DURA Maturity Scale – Framework

Purpose and boundaries.

The DURA Maturity Scale provides a **readiness level and implementation guidance** for Facilities that may support Dual-Use Research (DUR). It is not an accreditation, certification, or compliance verification program.

Scope Profile first.

Before assigning a DURA level, a Facility should define a **Scope Profile** (e.g., STRAC relevance, controlled goods/ export controls, data sensitivity, partner type). The Scope Profile determines which requirements are **applicable** versus **not applicable** at each level and prevents over-scoping controls for low-risk projects.

Facilities may maintain a baseline Scope Profile for typical work and document project-specific Scope Profiles where a collaboration's risk context differs; DURA level claims must reference the Scope Profile used for that claim.

Evidence review model.

References in this scale to "validation," "audit," or "assurance" refer to **evidence presence, completeness, recency, and internal consistency**—not technical certification. Where external programs/standards are cited, they remain owned and administered by their authoritative bodies. DURA requirements and levels are self-attested by Facilities; OCIP/eCampus Ontario do not validate, certify, examine, audit, or review selections.

Level	Status	Objective	Actions to reach / sustain readiness Items without 'o' prefix are mandatory for the level gate (subject to Scope Profile 'not applicable' rationale)	Reference Sources [1] (non-exhaustive) (o = optional / scope-dependent)
0	**Opted-out**	Explicit decision to exclude DUR from the lab's mandate.	No DURA assessment is conducted at this level.	N/A
1	**Neutral**	No current interest or formal consideration of DUR.	No DURA assessment is conducted at this level.	N/A

Level	Status	Objective	Actions to reach / sustain readiness Items without 'o' prefix are mandatory for the level gate (subject to Scope Profile 'not applicable' rationale)	Reference Sources [1] (non-exhaustive) (o = optional / scope-dependent)
2	**Interested**	Identification of dual-use potential in existing research.	☐ Formal recognition of the value of dual-use readiness for the Facility's mandate. ☐ Appointed leader for the dual-use readiness initiative (may be interim). ☐ Basic risk note (one page) identifying likely risk areas and owners. ☐ Preliminary Scope Profile completed to determine whether current or planned projects may trigger research security controls, export controls, controlled goods/ technology considerations, or partner-imposed security clauses. ☐ Completed OCIP's DURA survey (self-assessment), or documented plan to complete it within a defined timeframe. ○ Review G7 Best Practices for Secure and Open Research ○ Awareness communication to relevant personnel (who will be impacted and why). ○ Ontario RS readiness (if applicable): If the Scope Profile indicates likely Ontario Ministry research funding, identify the internal owner and lightweight process to (i) collect Named Researcher attestations and (ii) support completion of the Ontario research-security checklist / risk mitigation artifacts for the project. ○ Initial process sketch describing how collaboration review and data-handling decisions will be made at Level 3.	○ Introductory research security guidance (institutional / tri-agency / federal as applicable) ○ Export controls / controlled goods awareness references (only if indicated by Scope Profile) ○ G7 Best Practices for Secure and Open Research

Level	Status	Objective	Actions to reach / sustain readiness Items without 'o' prefix are mandatory for the level gate (subject to Scope Profile 'not applicable' rationale)	Reference Sources [1] (non-exhaustive) (o = optional / scope-dependent)
3	**Developing**	Building internal security policies and infrastructure.	☐ Executive Sponsorship: A named institutional Executive Sponsor (e.g., VP/AVP Research or equivalent) is assigned and provides a written charter for the RCSL/CSO (scope, decision rights, escalation path, and resourcing expectations) and participates in periodic governance reviews. ☐ Established, formalized strategy, along with the approach to mitigate risk with a Risk Mitigation Plan. a. Collaboration review process b. Publication pre-review trigger mechanism ☐ Documented review of research security guidance (including STRAC where applicable) and identification of which activities fall in-scope per the Scope Profile. ☐ Cybersecurity posture: a Cyber Security Plan with segmentation and access controls appropriate to the Scope Profile, plus a basic inventory of systems/data and assigned control owners. ☐ Information Siloing: A protocol is created to ensure that sensitive dual-use data is not accessible to lab members who are not authorized to work on that specific project. ☐ Departure Protocols: A formal off-boarding protocol is created to revoke access and retrieve/secure project assets from departing personnel (staff, students, researchers) who had access to in-scope systems or data.	○ Federal Security Plan for Controlled Goods ○ Tri-Agency STRAC Guidelines ○ STRAC Policy ○ National Security Guidelines for Research Partnerships (federal guidance) _____ ○ Preliminary Gap Analysis ○ Institutional / federal guidance on research security and partner due diligence (as applicable)

Level	Status	Objective	Actions to reach / sustain readiness Items without 'o' prefix are mandatory for the level gate (subject to Scope Profile 'not applicable' rationale)	Reference Sources [1] (non-exhaustive) (o = optional / scope-dependent)
3	**Developing**	Building internal security policies and infrastructure.	☐ Ontario RS workflow (Scope Profile dependent): Where Ontario Ministry research funding is in scope, a documented workflow exists to administer project-level research-security requirements (Named Researcher attestation collection, checklist support, risk-mitigation plan development as required), including record retention and an escalation path to the institutional research security function and Executive Sponsor. ○ Partner network / ecosystem map: Maintain an institutional map of key partner networks and contractual linkages (and viable alternative funding routes) to support collaboration due diligence and risk-mitigation planning where the Scope Profile indicates higher-risk partnerships. ○ Risk Mitigation Plan includes Visitor Control mechanism ○ Metrics are defined to enable internal governance performance monitoring. ○ Asset mapping: Maintain an asset map of relevant scientific infrastructure (key equipment, facilities, specialized capabilities) and enabling environments (e.g., secure enclaves where applicable) to support partnership discussions, Scope Profile decisions, and investment prioritization. ○ Incident Response: An incident reporting and escalation path is defined (roles, contacts, and decision authority), with an identified institutional function responsible for coordination. ○ Dedicated Research Security Officer (RSO) or team (recommended for higher-risk Scope Profiles).	

