

Dual-Use Readiness Assessment (DURA) Methodology

Target: Higher Education Institution (HEI)-Affiliated Research Facilities, including universities, colleges, and Indigenous Institutes

Date: September 1, 2026 | Version: 2.0

1. Executive Summary

Ontario's publicly funded HEIs are facing increased expectations around research security and responsible collaboration, particularly where projects have dual-use potential. DURA helps Facilities identify the organizational capabilities and controls needed to participate responsibly in dual-use collaborations, including defence-related opportunities. DURA is a self-guided assessment that may be used independently of any platform. It produces a readiness level and recommended actions, and it references authoritative programs and standards where relevant; it does not certify compliance or replace those authorities.

DURA is a seven-level stage-gate readiness framework, comprising Levels 0 through 6, designed to assess and guide the organizational readiness of Canadian HEI-affiliated research Facilities that may participate in Dual-Use Research collaborations. DURA does not assess the scientific merit of research; the technical performance, suitability, or readiness of equipment, infrastructure, or technologies; the quality of research outputs; or the competence of individual researchers. Facilities may use DURA for self-assessment. Institutions may use the resulting assessment for internal governance reporting or may commission an independent review conducted outside the DURA level-assignment process. Such review does not constitute DURA certification or change the self-assessed nature of the level.

Applying DURA requires balancing open and collaborative research with proportionate safeguards against unauthorized, inappropriate, or harmful access to research knowledge, information, assets, and outputs. This balance may also engage ethical, institutional, contractual, and public-policy considerations. Responsible management of intellectual property and other intangible assets forms part of this balance, supporting both research integrity and the protection of Canadian innovation.

IMPORTANT SCOPE NOTE:

DURA provides a readiness level and implementation guidance only. It is not an accreditation, certification, audit, or compliance-verification program. DURA uses evidence to support a Facility's self-assessed readiness claim. Evidence is reviewed internally under the coordination of the RCSL for presence, completeness, recency, and internal consistency, with responsible institutional and Facility functions participating as appropriate. Each evidence artifact must have an identified evidence owner and be traceable to the applicable requirement, Profile version, and declared scope. DURA does not validate, certify, audit, or determine compliance; perform security clearances or intelligence vetting; or replace authoritative standards, programs, regulators, funders, contracting authorities, or certification bodies.

2. Interpretive Foundations

2.1. Dual-Use Research Scope

The Glossary is the canonical source for the DURA definition of Dual-Use Research. For DURA purposes, dual-use potential may be intended, secondary, emerging, unintended, or identified after the work begins; it does not depend solely on how an activity was originally described or funded.

DURA uses this working concept to identify potential readiness needs and applicable requirements. It does not make an authoritative determination that an activity is dual-use, sensitive, or within the scope of an external program. Where a law, regulation, funding program, contract, or external authority invokes a particular definition, list, or threshold, that instrument governs for that purpose.

2.2. Collaboration Obligations and Flow-Down

Dual-use collaborations among Higher Education Institutions, industry partners, and government organizations may introduce governance and delivery challenges when projects involve sensitive technologies, foreign partners, controlled information or goods, intellectual property, publication constraints, or other legal, funding, institutional, or contractual requirements. Research Facilities therefore require clear processes to identify applicable obligations, determine whether they can be accepted, allocate responsibilities, and implement proportionate controls.

Requirements may apply directly to a party through law, regulation, funding conditions, institutional

policy, or an external program requirement. Other requirements may be allocated through a prime contract, subcontract, sponsored-research agreement, or other collaboration agreement. A downstream party does not automatically inherit every upstream obligation, and contractual flow-down does not relieve the upstream party of accountability to its own customer, funder, regulator, or contracting authority. Each party remains responsible for obligations that apply directly to it, commitments it accepts, and controls within its authority. The business partner is normally responsible for identifying and communicating applicable upstream requirements, obtaining required approvals, and managing its downstream relationship. The HEI is responsible for determining whether it can accept those requirements and for implementing agreed controls within its institutional and Facility environments. Responsibilities for shared controls, evidence, reporting, change management, and incident response should be allocated explicitly in the project agreement.

DURA provides a structured method for assessing whether a Facility has the governance capability to identify, accept, implement, evidence, and sustain the requirements applicable to a proposed collaboration. It does not determine legal liability, establish regulatory or contractual applicability, or reassign accountability among the parties.

