Dual-Use Readiness Assessment (DURA) Framework

Target: Higher Education Institution (HEI)-Affiliated Research Centres (Universities, Colleges, and Indigenous Institutes)

Date: March 31, 2026 | Version: 2.5

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 provides a practical readiness assessment and roadmap that helps Facilities identify the governance, personnel practices, infrastructure controls, and output controls they need in order to participate safely in dual-use collaborations through OCIP. DURA 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.

The DURA is a **seven-level** stage-gate maturity framework **(Levels 0, 1, 2, 3, 4, 5, and 6)** designed to evaluate and guide Canadian Higher Education Institutions (HEIs) in their ability to conduct Dual-Use Research (DUR), by assessing their organizational readiness and governance maturity (controls, compliance, risk management). DURA does not assess laboratory equipment, research output quality, or personnel competencies. Institutions may use DURA for self-assessment, internal governance reporting, or third-party validation.

The delicate nature of this initiative is largely due to the balance between open science and the need to prevent malicious knowledge transfer, as well as potential ethical, moral, or policy conflicts.

IMPORTANT SCOPE NOTE:

DURA provides a **readiness level** and **implementation guidance** only. It is **not** an accreditation, certification, or compliance verification program. Where DURA refers to "validation" or "evidence," this means an attestation by the HEI Facility (please refer to section 7.3). DURA and OCIP do **not** perform technical audits, security clearances, intelligence vetting, or formal compliance assurance, and instead reference authoritative standards and programs (e.g., Government of Canada guidance, ISO, NATO) that remain owned and administered by their respective authorities.

2. Policy Context

2.1. Dual-Use Research Context

Dual-Use Research (DUR) refers to scientific and technological work that is intended for legitimate civilian or commercial purposes but may also have potential applications in national security, defence, or other sensitive domains. Many emerging technologies—such as artificial intelligence, cyber capabilities, quantum technologies, advanced materials, space systems, and autonomous platforms—fall into this category.

In Canada and among allied countries, growing attention has been directed toward the governance of dual-use research conducted within publicly funded research environments. Higher Education Institutions (HEIs) and research institutes play a central role in the early stages of innovation, but their traditionally open research culture can create challenges when projects intersect with controlled technologies, sensitive data, or national security considerations.

Federal initiatives such as the Government of Canada's research security guidance, including Sensitive Technology Research and Affiliations of Concern (STRAC), and related export control and controlled goods regimes, highlight the importance of managing these risks while maintaining the benefits of open scientific collaboration. Research institutions increasingly require governance mechanisms that allow them to identify, assess, and manage dual-use risks in a structured and proportionate manner.

The DURA framework is intended to support this need by providing a **governance readiness model** that helps research facilities understand and progressively strengthen their internal controls and processes related to dual-use collaboration. Canada's approach to research security aligns with allied guidance on maintaining secure and open research, including the *G7 Best Practices for Secure and Open Research*.

2.2. Research-Industry Collaboration

Collaboration between higher education institutions (HEIs), industry partners, and government organizations is a central feature of Canada's innovation ecosystem. Research centres within HEIs frequently contribute to the early stages of technological development, including applied research, prototyping, and validation activities that may later transition to industrial development and commercialization.

Programs at both federal and provincial levels—including defence innovation initiatives, research partnership programs, and collaborative innovation platforms—encourage these partnerships in order to accelerate the development of advanced technologies and strengthen Canada's innovation capacity.

At the same time, such collaborations may introduce governance challenges when projects involve sensitive technologies, foreign partners, controlled information, or contractual security requirements. Research facilities therefore benefit from having clear internal processes to manage issues such as research security, export controls, partner due diligence, data governance, and the responsible dissemination of research outputs.

The DURA framework provides a structured method to help research facilities assess their governance readiness for these types of collaborations and to identify practical steps that support responsible participation in dual-use innovation ecosystems.

2.3. Canada's Defence Industrial Strategy

Canada's *Defence Industrial Strategy (DIS): Security, Sovereignty and Prosperity*, emphasizes strengthening the country's defence industrial base by supporting the development and commercialization of advanced and dual-use technologies through collaboration among industry, government, and research institutions.

Many of the technology domains highlighted in the strategy originate or mature within academic and publicly funded research environments. As collaboration between these facilities and defence-relevant industry expands, institutions require governance structures capable of supporting responsible dual-use research while protecting national security interests, intellectual property, and research integrity.

