons apprises intégrées à la pratique; • profil avancé facultatif ou dépendant de la portée : participation aux écosystèmes adjacents à l'OTAN ou au DIANA lorsque pertinent.

Capacité fonctionnelle	Niveau 2 : Intérêt	Niveau 3 : Élaboration	Niveau 4 : Validation	Niveau 5 : Prêt	Niveau 6 : Engagé
Infrastructure	Utilisation du Wi-Fi standard du campus et de l'espace serveur partagé.	Renforcement initial de la cybersécurité au-delà du Wi-Fi standard (p. ex. isolation du réseau local virtuel). L'installation maintient également une cartographie à jour des actifs relatifs à l'infrastructure scientifique pertinente et des environnements habilitants (le cas échéant) pour appuyer les conversations avec les partenaires et les décisions relatives au profil de portée.	Gestion documentée des risques de cybersécurité conforme à l'ITSG-33 (évaluation des menaces et des risques, sélection des contrôles, plan de correction/plan d'action et jalons), ou preuve de progression sur une voie de certification acceptée (p. ex. Programme canadien de certification en cybersécurité [PCCC]) lorsque applicable selon le profil de portée.	Environnement de traitement de données sécurisé et séparé conforme au profil de portée documenté et à la posture de risque.	Gouvernance de l'infrastructure institutionnalisée et démontrable au fil du temps (surveillance, examens et vérifications selon le cas, amélioration continue), soutenant les exigences élevées des partenaires et en matière de traitement des données selon le profil de portée.
Contrôle des résultats	Examen informel des publications pour détecter une utilisation abusive potentielle de la recherche à double usage.	Rédaction d'un plan de contrôle technologique (PCT) pour régir les données et la propriété intellectuelle.	Achèvement des modules « Science en sécurité » (ou l'équivalent) pour les risques en matière de diffusion et de collaboration, en harmonie avec le profil de portée.	Capacité de traiter et de protéger les données et les résultats protégés, contrôlés, réglementés ou soumis à des contrôles à l'exportation, selon le cas. Traitement classifié ou OTAN uniquement lorsque les exigences du partenaire et le profil de portée l'exigent explicitement.	Le laboratoire joue le rôle de pôle régional ou de mentor pour les laboratoires de niveau inférieur (renforcement des capacités, modèles, accompagnement) et démontre une amélioration continue des contrôles des résultats.

6. Critères détaillés de préparation

6.1. Capacités obligatoires

Pour chaque niveau, les éléments **obligatoires** définissent le « seuil » pour accéder au niveau.

Ces capacités prennent la forme de documents remplis, de formulaires, de dossiers, d'attestations et d'autres artéfacts de preuves qui sont examinés par le **responsable de la sécurité du centre de recherche** (RSCR) (ou son délégué) pour leur présence, leur exhaustivité, leur actualité et leur cohérence interne.

6.2. Capacités souhaitables

Les éléments **souhaitables**, précédés de la lettre « o », représentent une « distinction » ou une maturité plus élevée au sein de ce niveau.

Les capacités souhaitables sont incluses pour encourager la participation précoce et l'amélioration continue sans créer un obstacle excessif à l'entrée. Au fil du temps, certaines pratiques actuellement considérées comme « souhaitables » peuvent devenir des attentes standards en raison de changements dans les exigences des partenaires, les politiques institutionnelles ou la législation. Lorsque de tels changements surviennent, les installations seront avisées et le cadre sera mis à jour en conséquence.

6.3. Liste des références

La liste canonique des programmes externes, des normes, des documents d'orientation et des liens référencés par le DURA est maintenue dans l'artéfact « Glossaire et liens » et est également disponible sur la page de renvoi du DURA à l'adresse https://aka.pe/eCO/dur/ (en anglais seulement).

7. Considérations clés

7.1. Protocoles de données institutionnels et souveraineté des données autochtones

L'un des mandats clés du DURA est de considérer, tôt dans l'évaluation de la sécurité de la recherche, les principes de propriété, de contrôle, d'accès et de possession (PCAP®) et les autres exigences applicables en matière de gouvernance des données autochtones en relation avec les pratiques de gouvernance et de traitement des données institutionnelles de l'installation (collecte, stockage, accès, partage, conservation et élimination). Les principes PCAP® sont conçus pour protéger la souveraineté des données autochtones en assurant les droits des communautés à l'autodétermination sur leurs données et en établissant des attentes de gouvernance sur la façon dont les données sont gérées et partagées. La souveraineté des données autochtones (p. ex. les principes PCAP®) n'est pas un élément « souhaitable »; elle doit être intégrée aux piliers de gouvernance et de contrôle des résultats lorsque déclenchée par le profil de portée (p. ex. participation de partenaires ou de communautés autochtones, données autochtones ou contextes de recherche dirigée par des Autochtones).