The strategic and policy context for DURA, including its alignment with Canada's Defence Industrial Strategy and the Framework for the Ontario Defence Industrial Strategy, is addressed in Appendix D, the non-normative DURA Defence Industrial Policy Appendix.

2.3. Field Allocation and Cross-References

Record or document	Content maintained	Boundary
Appendix A: Facility Capability Profile	Standing Facility record: declared scope, capabilities, institutional and third-party dependencies, supported environments and information categories, external prerequisites, constraints, evidence and review dates.	Records what the Facility can support and under what conditions. It does not determine project compatibility.
Appendix B: Project Scope & Obligations Profile	Project input record: activities, technologies, partners and funders, participants and access, information and assets, outputs, obligations, external prerequisites, applicability indicators and not-applicable rationales.	Records what the project requires. It does not determine whether the Facility can support those requirements.
Appendix C: Project Compatibility Determination	Decision record: congruence, gaps, caveats, dependencies, treatments, conditions, hold points, responsibility allocations, approvals, monitoring, reassessment and the controlled compatibility outcome.	Applies to the referenced Appendix A and B versions. It is not project acceptance or external authorization.
DURA Framework	Readiness levels, Five Capability Pillars, requirement IDs and classifications, applicability conditions, level gates, evidence expectations, external-prerequisite boundaries and sustainment requirements.	Defines DURA requirements. Profiles may activate or evidence requirements but cannot create, remove or redefine them.
DURA Methodology	Assessment sequence, roles, profile use, compatibility process, evidence handling, reassessment, interpretation, boundaries and minimum records.	Explains how the Framework and controlled records are applied.
Glossary and Bibliography	Preferred terms and definitions; Source IDs, citations, authority, currency, mappings and review records.	Provide terminology and source governance; they do not create DURA requirements.

2.4 Scope and Interpretation

- Applicable law, regulation, funding conditions, contracts, institutional authorities, specialist committees, regulators and external programs govern their own definitions, thresholds, approvals and authorizations. DURA focuses on applicability, status, conditions and evidence expectations but does not replace those authorities.
- Ontario research-security requirements and federal STRAC or affiliations-of-concern requirements are separate processes and must be assessed and recorded separately when applicable.
- A registration, clearance, certification, permit, licence or authorization held by a business partner, another institution or another organizational unit does not automatically extend to the HEI, Facility, project, system, location or participant population.
- Participant and access decisions must be based on roles, activities and documented governing requirements. Nationality, citizenship, residency, immigration status or institutional affiliation must not be used as automatic proxies for risk or access restriction.
- When a Conditional Requirement does not apply, record a concise not-applicable rationale in Appendix B or the related assessment record. Detailed profiles, determinations, evidence, gaps and conditions are controlled institutional records unless an authorized disclosure or summary has been approved.
- A material change to project scope, obligations, participants, information, assets, outputs, environments, external prerequisites, Facility capabilities or evidence validity requires the affected profiles, requirements and compatibility determination to be reviewed before the affected work begins or continues.

3. DURA Purpose and Scope

3.1 Objective

The purpose of the DURA Methodology is to provide a structured approach for evaluating the organizational readiness of HEI-affiliated research Facilities that may participate in Dual-Use Research collaborations with industry or government partners.

The DURA Methodology supports consistent interpretation and application of the DURA Framework by defining the scope of assessment, the evidence-handling process used to substantiate readiness claims, and the process through which Facilities assess and improve their readiness.

The DURA assessment focuses on the organizational capabilities required to participate responsibly in Dual-Use Research collaborations. It considers Governance & Accountability, Partnerships & Obligations, People & Access, Environments & Assets, and Information, IP & Outputs. It does not assess the scientific merit of research; the technical performance, suitability, or readiness of equipment, infrastructure, or technologies; the quality of research outputs; or the competence of individual researchers. The DURA Methodology helps Facilities understand and progressively strengthen the organizational capabilities needed to manage research security, collaboration risks, applicable obligations, access, sensitive environments and assets, and the responsible handling and dissemination of information, intellectual property, and research outputs.

Within DURA, the Framework defines the readiness levels and requirements. The DURA Methodology defines the interpretation principles, roles, assessment process, evidence handling, and sustainment rules used to apply those requirements. Appendices A-C document the declared scope, applicability inputs, and project compatibility. DURA is applied using institutional records and processes.

