Échelle de maturité DURA – Cadre de travail

Objectif et limites.

L'échelle de maturité DURA fournit un **niveau de préparation** et des **conseils de mise en œuvre** pour les installations susceptibles de soutenir la recherche à double usage (RDU). Il ne s'agit **pas** d'un programme d'accréditation, de certification ou de vérification de la conformité.

Profil de portée en premier.

Avant d'attribuer un niveau DURA, une installation devrait définir un profil de portée (p. ex. pertinence pour la recherche en technologies sensibles et sur les affiliations préoccupantes [RTSAP], marchandises contrôlées/contrôles à l'exportation, sensibilité des données, type de partenaire). Le profil de portée détermine quelles exigences sont **applicables** ou **non** à chaque niveau, et évite d'imposer des mesures de contrôle excessives aux projets à faible risque.

Les installations peuvent maintenir un **profil de portée** de référence pour leurs activités courantes et documenter des profils de portée propres aux projets lorsque le contexte de risque d'une collaboration diffère; les déclarations de niveau DURA doivent faire référence au profil de portée utilisé pour cette déclaration.

Modèle d'examen des preuves.

Les références dans cette échelle à « validation », « vérification » ou « assurance » désignent **la présence, l'exhaustivité, l'actualité et la cohérence interne des preuves**, et non une certification technique. Lorsque des programmes ou des normes externes sont cités, ils demeurent la propriété des organismes qui font autorité en la matière et sont administrés par ces derniers. Les exigences et niveaux DURA sont autodéclarés par les installations; la PICO/ eCampusOntario ne valident pas, ne certifient pas, n'examinent pas, ne vérifient pas et n'évaluent pas les sélections.

Niveau	État	Objectif	Actions pour atteindre/maintenir l'aptitude Les éléments sans le préfixe « o » sont obligatoires pour le seuil du niveau (sous réserve de la justification « non applicable » du profil de portée).	Sources de référence [1] (non exhaustif) (o = facultatif/en fonction de la portée)
0	**Retrait**	Décision explicite d'exclure la RDU du mandat du laboratoire.	Aucune évaluation DURA n'est effectuée à ce niveau.	S. O.
1	**Neutre**	Aucun intérêt actuel ni considération formelle de la RDU.	Aucune évaluation DURA n'est effectuée à ce niveau.	S. O.

Niveau	État	Objectif	Actions pour atteindre/maintenir l'aptitude Les éléments sans le préfixe « o » sont obligatoires pour le seuil du niveau (sous réserve de la justification « non applicable » du profil de portée).	Sources de référence [1] (non exhaustif) (o = facultatif/en fonction de la portée)
2	**Intérêt**	Repérage du potentiel à double usage dans la recherche existante.	☐ Reconnaissance formelle de la valeur de l'aptitude à la recherche à double usage pour le mandat de l'installation. ☐ Responsable désigné pour l'initiative d'aptitude à la recherche à double usage (peut être intérimaire). ☐ Note de risque de base (une page) recensant les domaines de risque probables et les responsables. ☐ Profil de portée préliminaire effectué pour déterminer si les projets actuels ou prévus sont susceptibles de déclencher des contrôles de sécurité de la recherche, des contrôles à l'exportation, des considérations relatives aux marchandises/technologies contrôlées ou des clauses de sécurité imposées par les partenaires. ☐ Sondage DURA de la PICO (autoévaluation) rempli, ou plan documenté pour le remplir dans un délai défini. ○ Examiner les Meilleures pratiques du G7 pour une recherche sécuritaire et ouverte. ○ Communication de sensibilisation au personnel concerné (qui sera touché et pourquoi). ○ Préparation à la sécurité de la recherche en Ontario (le cas échéant) : si le profil de portée indique un financement probable de la recherche par le ministère de l'Ontario, identifier le responsable interne et mettre en place un processus allégé pour (i) recueillir les attestations des chercheurs désignés et (ii) soutenir la réalisation de la liste de vérification en matière de sécurité de la recherche en Ontario/des documents d'atténuation des risques pour le projet. ○ Ébauche de processus initiale décrivant comment les décisions relatives à l'examen des collaborations et au traitement des données seront prises au niveau 3.	○ Orientations d'introduction en matière de sécurité de la recherche (institutionnelles/des trois organismes/ fédérales, selon le cas) ○ Références de sensibilisation aux contrôles à l'exportation/ marchandises contrôlées (seulement si indiqué par le profil de portée) ○ Meilleures pratiques du G7 pour une recherche sécuritaire et ouverte

