A Modular Approach to Research Security

2025 WE/MW Section Meeting Session T105, 27 March 2025, 9:00-10:00 AM
Jacqueline Littlewood, Director, Research Security, University of Alberta, Canada

Research Security

What is research security?

- Research security refers to the efforts to safeguard research and researchers against activities which exploit research partnerships to access research information, research knowledge, and the resulting intellectual property and technology to facilitate unwanted knowledge transfer. These activities endanger national security, critical infrastructure, and the integrity of the research ecosystem. Examples of research security transgressions include foreign interference, espionage, and unwanted knowledge transfer or theft.

Why is safeguarding research important?

- To protect research investments (time, funding, expertise) against threat actors seeking to acquire and exploit knowledge and data for their own advantage. Safeguarding your research means you retain control over when, where, and how your research is shared, published, and applied, while also contributing to national security.

Challenges to Research Security Implementation

- Limited resources
- Rapidly evolving context and requirements
- Research administrators not security experts
- Institutions vary in size, structure, focus, research priorities, partnerships
- Different risk tolerances and each institution
- Varying research infrastructure
- Decentralized nature of postsecondary institutions

Ultimate Objectives

- Mitigation of risk and safeguarding of research, researchers, innovation
- Adherence to applicable requirements
- Culture of research security
- Individual and institutional competence
- Research security integrated to institutional processes, procedures, and supported by systems and technology
- Adaptation to evolving context – approaches which are flexible
- Continuous reinforcement learning and monitoring
- Enhanced collective resilience while preserving core academic values

Scene-Setting – Canadian Context

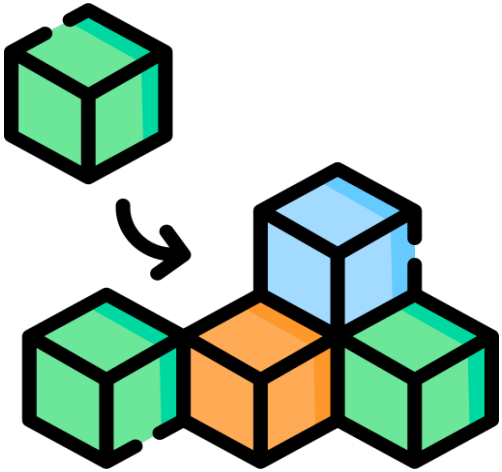
- Research security policy requirements introduced in 2021 and 2024
- Government of Canada funding for universities to implement – proportionate to research funding
- Strong communities of practice regionally and federally
  - Supporting capacity-building
  - Fostering of research security competency
  - Information exchange
- The Canadian context has demonstrated effectivity of a modular approach where institutions can adapt and build on elements that fit their size, context, and maturity level
- A modular approach allows for institutional autonomy and lends itself to capacity-building through communities of practice

Why A Modular Approach?

Rationale for a Modular Approach

- Right-sized
- Builds on results
- Leverages synergies and interconnections
- Solid foundation
- Risk-based
- Adaptable, flexible, transferrable
- Responsive to change in rapidly evolving context (geopolitical, technological, regulatory)
- Supports performance assessment, informed decision-making and ongoing improvement
- Applicable in any institution or jurisdiction - conducive to community of practice support

What Is the Modular Approach?



Modules

Module 1 – Awareness

Module 2 – Training and Competency Building

Module 3 – Governance Framework

Module 4 – Risk Assessment

Module 5 – Advisory

Module 6 – Reinforcement

Module 7 – Monitoring and Compliance

Module 1 - Awareness

- Institutional awareness of requirements
- Awareness-raising activities
- Website
- Webinars
- Targeted/Emails
- Events/Engagements
- Promotional materials
- Committee briefings
- Newsletters
- Podcast
- Promoters/allies

Module 2 – Training and Competency Building

- Establish training needs and topics; role-dependent
- Threats, due diligence, mitigations, requirements
- Review available training
- In-house, Regional, Government-offered or mandated, International
- Develop new training as required
- Segmentation/tailoring options
- Publicly available resources
- Variety of training modalities
- Explore opportunities to integrate into existing courses
- Track completion and emphasize benefits to enhance uptake

Module 3 – Governance Framework

Framework required to:

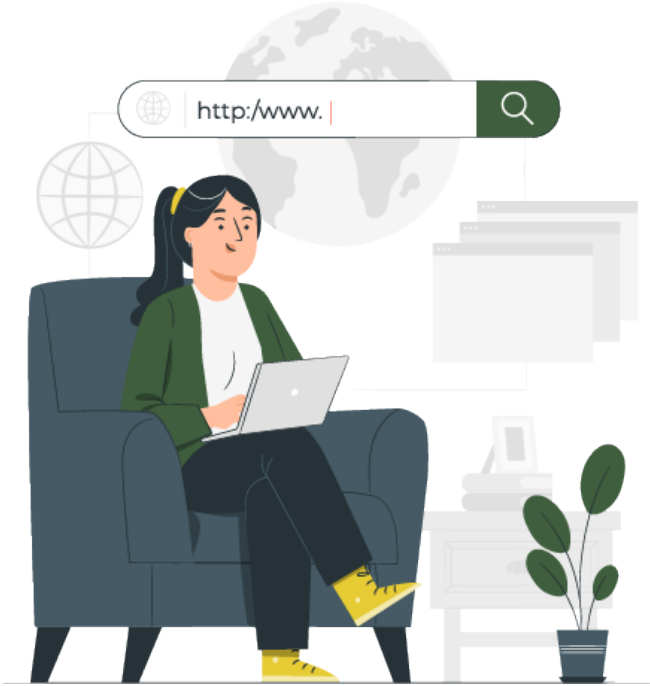
- Assign roles and responsibilities
- Identify decision making authorities
- Support allocation of resources
- Identify interest holders, collaborators, intersections

May comprise:

- Policies, procedures, processes
- Provision of guidance and direction
- Governance committees
- Size, scope and scale depends on context

Module 4 – Risk Assessment

- Risk assessment at the institutional and project level
- Informs prioritization and planning
- Risk assessment tools
- Commercial services vs. in-house
- Tools, methodologies, documentation and delivery of results
- Inventory mitigation measures available



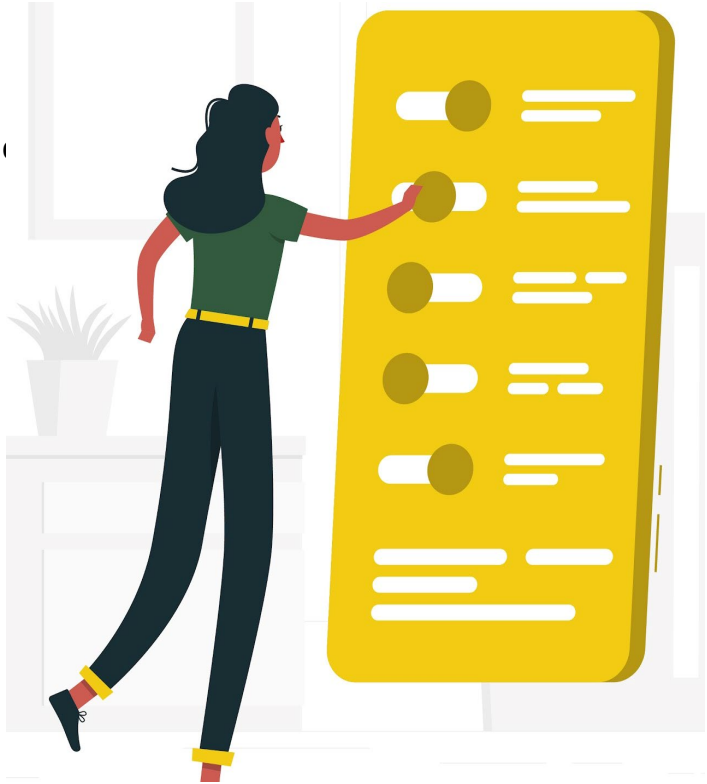
Module 5 - Advisory

Identifying advisory options available

- Institutionally?
- Government?
- Community of Practice?

On campus advisory

- Who?
- How?
- Services available?



Module 6 - Reinforcement

Reinforcement of:

- Progress
- Learning
- Culture change
- Security posture

Module 7 - Monitoring & Compliance

Tracking progress, maturity, adoption

- Feedback loop - continuous improvement
- Touchpoints – opportunities for integration
- Tracking options – case management systems, dashboards,
- Tracking challenges – decentralization, survey fatigue, culture

Compliance with relevant requirements

- Framing (implementation support vs. compliance)
- Risk tolerance

Questions and Discussion

Thank You!

Jacqueline Littlewood, Director, Research Security
University of Alberta, Canada
j.littlewood@ualberta.ca