Readiness, compatibility, project acceptance, and individual participation are separate determinations. A Facility may possess the capability to support a project and still decide not to accept it. A Compatible or Compatible with Conditions determination does not authorize or compel the project to proceed. Work may begin only after all required institutional approvals, project-acceptance decisions, contractual arrangements, and participant arrangements are complete.

3.2 Scope and Applicability

The DURA Methodology applies to the institutional and operational scope described below. It identifies the types of research Facilities covered by the Framework and the conditions that make particular readiness requirements applicable.

The initial DURA implementation is Ontario-focused. Institutions may apply the Framework, Methodology, and controlled records through their own governance and recordkeeping processes. DURA is designed for broader Canadian use because research security, export controls, and defence-collaboration obligations operate primarily at the federal level.

To avoid unnecessary compliance burden and ensure proportional controls, DURA uses a profile-first architecture. The architecture separates the Facility's standing capabilities from the requirements and obligations of a specific project, then records whether the two are compatible. A DURA level is meaningful only when referenced to the Facility Capability Profile on which the claim is based; it does not imply readiness for every possible dual-use project.

- **Facility Capability Profile.** Before claiming a DURA level, the Facility must maintain a version-controlled standing record of the organizational capabilities and institutional dependencies it can provide for dual-use work. The profile records capabilities across the DURA pillars, together with relevant external registrations,

certifications, authorizations, and constraints. It answers: What can this Facility support, and under what conditions?

- **Project Scope & Obligations Profile.** Before accepting a proposed collaboration, the Facility must document the project's activities, partners, funding, information, assets, outputs, and applicable legal, regulatory, funding, institutional, and contractual requirements. It must identify direct, flowed-down, and shared obligations, including the responsible and evidence-owning parties. Institutional posture, including affiliation with a military university or defence academy, must be recorded where it may affect security clauses, oversight expectations, or partner requirements. The profile answers: What does this project require?
- **Project Compatibility Determination.** The Facility compares the Project Scope & Obligations Profile with the Facility Capability Profile and records one of three outcomes: Compatible; Compatible with Conditions; or Not Currently Compatible. Conditions, gaps, required approvals, additional controls, responsibility allocations, and evidence requirements must be documented before the affected work begins. Where material information is incomplete or unresolved, the record remains Draft, Under review, or Deferred and no compatibility outcome is selected. These are record statuses, not additional outcomes. The determination answers: Can this Facility support this project under its actual requirements?

Both profiles and the determination are living, version-controlled records. A material change to Facility capabilities or project scope and obligations requires the affected requirements and compatibility determination to be reassessed. This architecture determines which Conditional Requirements apply, supports a documented not-applicable rationale where appropriate, and avoids imposing controls that are not relevant to lower-risk work. Appendices A-C define and maintain the operational questions

and fields used in those instruments; the Framework defines the requirements, and this Methodology defines process, interpretation, and cross-cutting boundaries.

3.3 Assessment Principles

The DURA Methodology aligns with Canadian safeguarding-research principles commonly used by research-intensive U15 universities, including transparency, predictability, meaningful engagement and inclusivity, and shared responsibility. Its application remains proportionate to the Facility Capability Profile, Project Scope & Obligations Profile, and applicable obligations.

The following principles guide how research Facilities apply DURA:

1. **Proportionality:** requirements are applied according to the Facility Capability Profile, the Project Scope & Obligations Profile and the associated risk and obligation context.
2. **Open and secure research:** restrictions on access, collaboration, or dissemination must be risk-based, proportionate, justified, documented, and no broader or longer than necessary for the declared scope and applicable obligations.
3. **Evidence-Based Assessment:** advancement requires documentary or procedural evidence demonstrating that governance mechanisms are implemented.
4. **Cumulative stage gates:** level claims are determined using the cumulative and pillar-level gates defined in the DURA Framework; this Methodology governs the related applicability, evidence, and assessment records.
5. **Organizational Readiness Focus:** the assessment evaluates organizational readiness, not research quality, technical capability or personnel competence.

6. **Continuous Improvement:** higher readiness levels require monitoring and periodic review to sustain governance practices.

