Selling the Risks: Lessons on Security Modernization from Canada's Contract Security Program

Oliver Jones, Karena Kyne, Alexandre Picard

JUNE 2026

HARVARD Kennedy School
BELFER CENTER
for Science and International Affairs

The challenge of security modernization

Modernization, a watchword in governance and public administration, is an imperative for security organizations that need to adapt their outlooks and processes to an increasingly unsettled world. Yet rigid processes obstruct modernization. Agencies face a dual challenge: They need to adapt to a complex threat environment while constrained by legacy systems and reactive approaches to risk (Lloyd 2024). Security organizations that can capitalize on unusual, high-value cases and new forms of social knowledge will be better positioned to anticipate risks in a world defined by accelerating change and uncertainty.

In late 2023, the Government of Canada's Contract Security Program (CSP) partnered with the Archipelago of Design to run a design-led modernization initiative with CSP staff. Using the Three Horizons foresight framework, participants identified systemic barriers to modernization and generated practical pathways to increase buy-in on modernization initiatives. Their work illuminates key lessons relevant not only for CSP but for all security agencies grappling with modernization.

The most salient insights from these workshops centered on the need for organizations to learn to embrace calculated, appropriate risk-taking and enhance their tolerance for failure as a necessary feature of organizational learning and innovation. The workshops identified three key themes for enabling modernization:

Redefining Risk: Risk cannot be eliminated. It must be managed as a constant. Having a sense that failure is an inevitable outcome for some processes generates a psychological safe space from which to test new approaches.

Reframing Identity: Where possible, agencies should focus on high-value, complex cases where their expertise is indispensable (e.g., emerging industries, sensitive domains, cases that require subject matter expertise and unconventional capabilities), while delegating low-value, routine tasks that create organizational drag and inertia.

Formalizing Agility: Improvisational problem-solving should be recognized as a core organizational competency and formalized into existing processes, not treated as a workaround. This improvisational agility can be sold as a feature, not a bug.

All three themes require people leading organizational modernization to *sell the changes*: Transformation depends on stakeholder buy-in and agencies must develop narratives that make modernization compelling for internal and external partners. Likewise, policymakers should cultivate risk-tolerant cultures and support organizational redesign that capitalizes on agility to accelerate modernization.

Defining a vision for modernization

The workshops followed a "Three Horizons" approach (Sharpe 2013). The Three Horizons approach helps organizations examine their present state, imagine alternative futures, and chart pathways for change. Following this approach, the workshop facilitators asked participants to develop a set of comprehensive perspectives on CSP's current operations, envision possible and desired futures for the organization, and identify potential pathways to realize these future aspirations. The value of this workshop approach is that it uses a staff-driven process to develop a future-oriented outlook on modernization that is adaptable to complexity.

- **Horizon 1 – Current Operations:** Participants began by mapping CSP's existing structures, processes, and limitations. This grounded the discussion in the agency's immediate realities.
- **Horizon 2 – Transition:** They then explored possible futures, identifying systemic barriers and refining ideas for bridging the agency's modernization efforts from the present into the future.
- **Horizon 3 – Desired Futures:** Finally, participants defined CSP's aspirational future, envisioning what the agency could look like if fully modernized.

Working to define modernization along these three timescales, participants generated three core mechanisms of change (*redefining*, *reframing*, and *redesigning*) that can mobilize CSP staff and stakeholders. Understanding these mechanisms of change and seeing how a new set of structures can reshape the system also has the positive effect of motivating those involved and increasing buy-in.

A key aim of the workshops was to develop a set of tasks that can be carried out independently after the facilitator leaves the building, using in-house capabilities to drive the necessary changes. Using this approach, the workshop created practical knowledge for CSP staff that could apply to other agencies that need to address complex security challenges. This provisional set of practical ideas provides a set of concepts that can be expanded as CSP develops new insights in the modernization challenge. In this sense, these themes are iterative. They are not a one-size-fits-all approach to modernization. They make the case for a robust, iterative process for validating the knowledge and experience of staff as the drivers of modernization in CSP and other security agencies. This ensures that CSP and agencies like it can modernize using their own staff and resources, without reliance on outside experts.

Case study: solving wicked problems

The Contract Security Program is the Government of Canada's national authority and lead agency for industrial security. It plays a central role in contract verification and risk management for Public Services and Procurement Canada (PSPC). CSP's processes were originally conceived to settle high volumes of simple cases, like ensuring security of protected and classified information, and vetting access to work sites. However, in a competitive, multipolar world, it is increasingly more strategic for CSP to focus on high-level, classified, complex cases that reflect shifting landscapes in geopolitics and national security.