Lorsqu'applicable, la validation du niveau 4 comprend la confirmation que l'installation a documenté son harmonisation avec les cadres de gouvernance autochtones applicables (p. ex., PCAP®, le cas échéant), attestée par les approbations de gouvernance appropriées et les artéfacts propres au projet, comme un plan de gouvernance ou de gestion des données, des ententes de partage de données ou de recherche (le cas échéant), des contrôles d'accès définis et des attentes documentées en matière de conservation et d'élimination. Cet examen évalue la présence, l'exhaustivité, l'actualité et la cohérence interne des preuves, et ne constitue pas une certification ou une assurance de la conformité par eCampusOntario ou la PICO.

Remarque : Les communautés des Premières Nations, inuites et métisses peuvent avoir des protocoles de gouvernance des données distincts; la mobilisation et les exigences doivent être confirmées communauté par communauté.

7.2. La « falaise » au niveau 4

Puisque le niveau 4 introduit des contrôles assujettis à des preuves, les installations devraient déjà avoir un responsable institutionnel en place à partir du niveau 3 (élaboration). La transition du niveau 3 au niveau 4 doit être appuyée par le responsable institutionnel (p. ex. VP/VPA Recherche ou l'équivalent), qui fournit une charte écrite pour le RSCR (portée, droits décisionnels, voie de recours hiérarchique et attentes en matière de ressources), ainsi que par les bureaux de sécurité de la recherche (BSR) institutionnels, non seulement pour signaler et gérer les atteintes à la sécurité, mais aussi pour prévenir la « fatigue de la conformité » au fil du temps. Leur rôle est également celui d'« agents du changement » officieux pour soutenir continuellement les efforts des installations en vue de l'acquisition du niveau de maturité en matière de sécurité de la RDU et le maintien du statut de maturité et des meilleures pratiques (et plus tard des protocoles).

7.3. Auto-attestation dans la PICO (sans examen ni vérification)

Auto-attestation uniquement. Les exigences et les niveaux du DURA consignés dans la PICO sont auto-déclarés par l'installation. eCampusOntario et la PICO ne valident pas, ne certifient pas, n'examinent pas, ne vérifient pas et ne révisent pas les sélections, les preuves, les contrôles, les politiques ou les pratiques d'une installation.

Flux de travail de la mise à niveau (comportement de la PICO). Pour demander une mise à niveau du niveau DURA, le RSCR de l'installation doit se connecter à la PICO et cocher toutes les exigences obligatoires applicables (et toutes les exigences facultatives) pour le niveau cible. Chaque case cochée est enregistrée avec l'identifiant d'utilisateur et l'horodatage, ainsi qu'un document de preuve facultatif. Lors de la soumission, la PICO met à jour le niveau DURA de l'installation comme valeur auto-attestée, consigne le changement et envoie une notification automatique par courriel au gestionnaire de la PICO, au gestionnaire de l'installation de l'EES, à l'ASR de l'EES et au responsable institutionnel de l'EES. Aucun examen, approbation ou vérification des preuves par la PICO n'est effectué dans le cadre de la mise à niveau.

Surveillance du programme uniquement. Les notifications de la PICO soutiennent la surveillance du programme et la sensibilisation; elles ne constituent pas une validation du niveau de préparation auto-attesté par l'installation.

7.4. Harmonisation avec les alliés

Pour les profils de portée impliquant des partenaires de défense alliés ou des exigences liées à l'OTAN, les attentes du niveau 5 devraient faire référence aux exigences alliées applicables lorsque le contrat ou le partenaire l'exige explicitement.

8. Gouvernance post-évaluation

8.1. Analyse des écarts et feuille de route de correction

L'analyse des écarts et la feuille de route de correction aident les installations à prioriser les mesures nécessaires pour atteindre leur niveau cible et le maintenir au fil du temps.

8.2. Cycle de surveillance continue et de réévaluation

Passer du niveau 5 au niveau 6 exige généralement d'institutionnaliser la surveillance et l'amélioration continue plutôt que d'ajouter un seul nouveau contrôle. Les installations devraient mettre en œuvre des examens de routine, actualiser la formation et suivre les mesures de correction afin que les pratiques de gouvernance fassent partie des activités normales plutôt que d'exercices de conformité périodiques.

Les activités de **surveillance et de réévaluation** continues seront répétées sur une base annuelle. Pour s'assurer que les centres de recherche maintiennent leurs efforts de surveillance et d'évaluation, le processus d'autoévaluation sera répété tous les douze mois, avec des preuves actualisées selon les exigences en matière d'actualité applicables.