Level	Status	Objective	Actions to reach / sustain readiness Items without 'o' prefix are mandatory for the level gate (subject to Scope Profile 'not applicable' rationale)	Reference Sources [1] (non-exhaustive) (o = optional / scope-dependent)
4	**Validating**	Evidence-supported readiness: controls and governance are documented and reviewable for completeness and consistency.	☐ **If applicable** (controlled goods/technology involved): CGP registration initiated/ completed or documented "not applicable" rationale based on Scope Profile. ☐ **Indigenous data governance** (when triggered): provide evidence of applicable Indigenous data governance (e.g., OCAP® where relevant), including approvals/decision records and a project-specific data stewardship plan (access, sharing, retention). ☐ Research **security controls** documented and in operation, aligned to applicable guidance (including STRAC where relevant). ☐ Cyber baseline implemented via **ITSG-33-aligned risk management** (TRA, control selection, remediation plan/POA&M) or an accepted certification pathway where applicable (e.g., CPCSC). ☐ For STRAC-in-scope work: required **attestations are completed** and a documented **review/escalation/record-retention process** exists (DURA/OCIP do not conduct intelligence vetting). ☐ Evidence package is administratively verifiable (artifact type, owner, recency) and **internally checked by the Facility** for completeness and internal consistency. ☐ Training and facility-level protocols are developed and integrated into operational practice.	○ Controlled Goods Program (CGP): Application for Registration (Form PSPC-TPSGC 445) (if applicable) ○ Tri-Agency STRAC: applicable attestation(s) and guidance (as required by Scope Profile) ○ CFI: applicable attestation(s) where relevant ○ Cybersecurity (CSE): ITSG-33 risk management lifecycle guidance --- ○ Northern/Arctic or Indigenous-affiliated research (Scope Profile trigger): • Public Safety Canada safeguarding research resources • Impact Assessment Act (where applicable) • Indigenous data governance principles (e.g., OCAP®) as applicable

Level	Status	Objective	Actions to reach / sustain readiness Items without 'o' prefix are mandatory for the level gate (subject to Scope Profile 'not applicable' rationale)	Reference Sources [1] (non-exhaustive) (o = optional / scope-dependent)
5	**Ready**	Governance and security controls are active and sufficient for compliant execution of partner agreements that impose elevated security, data, or sovereignty requirements (as indicated by Scope Profile).	☐ Secure research enclave (physical and/or digital) with segmentation and controlled data transfer appropriate to Scope Profile. ☐ Contracting process supports insertion of research security clauses, data sovereignty clauses, and export/control handling where applicable. ☐ Open-source / partner due diligence performed prior to signing agreements (risk-based). ☐ Tabletop incident response exercise conducted within the past 12 months (scenario tied to Scope Profile). ☐ Contracts incorporate appropriate security and sovereign control clauses consistent with applicable federal requirements and partner needs. ○ Unsolicited contact / suspicious activity reporting protocol in place. ○ Physical security baseline assessment completed (institutional + project-specific), with documented remediation actions. ○ Where relevant: formalized participation in government-led defence innovation ecosystems (e.g., defence-ministry–sponsored centres / national defence research networks), with documented governance interfaces and contracting pathways. ○ Advanced profile: demonstrated capability to execute secure collaborations across multi-institution networks or defence-funded centres (where applicable), with repeatable governance and output-control practices.	○ Public Safety Canada: open-source / partner due diligence resources (where applicable) ○ DND / PSPC: industrial security / physical security guidance and contracting security clauses (where applicable) ○ RCMP: physical security guidance (where applicable --- ○ NATO interoperability and TEMPEST references (only if explicitly required by partner or Scope Profile)

Level	Status	Objective	Actions to reach / sustain readiness Items without 'o' prefix are mandatory for the level gate (subject to Scope Profile 'not applicable' rationale)	Reference Sources [1] (non-exhaustive) (o = optional / scope-dependent)
6	**Engaged**	Governance system institutionalized and demonstrated through sustained, compliant execution of multiple dual-use collaborations, with measurable continuous improvement.	☐ Continuous monitoring of enclave systems. ☐ Periodic internal reviews of DUR controls and governance (findings documented and tracked to closure). ☐ Formalized industry engagement pipeline, if applicable. ☐ Training is regularly updated and deployed. _____ ○ Advanced profile: Meet applicable eligibility thresholds for NATO-adjacent participation (e.g., DIANA Test Centre pathway) and contribute to relevant ecosystems (where appropriate).	○ NATO-adjacent / defence innovation ecosystem references (optional; Scope Profile dependent): • IDEaS (Innovation for Defence Excellence and Security) program references. • NATO DIANA Test Centre pathway references. • NATO Science & Technology Organization (STO) information portal.