CSP's modernization challenge is arguably a "wicked problem" (Ackoff 1974; Rittel and Webber 1973). Wicked problems defy tidy solutions and necessitate trade-offs. While there is a strong pressure for CSP to modernize its processes so it can be more effective and efficient in assessing risks to industrial security, modernization itself is received as an unstructured problem without a clear definition. At the same time, any action to fix CSP's processes risks creating second- and third-order consequences. The agency must satisfy multiple, sometimes competing stakeholders: government departments, industry, international partners, and security officials. The organization has limited options for trial and error, and the issues they are attempting to fix are often symptoms of other, larger problems. This makes it difficult for the agency to fulfill its existing mandate while adapting to new challenges. Workshop participants captured this dilemma in their initial problem statement: *How do we maintain our security focus while also catering to contract systems' and prosperity systems' needs*?

For example, CSP's close coupling with procurement processes and the timeline pressures involved constrains CSP's ability to make autonomous decisions that would empower them to capitalize on their mandate. This lack of autonomy is compounded by mismatched policy, immobile bureaucratic processes, and constraints on

funding and resources. CSP's comprehensive mandate for securing protected information requires the agency to over-mitigate risk. This includes cases where the potential for injury to national security is minimal. Many of the Government of Canada's requirements for securing protected information exceed those of Canada's partners and allies, including most Five Eyes and NATO countries (Lloyd 2024). Prioritizing these kinds of tasks creates significant drag on agency resources and slows down the evaluation of more high-value cases. The large-scale vetting of low-risk cases fails to deliver value for the intensive investment of CSP resources. The workshop participants felt that the volume of these low-risk and low-impact routine tasks undersells the agency's unique skillset in managing complex cases, which creates significant opportunity costs for Canadian industry and procurement goals. Moreover, complex cases need to be treated by a specialized team, because complex cases challenge the idea that everything must be interoperable, linear and easy to represent.

To capitalize on its unique capabilities, CSP needs a coordinated approach between stakeholders that grants its staff agency to drive significant changes in the way CSP conducts its business. This means that change in CSP's organizational context is more complex than simply identifying what needs changing (see Lloyd, 2024, for recommendations on how CSP can retool handling of protected and classified information). The challenge for modernizing CSP lies in how to implement change in a way that satisfies internal and external stakeholders, and refrains from destroying that which already works.

The workshop tasked CSP staff with describing an actionable vision of modernization that can mobilize these stakeholders. The participants framed their aspiration for modernizing CSP in this language: "Canada's security and economic prosperity are strengthened by a unified security service agency that can anticipate and respond to the evolving threat landscape." Aspirationally, this would "inspire confidence in Canada's security services at home and abroad." Their key themes emphasized a need to *unify* staff and partners, *anticipate* and *respond* to evolving threats, and *inspire* confidence in Canada's industrial security processes. This language can be posed as a series of questions about CSP that would suggest starting points for implementing their ideas:

1. How does CSP unify on an idea?
2. How does CSP anticipate a future and work toward it?
3. How does CSP create an agile environment that can quickly respond to threats?
4. How can the competence of CSP skills be "sold" in such a way to inspire confidence and articulate skills?

To the last question, highlighting narratives that can impress CSP's adaptive skills is a key means of achieving their aspirations for modernizing the agency.

An illustrative case makes CSP's challenges and unique skills clear. Imagine a CSP team assessing the risk of an important contract in a village in North Africa. The team works in a high-trust culture where norms, laws, and hierarchies of information provide a foundation for verifying the essentials of risk management. PSPC requires out-of-country verifications to confirm the identity of the engaged parties and the key sites involved. However, the agency's process is mismatched with the institutional norms of North African culture. Their own institutional process was conceived as a one-size-fits-all template to assess the trustworthiness of vendors and applicants in a Canadian context. The team is now working to impose their institutional norms on a culture where very different norms apply. The team recognizes that in a rural village in North Africa, trust is granted on an interpersonal basis. Standard means for verifying identity like birth certificates may be impossible to acquire, and most social knowledge isn't set by state institutions.

The team finds workarounds. They organize person-to-person interactions with locals who can verify key details, an improvised approach using nonstandard methods for documenting the social knowledge of this rural village's informal social traditions. This approach does not eliminate risk entirely. But these informal workarounds provide the team with a set of reasonable verifications that settle the key questions surrounding the identity of its overseas partners, which enables them to provide the necessary security assurances to settle the contract and do the deal.

The team has improvised an approach for reconciling different cultural approaches to validating information and establishing trust. They've found a way to settle the risks in an organizational culture with vastly different structures for authorizing knowledge and validating truth. But the agency suppresses this episode, compartmentalizing it as a special case. There is little acknowledgement of the ingenious workaround. The episode is forgotten by all but those who were directly involved, and institutional memory of it is suppressed. By excluding the contextual details that make the case hold together, they undersell the value and significance of their skill sets to a world of risk assessment defined by uncertainty.

This case illustrates the gap between CSP's rigid institutional processes and the adaptive skills of its staff. These are skills that modernization should elevate, not suppress. They offer a model for agile risk verification that should be a critical enabler of CSP's modernization. It's this unique skill set that CSP should highlight to sell its capabilities and drive its modernization.