The relationship between the DURA framework and the Defence Industrial Strategy is described in greater detail in the *Appendix: "DURA Framework in the Context of Canada's Defence Industrial Strategy*

(DIS)." The Appendix explains how DURA operates at the institutional level by providing a governance readiness model for research facilities participating in the broader defence innovation ecosystem.

The following section describes the methodology used to apply the DURA readiness model and evaluate governance maturity within HEI research facilities.

3. DURA Purpose and Scope

3.1. Objective

The purpose of the DURA methodology is to provide a structured approach for evaluating the governance readiness of HEI research facilities that may participate in dual-use research collaborations with industry or government partners.

The methodology supports the consistent interpretation and application of the DURA readiness model by defining the scope of the assessment, the evidence model used to substantiate readiness claims, and the process through which facilities progress through the readiness levels.

The DURA assessment focuses exclusively on governance readiness. It does not assess laboratory infrastructure performance, scientific output quality, or the competencies of individual researchers. The framework is intended to help research facilities understand and progressively strengthen their internal governance mechanisms related to research security, collaboration risk management, and responsible handling of sensitive technologies and information.

3.2. Scope and Applicability

This section defines the institutional and operational scope of the DURA methodology. It clarifies which types of research facilities the framework is intended to evaluate and establishes the applicability conditions under which specific readiness requirements become relevant.

The initial implementation of DURA focuses on research facilities participating in the Ontario Collaborative Innovation Platform (OCIP) operated by eCampusOntario. While the current deployment is limited to Ontario institutions, both the DURA framework and the OCIP platform are designed to be applicable across Canada given that research security, export controls, and defence collaboration policies operate primarily at the federal level.

3.2.1. Scope Profile (Applicability Triggers)

To avoid unnecessary compliance burden and to ensure proportional controls, DURA uses a Scope Profile mechanism. The **Scope Profile** defines the risk environment of the intended collaborations and determines which readiness requirements are applicable.

Institutional posture note: Facilities embedded within, or formally affiliated with, military universities/defence academies (e.g., institutions under defence authority) should record this posture in the Scope Profile, as it may affect applicable security clauses, oversight expectations, and partner requirements even when the research activity remains civilian-led.

Before assigning a DURA level, the Facility should define a Scope Profile for the intended collaboration(s). The Scope Profile is a living record. Facilities should maintain a **Baseline Scope Profile** representing their typical collaboration posture, and document project-specific **deltas** when a proposed collaboration introduces higher sensitivity, different partners, regulated/controlled technology, or segregated environment needs.

The Scope Profile determines which conditional readiness requirements are **applicable** versus **not applicable** and prevents over-scoping controls for low-risk projects. The Scope Profile should record, at minimum:

- **STRAC relevance:** whether the work involves **Sensitive Technology Research Areas** and therefore triggers enhanced research security measures.

- **Ontario research-funding Research Security (RS) (project-based):** whether the collaborations are expected to be submitted under Ontario Ministry research funding programs that apply Ontario's research security process (e.g., named-researcher attestations, risk checklist, mitigation plan). If triggered, include the project's Ontario RS artifacts and identify the Facility's internal owner for administering them.
- **Controlled goods / export controls:** whether the work involves controlled goods, **controlled technology, or export-controlled items/data,** which may trigger specific federal programs and contractual requirements.
- **Data sensitivity classification:** the highest sensitivity class of data expected (e.g., public, protected, controlled, regulated, export-controlled).
- **Indigenous data / partnership trigger:** whether the project involves Indigenous partners/communities, Indigenous-led research, Indigenous-identifiable data, or research conducted on Indigenous lands/contexts. If triggered, the evidence package must include project-specific Indigenous data governance artifacts (e.g., Ownership, Control, Access, and Possession (OCAP®)-aligned stewardship plan where relevant, community-specific protocols, approvals/decision records, and data sharing/access/retention terms). Indigenous data governance requirements are community-specific and must be confirmed on a project-by-project basis.
- **Partner profile:** domestic SME, defence prime, government department / agency, government-affiliated or defence-ministry–anchored research centre, or foreign partner (and whether the partner imposes specific security clauses).
- **Facility posture:** whether the work requires **segregated environments** (physical and/or digital) beyond standard campus controls.
- **Engagement model:** single competitive project, industry-sponsored collaboration, multi-institution network, or defence-funded centre / defence-affiliated research structure (as applicable).

Where a requirement is not applicable based on the Scope Profile, the Facility must provide a brief **"not applicable" rationale** as part of the evidence package for the DURA level claim.