7. **Equity and non-profiling:** DURA implementation and research security messaging must be applied in an anti-racist, inclusive manner, avoiding prejudice or profiling while still managing legitimate research security risks.

3.4 Key Roles in the DURA Process

DURA is intended for routine use within existing HEI structures. Its core institutional functions are an Executive Sponsor, an institutional research security function where one exists, and a Facility-level Research Centre Security Lead responsible for day-to-day coordination. Titles and organizational structures vary; the responsibilities below define the functions required for DURA and do not require new positions.

For each applicable requirement, the Facility must identify the accountable party, operational control owner, evidence owner, and applicable approval, reporting, and escalation path. Responsibilities that apply to the business partner, HEI, Facility, or multiple parties must be recorded explicitly. A Facility may rely on capabilities delivered by central institutional functions or third parties, but it must not assume those capabilities satisfy a DURA requirement until their scope, availability, responsible owner, and supporting evidence have been confirmed for the declared Facility or project scope.

8. **Executive Sponsor (e.g., VP/AVP Research or equivalent).** The Executive Sponsor is the accountable institutional leader for DURA governance and for institutional decisions that exceed the Facility's delegated authority. The role provides decision authority, resolves escalations, supports allocation of resources, and ensures that institutional functions required by the Facility Capability Profile or a Project

Compatibility Determination are engaged. The Executive Sponsor also ensures that external prerequisites, elevated risks, unresolved responsibility gaps, and obligations requiring institutional acceptance are referred to the appropriate authority. Accountability in this role does not mean that the Executive Sponsor is the operational owner of every control.

9. Research Security Officer (RSO) / Research Security Office (institutional function). Where present, the RSO supports consistent research security practices across the HEI. The function provides guidance on research security policy, partner due diligence, training, incident reporting, escalation pathways, and applicable government or funding-program requirements. It coordinates, as appropriate, with institutional functions responsible for legal and contracting matters, cybersecurity, privacy, ethics, controlled goods, export controls, records management, Indigenous engagement and data governance, and other relevant services. The RSO helps confirm whether institutional research security services cover the declared scope and identifies gaps, dependencies, or external prerequisites requiring escalation. The RSO does not certify, validate, or approve a Facility's DURA level and does not replace the authority of other institutional or external functions.

10. Research Centre Security Lead (RCSL). The RCSL is the Facility-designated lead responsible for coordinating DURA activities within a lab, institute, centre, or other research Facility. The RCSL maintains the Facility Capability Profile, coordinates preparation of the Project Scope & Obligations Profile and Project Compatibility Determination, and coordinates reassessment when the Facility or project scope changes. The RCSL maps applicable requirements to business, HEI, Facility, or shared responsibilities; coordinates the assignment of operational control and evidence owners; confirms institutionally supplied capabilities with the responsible functions; and maintains the

Facility's DURA assessment documentation and evidence references. The RCSL escalates unresolved gaps, required approvals, external prerequisites, and resource or authority needs to the RSO, Executive Sponsor, or other responsible function. For DURA purposes, "RCSL" is a role definition; the individual may hold another formal title at the HEI, such as lab manager, operations director, centre administrator, research security officer, or another appropriately authorized role.

3.5 Assessment Process

The assessment process does not use scoring or weighting. The Facility applies the DURA Framework to the current Profile records, determines applicability, assigns responsible functions, records results, and addresses gaps and external prerequisites before claiming or retaining a level.

The RCSL coordinates the assessment by confirming current Profile versions and declared scope; identifying applicable Mandatory and Conditional Requirements; recording each applicability indicator outcome and any required not-applicable rationale; assigning responsible entities, control owners, evidence owners, and reporting paths; and escalating unresolved gaps, responsibility issues, or external prerequisites. Evidence records and internal review are handled under section 3.6.

11. Ontario-specific note (MCURES research security): MCURES research-security requirements are assessed on a per-project basis as part of a funding process. In DURA, these requirements become applicable when the relevant indicator is met in the Project Scope & Obligations Profile. Facilities are not expected to maintain MCURES forms as standing Facility artifacts unless they anticipate MCURES funding, in which case the Facility should demonstrate an internal process to collect, retain, and escalate the required project-level attestations and mitigation artifacts.