Niveau	État	Objectif	Actions pour atteindre/maintenir l'aptitude Les éléments sans le préfixe « o » sont obligatoires pour le seuil du niveau (sous réserve de la justification « non applicable » du profil de portée).	Sources de référence [1] (non exhaustif) (o = facultatif/en fonction de la portée)
3	**Élaboration**	Élaboration de politiques et d'infrastructures de sécurité internes.	☐ Cadre responsable : un cadre responsable institutionnel désigné (p. ex. VP/VPA Recherche ou l'équivalent) est assigné, et fournit une charte écrite pour le responsable de la sécurité du centre de recherche (RSCR)/ chef de la sécurité (portée, droits décisionnels, voie de recours hiérarchique et attentes en matière de ressources) et participe aux examens périodiques de gouvernance. ☐ Stratégie établie et formalisée, ainsi que l'approche pour atténuer les risques avec un plan d'atténuation des risques. a. Processus d'examen des collaborations b. Mécanisme de déclenchement de l'examen préalable des publications ☐ Examen documenté des orientations en matière de sécurité de la recherche (y compris la RTSAP, le cas échéant) et délimitation des activités qui entrent dans le champ d'application selon le profil de portée. ☐ Position en matière de cybersécurité : un plan de cybersécurité comprenant une segmentation et des mesures de contrôle d'accès adaptées au profil de portée, ainsi qu'un inventaire de base des systèmes/ données et des responsables des mesures de contrôle assignés. ☐ Cloisonnement de l'information : un protocole est créé pour s'assurer que les données sensibles à double usage ne sont pas accessibles aux membres du laboratoire qui ne sont pas autorisés à travailler sur ce projet précis. ☐ Protocoles de départ : un protocole formel de fin d'emploi est créé pour révoquer l'accès et récupérer/sécuriser les actifs du projet auprès du personnel sortant (employés, étudiants, chercheurs) qui avait accès aux systèmes ou données visés par la portée.	○ Plan de sûreté fédéral pour les marchandises contrôlées ○ Lignes directrices des trois organismes sur la RTSAP ○ Politique sur la RTSAP ○ Lignes directrices sur la sécurité nationale pour les partenariats de recherche (orientation fédérale) _____ ○ Analyse préliminaire des écarts ○ Orientation institutionnelle/ fédérale sur la sécurité de la recherche et la diligence raisonnable des partenaires (le cas échéant)