3.3. Assessment Principles

The DURA methodology is designed to align with Canadian safeguarding-research principles commonly used by research-intensive U15 universities (e.g., transparency, predictability, engagement and inclusivity, and shared responsibility), while remaining proportional to the Facility's Scope Profile.

The DURA framework is guided by the following principles to ensure consistent and proportionate application across participating research facilities:

- **Proportionality:** requirements are applied according to the Facility's Scope Profile and associated risk context.
- **Evidence-Based Assessment:** advancement requires documentary or procedural evidence demonstrating that governance mechanisms are implemented.
- **Clear Stage Gates:** each readiness level contains mandatory capabilities that must be satisfied before progression.
- **Governance Focus:** the assessment evaluates governance readiness, not research quality, technical capability, or personnel competence.
- **Continuous Improvement:** higher readiness levels require monitoring and periodic review to sustain governance practices.
- **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 designed to be applied in a lightweight, repeatable way within HEIs. To do so, it relies on three complementary roles: an institutional executive sponsor, an institutional research security function (where present), and a Facility-level lead responsible for day-to-day execution. Titles vary across HEIs; the responsibilities below define the roles for DURA purposes.

- **Executive Sponsor** (e.g., VP/AVP Research or equivalent). The Executive Sponsor is the accountable institutional leader for dual-use readiness governance. This role provides decision authority, resolves escalations, and ensures the Facility-level lead can engage institutional functions (e.g., research office, legal, IT, risk, Indigenous engagement) when required by a project's Scope Profile. The Executive Sponsor approves the establishment of dual-use readiness practices at the institutional level, supports resourcing expectations, and is the senior point of accountability when a proposed collaboration introduces elevated risk.
- **Research Security Officer (RSO)** / Research Security Office (institutional function). The RSO is the institutional function that supports consistent research security practices across the HEI. Where present, the RSO provides guidance on research security policy, partner due diligence practices, incident reporting and escalation pathways, and alignment with applicable federal guidance (e.g., STRAC-related expectations where relevant) and institutional governance requirements. The RSO may advise Facilities on appropriate controls based on the Scope Profile, coordinate training and awareness, and provide a point of liaison with institutional units responsible for cybersecurity, legal/contracting, privacy, and ethics. The RSO does not certify Facility readiness; it supports governance and consistency.
- **Research Centre Security Lead (RCSL).** The RCSL is the Facility-designated lead responsible for coordinating DURA activities within a lab, institute, centre, or facility. The RCSL maintains the Facility's baseline Scope Profile, coordinates completion of DURA checklists for upgrades, and ensures that required internal artifacts exist and are current (e.g., policies, plans, training records, governance approvals). The RCSL also coordinates Facility-level stakeholders (PI(s), lab management, IT support, data stewards) and escalates issues to the RSO and Executive Sponsor when a project requires additional institutional decisions or resources. For DURA purposes, "RCSL" is a role definition; the individual may hold another formal title at the HEI (e.g., lab manager, operations director, centre administrator).

Note on OCIP: DURA levels recorded in OCIP are self-attested by Facilities. OCIP logs checklist selections and level changes (user ID and timestamp) and notifies the OCIP Manager, the HEI RSO, and the Facility RCSL. OCIP does not validate, certify, examine, or review Facility claims.

3.5. Assessment Process

The assessment methodology is intentionally simple and avoids scoring or weighting; it focuses on documentary evidence required at each level.

Evidence artifacts are checked internally by the Facility Research Centre Security Lead (RCSL or designate) to confirm presence, completeness, recency, and internal consistency.

Project-specific note (Ontario RS): Ontario Ministry research-security requirements are assessed on a per-project basis as part of a funding process. In DURA, these requirements are treated as a Scope Profile trigger: Facilities are not expected to maintain Ontario RS forms as standing lab artifacts unless they anticipate Ontario Ministry funding, in which case the Facility should demonstrate an internal process to collect, retain, and escalate the required project-level attestations and mitigation artifacts.

To sustain the assessment effort over time for Facilities at levels 5 and 6, the RCSL is responsible for coordinating periodic check-ins with relevant stakeholders (e.g., leadership, IT, research office, lab management) and tracking completion of required artifacts.

Scope change rule: When the Scope Profile changes in a way that makes additional requirements applicable, the Facility RCSL must re-check level gates impacted by the newly applicable requirements before claiming or retaining the higher level for that collaboration, and record the effective date/version of the updated Scope Profile.