For each pillar, the Facility records whether all applicable requirements through the target level are satisfied and determines the overall level using the DURA Framework's cumulative and pillar-level gates. Optional Practices may be recorded as improvement opportunities or evidence of stronger implementation, but they do not affect level determination.

Project-specific assessment uses the current Facility Capability Profile, Project Scope & Obligations Profile, and Project Compatibility Determination. The resulting assessment record is maintained under section 5.2. Reassessment and sustainment are governed by section 6.2.

3.6 Evidence Records and Internal Review

The following rules govern the internal creation, review, retention, and maintenance of evidence records. Within DURA, the Framework defines the evidence expected by each requirement and level. DURA is self-guided; evidence is reviewed through the Facility's institutional process and is not externally validated or approved as part of DURA.

Required evidence must be retained by the Facility or responsible institutional function. Each artifact must identify an evidence owner and remain traceable to the applicable requirement, Profile version, declared scope, and, where relevant, the external prerequisite or authorization it supports. Evidence may be indexed in an Evidence Register and assembled into an Evidence Package.

- **Evidence review:** the RCSL coordinates an internal review for presence, completeness, recency, and internal consistency, with responsible evidence owners and institutional or Facility functions participating as appropriate. These checks apply to the evidence required by the Framework and do not create an additional level gate.
- **Internal review:** the RCSL confirms that the responsible institutional and Facility functions have completed their portions of the

assessment. Review participation should reflect the declared scope and may include IT, the research office, environmental health and safety, biosafety, radiation safety, emergency management, legal, privacy, or other responsible functions. More structured review may be used as the claimed level, scope, or risk increases.

- **Assurance boundary:** internal review does not constitute DURA certification, validation, approval, audit, or a legal-compliance determination. DURA does not require independent review as a level gate. A Facility may commission one based on its risk posture or may be required to obtain one under a law, contract, funding condition, institutional policy, or external program. Any resulting opinion, report, or certification must be described using the terminology and scope of that external process and must not be represented as DURA validation or certification.

The RCSL should have sufficient knowledge of the Facility and applicable institutional requirements to coordinate the assessment while engaging independent institutional functions where their authority or expertise is required.

3.7 Terminology & Definitions

A common language is required to support consistent interpretation across Research Facilities, HEIs, businesses, government partners, and the defence and security community. The controlled DURA Glossary is the canonical source for terminology, acronyms, definitions, and related Source IDs. The controlled DURA Bibliography is the canonical source register for citations, issuing authorities, links, source classifications, mappings, and currency information. DURA documents should reference the relevant controlled term or Source ID rather than duplicate definitions or source URLs, except where a direct operational link is necessary.

The Government of Canada's Safeguarding Your Research portal, Emerging Technology Trend Cards, Research Security Centre, and Safeguarding Science training modules, including Module 2 on dual-use technologies, are complementary awareness and implementation resources. They may support education, risk recognition, due diligence, and institutional capacity development, but they do not independently create DURA requirements or replace applicable laws, policies, funding-program criteria, contracts, or external-authority determinations.

4. Applying the DURA Framework

4.1 Framework Application

Within DURA, the Framework defines the seven readiness levels, status labels, objectives, requirements, classifications, pillar assignments, evidence expectations, external prerequisites, and level gates. This Methodology governs how applicability, evidence, and assessment results are interpreted, documented, and maintained.

A DURA level claim is tied to a version-controlled Facility Capability Profile and its declared scope. DURA assessments are organized across the Five Capability Pillars: Governance & Accountability, Partnerships & Obligations, People & Access, Environments & Assets, and Information, IP & Outputs. The Glossary is the canonical source for the pillar definitions, and the Framework defines the assignment of requirements to pillars and levels.

4.2 Assessment Application

Apply the DURA Framework using the assessment process in section 3.5, the evidence-record and internal-review process in section 3.6, and the level-claim recordkeeping requirements in section 5.2. Within DURA, the Framework defines requirement classifications, cumulative and pillar-level gates, evidence expectations, and level determination.

5. Key Considerations

5.1 Institutional Data Governance and Indigenous Data Sovereignty

The Project Scope & Obligations Profile identifies whether the project involves Indigenous partners or communities, Indigenous-led research, Indigenous data, Indigenous IP, traditional knowledge, research on Indigenous lands or contexts, or other community-specific governance considerations. The applicable authority, protocol, agreement, or principle must be confirmed with the community or its authorized representative. OCAP® may be relevant to First Nations data, but it is not a universal Indigenous data-governance framework.