Niveau	État	Objectif	Actions pour atteindre/maintenir l'aptitude Les éléments sans le préfixe « o » sont obligatoires pour le seuil du niveau (sous réserve de la justification « non applicable » du profil de portée).	Sources de référence [1] (non exhaustif) (o = facultatif/en fonction de la portée)
3	**Developing**	Building internal security policies and infrastructure.	☐ Flux de travail de sécurité de la recherche en Ontario (selon le profil de portée) : lorsque le financement de la recherche par le ministère de l'Ontario est visé par la portée, un flux de travail documenté existe pour administrer les exigences en matière de sécurité de la recherche à l'échelle du projet (collecte des attestations des chercheurs désignés, soutien à la liste de vérification, élaboration d'un plan d'atténuation des risques au besoin), y compris la conservation des dossiers et une voie de transmission vers la fonction de sécurité de la recherche institutionnelle et le cadre responsable. ○ Cartographie du réseau de partenaires/de l'écosystème : tenir à jour une carte institutionnelle des principaux réseaux de partenaires et des liens contractuels (ainsi que des autres voies de financement viables) pour appuyer la diligence raisonnable en matière de collaboration et la planification de l'atténuation des risques lorsque le profil de portée indique des partenariats à risque plus élevé. ○ Le plan d'atténuation des risques comprend un mécanisme de contrôle des visiteurs. ○ Des indicateurs sont définis pour permettre le suivi du rendement de la gouvernance interne. ○ Cartographie des actifs : tenir à jour une cartographie des actifs relatifs à l'infrastructure scientifique pertinente (équipement clé, installations, capacités spécialisées) et des environnements habilitants (p. ex. enclaves sécurisées, le cas échéant) pour appuyer les discussions sur les partenariats, les décisions relatives au profil de portée et l'établissement des priorités d'investissement. ○ Intervention en cas d'incident : une voie de signalement et de transmission des incidents est définie (rôles, personnes-ressources et autorité décisionnelle), avec une fonction institutionnelle désignée responsable de la coordination. ○ Agent de sécurité de la recherche (ASR) ou équipe attitrés (recommandé pour les profils de portée à risque plus élevé).	

Niveau	État	Objectif	Actions pour atteindre/maintenir l'aptitude Les éléments sans le préfixe « o » sont obligatoires pour le seuil du niveau (sous réserve de la justification « non applicable » du profil de portée).	Sources de référence [1] (non exhaustif) (o = facultatif/en fonction de la portée)
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.	☐ **Le cas échéant** (marchandises/technologies contrôlées en cause) : inscription au Programme des marchandises contrôlées (PMC) amorcée/achevée ou justification documentée de non-applicabilité basée sur le profil de portée. ☐ **Gouvernance des données autochtones** (lorsque déclenchée) : fournir des preuves de la gouvernance des données autochtones applicable (p. ex. PCAP®, le cas échéant), y compris les approbations/dossiers de décision et un plan de gestion des données propre au projet (accès, partage, conservation). ☐ **Mesures de contrôle de sécurité** de la recherche documentées et opérationnelles, et conformes aux orientations applicables (y compris la RTSAP, le cas échéant). ☐ Base de référence cybernétique mise en œuvre au moyen d'une **gestion des risques conforme à l'ITSG-33** (évaluation des menaces et des risques, sélection des contrôles, plan d'action et jalons) ou une voie de certification reconnue, le cas échéant (p. ex. Programme canadien de certification en cybersécurité [PCCC]). ☐ Pour les travaux visés par la RTSAP : les **attestations requises sont dûment remplies** et un **processus documenté d'examen/de recours hiérarchique/de conservation des dossiers** existe (le DURA/la PICO n'effectuent pas de vérification de sécurité par les services de renseignement). ☐ Le dossier de preuves est vérifiable sur le plan administratif (type d'artéfact, responsable, actualité) et **vérifié à l'interne par l'installation** pour en assurer l'exhaustivité et la cohérence interne. ☐ La formation et les protocoles au niveau de l'installation sont élaborés et intégrés à la pratique opérationnelle.	• Programme des marchandises contrôlées (PMC) : Demande d'inscription (formulaire PSPC-TPSGC 445) (le cas échéant) • Trois organismes – RTSAP : attestation(s) et orientations applicables (selon les exigences du profil de portée) • Fondation canadienne pour l'innovation (FCI) : attestation(s) applicable(s), le cas échéant • Cybersécurité (Centre de la sécurité des télécommunications [CST]) : lignes directrices axées sur le cycle de vie de la gestion des risques du guide ITSG-33 ○ Recherche nordique/ arctique ou affiliée aux Autochtones (déclencheur du profil de portée) : • Ressources de Sécurité publique Canada pour la protection de la recherche • *Loi sur l'évaluation d'impact* (le cas échéant) • Principes de gouvernance des données autochtones (p. ex. PCAP®), le cas échéant