3.6. Evidence Handling Guide (Facility Internal)

This section describes internal Facility handling of evidence; OCIP does not validate or review evidence.

The appointed Research Centre Security Lead (RCSL) will determine whether —with the mandatory capabilities checklist as a guide— a level's gate has been passed to enter the next level, ensuring that all research centre departments have executed their own self-assessment.

- **Levels 2–3:** self-attestation supported by basic evidence upload (minimum viable artifacts).
- **Level 4:** structured internal review (RCSL plus relevant institutional functions, e.g., IT and research office) supported by an evidence register and documented review notes.
- **Levels 5–6:** independent third-party validation is **optional and scope-dependent** (encouraged where required by partner contracts, regulated data/technology, or higher-risk Scope Profiles). Independent validation may include institutional audit functions, external consultants, or certification programs required by partner contracts.

To avoid "self-grading" bias through the self-assessment process, the appointed Research Centre Security Lead (RCSL) should be an individual with knowledge of and experience with research centre requirements.

3.7. Terminology & Definitions

A common language is required to ensure a common understanding by research centres, industry, and the Defence establishment. To this end, we have compiled a *Glossary of Terms*, which is attached to this document and is also incorporated in eCO's *Dual-Use Landing Page* (https://aka.pe/eCO/dur/).

DURA Readiness Model

4.1. Readiness Scale Overview

The DURA readiness scale comprises seven levels **(Levels 0 through 6)** that represent increasing governance maturity.

The scale maps the progression from initial dual-use awareness to the comprehensive implementation of federal requirements and Canadian policy context and applicable institutional governance practices. It covers four key **functional pillars**: governance, personnel, infrastructure, and output control. These pillars are described in detail in sections 4.4 and 5 below.

The model also emphasizes the need for **continuous monitoring** and **continuous improvement** as operational best practices. At higher readiness levels, these mechanisms should be **institutionalized** (i.e., embedded in routine operations, reviewed periodically, and improved based on lessons learned) to sustain research security governance over time.

The readiness scale is summarized in section 4.2; interpretation rules and canonical references are provided in section 4.3.

4.2. Readiness Scale Table

Level	Status	Objective
0	**Opted out**	Explicit decision to exclude DUR from the Facility's mandate.
1	**Neutral**	No current interest or formal consideration of DUR.
2	**Interested**	Identification of dual-use potential in existing research.
3	**Developing**	Building internal security policies and infrastructure.
4	**Validating**	Evidence-supported readiness: controls and governance are documented and reviewable for completeness and consistency.
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).
6	**Engaged**	Governance system institutionalized and demonstrated through sustained, compliant execution of multiple dual-use collaborations, with measurable continuous improvement.

4.3. Level Definitions

The DURA maturity scale is defined as seven states (Levels 0, 1, 2, 3, 4, 5, and 6). Level objectives and readiness expectations are summarized in the Readiness Scale Table above (Section 4.2).

Canonical level definitions (status, objective, actions, and authoritative references) are maintained in the companion document, *DURA Maturity Scale Framework*.

This Methodology document defines how the levels are applied:

- **Scope Profile first:** Before claiming a DURA level, the Facility defines a Scope Profile, as described in section 3.2.1. The Scope Profile determines which requirements are applicable versus not applicable.
- **Governance sponsor:** At Levels 3 and above, Facilities must assign a named institutional Executive Sponsor (e.g., VP/AVP Research or equivalent) to provide escalation authority and ensure the RCSL can engage institutional functions (IT, legal, research office) when Scope Profiles trigger elevated requirements.
- **Mandatory vs Conditional vs Desirable:** "Mandatory" items define the gate to claim a level; "Conditional" items are dependent on the applicable Scope Profile; "Desirable" items reflect higher maturity within a level but do not increase the level.
- **No partial credit for gates:** Advancement requires 100% completion of mandatory items that are applicable to the Scope Profile. If an item is not applicable, the Facility must provide a brief "not applicable" rationale as part of the evidence package.
- **Evidence model:** "Validation" refers to administrative review for evidence presence, completeness, recency, and internal consistency—not certification or technical compliance assurance.

For operational interpretation by capability area (Governance, Personnel, Infrastructure, Output Control), see the Functional Assessment Pillars section that follows.

4.4. Functional Assessment Pillars

The DURA framework evaluates governance readiness across four functional assessment pillars. These pillars represent the primary institutional capability areas required to manage dual-use research risks in a structured and sustainable manner.