Where an Indigenous context is identified, DURA Framework requirement IIO-4.01 governs the applicable requirement and evidence expectations. Depending on the project, related controls may also engage Governance & Accountability, Partnerships & Obligations, People & Access, and Environments & Assets. The Facility should document roles, decision rights, consent and approval processes, data and IP ownership or stewardship, attribution, access, use, sharing, publication, benefit-sharing, retention, and disposal.

Evidence should demonstrate that the applicable community-specific requirements have been agreed and implemented. It may include governance approvals, community or research agreements, protocols, stewardship plans, provisions for Indigenous IP and traditional knowledge, access controls, and retention or disposal arrangements. Evidence records and internal review follow section 3.6. DURA does not determine community rights or certify compliance with Indigenous governance requirements.

5.2 Recording and Maintaining a DURA Level Claim

Self-assessment only. DURA levels are self-assessed by the Facility using controlled institutional processes and assessment documentation. The self-assessment does not constitute external review, approval, validation, certification, audit, or assurance over the Facility's requirement selections, evidence, controls, policies, or practices.

Claim prerequisites. Before recording or maintaining a level claim, the RCSL must confirm that:

- A current, version-controlled Facility Capability Profile and declared scope are in place;
- Any Project Scope & Obligations Profile and Project Compatibility Determination relevant to the claim are current;
- Applicability decisions and any required not-applicable rationales have been recorded;
- Pillar-level results and the overall level have been determined and recorded in accordance with the DURA Framework; and
- Required evidence has been retained and checked under section 3.6, and the sustainment and reassessment conditions in section 6.2 are satisfied.

Minimum claim record. The recorded claim must identify the applicable Facility Capability Profile version and declared scope, submitting role, submission date, pillar-level results, and resulting self-assessed level. It must also identify any Project Scope & Obligations Profile and Project Compatibility Determination versions relevant to the claim.

Evidence retention and implementation boundary. Evidence remains institutionally retained. DURA does not require evidence to be uploaded outside the institution as a level gate.

Claim maintenance and history. A DURA level claim remains valid only while the sustainment conditions in section 6.2 are met. Superseded claims must remain controlled historical records linked to the replacement claim and the applicable Profile versions.

5.3 Allied and NATO-Linked Requirements

Where a Project Scope & Obligations Profile identifies allied or NATO-linked requirements, the Facility must record the governing source, responsible authority, obligated entity, applicable prerequisites, required evidence, and any conditions or restrictions. External prerequisites are assessed and tracked under DURA Framework requirement PAR-5.02.

Participation in NATO-adjacent or defence-innovation ecosystems may be recorded as an Optional Practice under PAR-6.03. No DURA level establishes eligibility for a DIANA program, participation in the DIANA test-centre network, technical competence, NATO accreditation, authorization to access or handle classified information, or personnel security clearance. These determinations remain with the responsible external authority.

6. Post-Assessment Governance

6.1 Gap Analysis and Remediation Planning

The gap analysis identifies each unsatisfied or at-risk requirement and records the required action, responsible owner, target date, interim control where needed, evidence required for closure, and closure status. The remediation plan must be updated as actions progress, conditions change, or new gaps are identified. Closed actions remain traceable to the affected requirement, Profile version, and level claim. Corrective actions arising from reassessment under section 6.2 are managed through this process.

6.2 Continuous Monitoring and Reassessment Cycle

Continuous monitoring and reassessment sustain a DURA level after it is recorded. Facilities at Levels 5 and 6 must reassess at least annually. At any level, reassessment is also required when there is a substantive change to a Facility Capability Profile or Project Scope & Obligations Profile; a material change to personnel, partners, obligations, information, assets, authorizations, external prerequisites, or operating conditions; or evidence or a prerequisite expires, is suspended, or is no longer valid.

The RCSL coordinates review of the affected Profile records, requirements, evidence, pillar results, level claim, and Project Compatibility Determination. The Facility must document remediation under section 6.1, revise project conditions as required, and temporarily lower its self-assessed level if current-level requirements are no longer met. At Level 6, monitoring, internal review, training refresh, and continuous improvement should form part of normal institutional practice and feed the remediation and reassessment cycle.