Niveau	État	Objectif	Actions pour atteindre/maintenir l'aptitude Les éléments sans le préfixe « o » sont obligatoires pour le seuil du niveau (sous réserve de la justification « non applicable » du profil de portée).	Sources de référence [1] (non exhaustif) (o = facultatif/en fonction de la portée)
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).	☐ Enclave de recherche sécurisée (physique et/ou numérique) avec segmentation et transfert contrôlé des données adaptés au profil de portée. ☐ Le processus contractuel permet l'insertion de clauses de sécurité de la recherche, de clauses de souveraineté des données et de dispositions relatives aux contrôles et aux exportations, le cas échéant. ☐ Diligence raisonnable (sources ouvertes/ partenaires) avant la conclusion des ententes, selon une approche fondée sur le risque. ☐ Exercice sur table d'intervention en cas d'incident effectué au cours des 12 derniers mois (scénario lié au profil de portée). ☐ Les contrats intègrent des clauses appropriées de sécurité et de contrôle souverain conformes aux exigences fédérales applicables et aux besoins des partenaires. ○ Protocole de signalement des contacts non sollicités/activités suspectes en place. ○ Évaluation de base de la sécurité physique complétée (institutionnelle + propre au projet), avec des mesures correctives documentées. ○ Le cas échéant : participation formalisée aux écosystèmes d'innovation en matière de défense dirigés par le gouvernement (p. ex. centres parrainés par le ministère de la Défense/réseaux de recherche sur la défense nationale), avec des interfaces de gouvernance et des voies contractuelles documentées. ○ Profil avancé : capacité démontrée à mener des collaborations sécurisées à travers des réseaux multi-institutionnels ou des centres financés par la défense (le cas échéant), avec des pratiques de gouvernance et de contrôle des extrants reproductibles.	• Sécurité publique Canada : ressources de diligence raisonnable (source ouverte/partenaire), le cas échéant • MDN/SPAC : orientation sur la sécurité industrielle/sécurité physique et clauses de sécurité contractuelles (le cas échéant) • GRC : orientation sur la sécurité physique (le cas échéant) --- ○ Références d'interopérabilité OTAN et TEMPEST (seulement si explicitement requis par le partenaire ou le profil de portée)

Niveau	État	Objectif	Actions pour atteindre/maintenir l'aptitude Les éléments sans le préfixe « o » sont obligatoires pour le seuil du niveau (sous réserve de la justification « non applicable » du profil de portée).	Sources de référence [1] (non exhaustif) (o = facultatif/en fonction de la 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.	☐ Surveillance continue des systèmes d'enclave. ☐ Examens internes périodiques des contrôles et de la gouvernance de la RDU (constatations documentées et suivies jusqu'à la clôture). ☐ Pipeline formalisé de mobilisation de l'industrie, le cas échéant. ☐ Contribution aux écosystèmes nationaux à double usage (Accélérateur d'innovation de défense pour l'Atlantique Nord [DIANA], entreprises principales de défense, réseaux de recherche parrainés par la défense), le cas échéant. ☐ Examen documenté d'amélioration continue effectué au moins annuellement. ☐ La formation est régulièrement mise à jour et déployée. ——————————————————— ○ Profil avancé : satisfaire aux seuils d'admissibilité applicables pour la participation adjacente à l'OTAN (p. ex. voie des centres d'essai du DIANA) et contribuer aux écosystèmes pertinents (le cas échéant).	○ Références des écosystèmes d'innovation adjacents à l'OTAN/de défense (facultatif; selon le profil de portée) : • Références du programme IDEeS (Innovation pour la défense, l'excellence et la sécurité). • Références de la voie des centres d'essai du DIANA de l'OTAN. • Portail d'information de l'Organisation pour la science et la technologie (STO) de l'OTAN.

Notes de bas de page :

1 — Pour les URL et la liste complète des références, voir le document **Glossaire et liens**; cette colonne ne liste que les ancres principales.