Governance: Institutional policies, oversight structures, and decision-making processes that define how dual-use research risks are identified, managed, and monitored.

Personnel: Human-resource practices related to awareness, training, access control, and role-based responsibilities for individuals participating in dual-use research activities.

Infrastructure: Physical and digital environments used to store, process, and transmit research data and technology, including cybersecurity and facility-level safeguards appropriate to the Scope Profile.

Output Control: Mechanisms governing the dissemination, transfer, and protection of research outputs, including publications, intellectual property, datasets, and collaboration artifacts.

5. Illustrative Interpretation of Functional Pillars

The following table provides a high-level interpretation of how the functional assessment pillars typically evolve across the DURA readiness levels **above Level 1 Neutral**. The authoritative definitions of level requirements, actions, and references are maintained in the companion document *DURA Maturity Scale (Framework)*.

Functional Capability	Level 2: Interested	Level 3: Developing	Level 4: Validating	Level 5: Ready	Level 6: Engaged
Governance	Formal identification of dual-use potential in existing research.	Appointment of a Research Centre Security Lead (RCSL) and a named institutional Executive Sponsor (e.g., VP/AVP Research or equivalent) to provide decision authority and escalation support for dual-use readiness governance	If applicable (controlled goods/ technology involved): CGP registration initiated/ completed or documented "not applicable" rationale based on Scope Profile; governance evidence package reviewed for completeness and internal consistency (not certification).	Institutional contracting authority and process to execute agreements with required research security / data handling clauses is active (as indicated by Scope Profile and partner requirements).	Established continuous monitoring and continuous improvement loop for security risks and governance controls.

Functional Capability	Level 2: Interested	Level 3: Developing	Level 4: Validating	Level 5: Ready	Level 6: Engaged
Personnel	Baseline awareness of research sensitivities among PIs.	Determine STRAC relevance and identify in-scope activities (where applicable per Scope Profile); define role-based training and onboarding requirements for personnel supporting dual-use projects.	For STRAC-in-scope work: required attestations completed and a documented review / escalation / record-retention process exists for affiliations-of-concern risks (DURA/OCIP do not conduct intelligence vetting).	Access restricted via need-to-know zones and access controls appropriate to the Scope Profile (physical and/or digital).	Sustained, measurable capability: training refresh cycles, staffing controls, and lessons-learned incorporated into practice; optional / scope-dependent advanced profile: participation in NATO-/DIANA-adjacent ecosystems where relevant.
Infrastructure	Use of standard campus Wi-Fi and shared server space.	Initial cybersecurity hardening beyond standard Wi-Fi (e.g., VLAN isolation). The Facility also maintains a current asset map of relevant scientific infrastructure and enabling environments (where applicable) to support partner conversations and Scope Profile decisions.	Documented cybersecurity risk management aligned to ITSG-33 (TRA, control selection, remediation plan/ POA&M), or evidence of progression on an accepted certification pathway (e.g., CPCSC) where applicable per Scope Profile.	Segregated secure data processing environment consistent with documented Scope Profile and risk posture.	Infrastructure governance institutionalized and demonstrable over time (monitoring, reviews/audits as appropriate, continuous improvement), supporting elevated partner and data-handling requirements as indicated by Scope Profile.

Functional Capability	Level 2: Interested	Level 3: Developing	Level 4: Validating	Level 5: Ready	Level 6: Engaged
Output Control	Informal review of publications for potential dual-use misuse.	Drafting of a Technology Control Plan (TCP) to govern data and IP.	Completion of "Safeguarding Science" modules (or equivalent) for dissemination and collaboration risks, aligned to Scope Profile.	Capability to handle and protect protected/ controlled/ regulatory/ export-controlled data and outputs as applicable; Classified or NATO handling only where explicitly required by partner requirements and Scope Profile.	Lab serves as a regional hub or mentor for lower-level labs (capability-building, templates, coaching) and demonstrates continuous improvement in output controls.

6. Detailed Readiness Criteria

6.1. Mandatory Capabilities

For each level, **Mandatories** define the "Gate" to enter the level.

These capabilities take the form of completed documents, forms, records, attestations, and other evidence artifacts that are reviewed by the **Research Centre Security Lead** (RCSL) (or designate) for presence, completeness, recency, and internal consistency.

6.2. Desirable Capabilities

Desirables, prefixed by a letter "o", represent "distinction" or higher maturity within that level.

Desirable capabilities are included to encourage early participation and continuous improvement without creating an undue barrier to entry. Over time, some practices currently treated as 'desirable' may become standard expectations due to changes in partner requirements, institutional policy, or legislation. Where such changes occur, Facilities will be notified and the framework will be updated accordingly.

6.3. Reference Inventory

The canonical inventory of external programs, standards, guidance documents, and links referenced by DURA is maintained in the "Glossary & Links" artifact and is also available in the DURA landing page at https://aka.pe/eCO/dur/

7. Key Considerations

7.1. Institutional data protocols vs Indigenous Data Sovereignty

One of DURA's key mandates is to consider, early in the DURA research security assessment, the Ownership, Control, Access, and Possession (OCAP®) principles and other applicable Indigenous data governance requirements in relation to the Facility's institutional data governance and handling practices (collection, storage, access, sharing, retention, and disposal). The OCAP® Principles are

designed to protect Indigenous Data Sovereignty by ensuring community rights to self-determination over their data, and by establishing governance expectations for how data is managed and shared. Indigenous data sovereignty (e.g., OCAP® principles) is not a "desirable" element; it must be embedded within the Governance and Output Control pillars when triggered by the Scope Profile (e.g., Indigenous partner/community involvement, Indigenous data, or Indigenous-led research contexts).

Where applicable, Level 4 validation includes confirmation that the Facility has documented alignment to applicable Indigenous governance frameworks (e.g., OCAP® where relevant), evidenced by appropriate governance approvals and project-specific artifacts such as a data governance / stewardship plan, data sharing or research agreements (where applicable), defined access controls, and documented retention/disposal expectations. This review assesses evidence presence, completeness, recency, and internal consistency and does not constitute certification or compliance assurance by eCO/OCIP.

Note: First Nations, Inuit, and Métis communities may have distinct data governance protocols; engagement and requirements must be confirmed on a community-by-community basis.

7.2. The "Cliff" at Level 4

Because Level 4 introduces evidence-gated controls, Facilities should already have an Executive Sponsor in place starting at Level 3 (Developing). The transition from Level 3 to Level 4 must be supported by the Executive Sponsor (e.g., VP/AVP Research or equivalent) —who provides a written charter for the RCSL (scope, decision rights, escalation path, and resourcing expectations)— as well as institutional Research Security Offices (RSOs) to not only report and manage security breaches, but to also prevent "compliance fatigue" over time. Their role is also that of unofficial "change agents" to continuously support ongoing facility efforts for DUR security maturity level acquisition and maturity status and best practice (and later protocol) maintenance.

7.3. Self-Attestation in OCIP (No Review / No Verification)

Self-attestation only. DURA requirements and levels recorded in OCIP are self-declared by the Facility. eCampusOntario and OCIP do not validate, certify, examine, verify, audit, or review any Facility's selections, evidence, controls, policies, or practices.

Upgrade workflow (OCIP platform behaviour). To request a DURA level upgrade, the Facility RCSL logs in to OCIP and checkmarks all applicable Mandatory requirements (and any Optional requirements) for the target level. Each checkmark is recorded with user ID and timestamp, and an optional evidence document. Upon submission, OCIP updates the Facility's DURA level as a self-attested value, logs the change, and sends an automated email notification to the OCIP Manager, HEI Facility Manager, HEI RSO and HEI Executive Sponsor. No OCIP review, approval, or evidence checking is performed as part of the upgrade.

Program monitoring only. OCIP notifications support program monitoring and outreach; they do not imply endorsement of the Facility's self-attested readiness level.

7.4. Alignment with Allies

For Scope Profiles involving allied defence partners or NATO-linked requirements, Level 5 expectations should reference applicable allied requirements where explicitly required by contract/partner.

8. Post-Assessment Governance

8.1. Gap Analysis & Remediation Roadmap

The gap analysis and remediation roadmap helps Facilities prioritize actions needed to reach their target level and maintain it over time.

8.2. Continuous Monitoring & Re-Assessment Cycle

Advancing from Level 5 to Level 6 typically requires institutionalizing monitoring and continuous improvement rather than adding a single new control. Facilities should implement routine reviews, refresh training, and track remediation actions so that governance practices become part of normal operations rather than periodic compliance exercises.

The continuous **monitoring and re-assessment** activities will be repeated on an annual basis. To ensure the research centres maintain their monitoring and assessment efforts, the self-assessment process will be repeated once every twelve months, with evidence refreshed according to applicable recency requirements.