Lessons for Security Modernization

We can point to four key takeaways from the workshop, which we can generalize to other security leaders modernizing their organizations:

1. Redefine Risk

Redefining risk is critical because contending with risk is integral to the agency's function. In that sense, it is not helpful to conceptualize risk as something that can be neatly avoided. Risk is inevitable. It must be managed, not eliminated. Organizations like CSP should learn to embrace appropriate risk-taking and enhance their tolerance for failure as a necessary feature of organizational learning.

This is a shift from resilience to antifragility. Where resilience assumes an organization can build structures that mitigate risk and prevent damage from shocks, antifragility treats risk and failure as critical enablers of organizational improvement. To capitalize on this redefined concept of risk, agencies need to create psychological safety around failure. This would encourage trial-and-error experimentation to enable learning and innovation that enhance risk assessment and management.

2. Reframe Identity

Reframing the agency's identity would highlight its value as a key enabler of industrial and national security. This would allow CSP to align its mandate with a focus on complex cases that require subject matter expertise and unconventional capabilities.

Where CSP's processes were originally conceived to settle high volumes of simple cases, it is increasingly more strategic for CSP to focus on high-level, classified, complex cases that reflect the shifting landscapes in geopolitics and national security. Agencies should shed or automate routine work so that expert capacity is reserved for cases where they can make a significant impact.

3. Formalize Agility

CSP's high-value risk assessment capabilities should be recognized, codified, and institutionalized. The nuanced workarounds carried out by the team in the North Africa case capture a unique and sophisticated skill set representative of the competencies of CSP staff. When these details are passed over, the value of staff's adaptive skills is diminished.

Staff's ability to assess complex risk in conditions of ambiguity should be a critical enabler of CSP's modernization initiatives. CSP can formalize these processes and reprioritize them as critical enablers of the agency's core mandate. At the same time, CSP needs to reposition the organization to play to this strength, which should be sold as a feature, rather than marginalized as a bug.

4. Sell the Change

Efforts to change the organization aren't likely to move forward without stakeholder buy-in. The purpose of these initiatives is to identify priorities for change in a way that heightens stakeholders' awareness of their value to the organization. Narratives of successful change and modernization allow them to sell the organization's capabilities in terms that resonate with broader government mandates.

CSP has developed an infrastructure of valuable workarounds and improvised solutions in its day-to-day operations, but these skills have not been granted the visibility that would help sell the organization's skill set to partners and clients. This kind of selling is critical for situating the identity of the organization, both internally and externally. As a workshop participant put it in one of several post-workshop interviews conducted by AOD, "Who we think we are informs where we play."

CSP's challenge is to work with outside agencies and partners in a way that maximizes strategic alignment with CSP's team, helps them make independent, deliberate strategic choices, and builds compelling business narratives to drive the resourcing to accelerate modernization. To do this, they need to develop both internal and external narratives that frame change as an enabler of national security.

Mobilizing a vision of change

CSP's example provides some actionable insights that security practitioners can implement in their own organizations.

Building risk-tolerant organizational cultures: Policymakers in security organizations should foster risk management cultures that recognize failure as a part of innovation, rather than as grounds for sanction. This includes granting staff the agency to draw a red line around situations where the truth of a risk assessment cannot be settled with available tools, and treating those judgment calls as expertise, not failure.

Supporting improvisation to institutionalize agility: Adaptive problem-solving is already happening on the ground. Leaders should formalize, as part of their institutional design, critical skills that might otherwise be passed over as banal and grant these workarounds the visibility that clarifies their value to key stakeholders.

Integrating design methods into planning cycles: Governments can incorporate foresight methods, such as Three Horizons, into their planning cycles to surface staff insights, build momentum for change, and ensure modernization efforts remain iterative rather than static. These kinds of approaches can be invaluable for prototyping and implementing novel solutions to complex challenges.

Developing communications that highlight the benefits: Modernization will stall without buy-in. Agencies should invest in communication strategies that frame modernization as enabling national security and economic resilience, and that demonstrate change can be driven by in-house staff without reliance on expensive tools or outside consultants. Narratives aimed at staff, partners, and the public are essential to mobilize support and secure resources.

Conclusion: Staff as enablers of modernization

Modernization is not optional for security agencies. They need to adapt to an increasingly complex threat environment while working around legacy processes and reactive approaches to risk. This is a multifaceted challenge that requires leaders to foster and sustain organizational agility—both internally with staff and existing processes, and with external partners—to drive change.

CSP's case proves that risk-averse agencies can innovate, and that their staff are key enablers of organizational adaptation. CSP's staff identified systemic barriers to modernization and generated practical pathways to increase buy-in. Improvisational problem-solving reinforced by a complex understanding of risk should be recognized as a core organizational competency and built into organizational processes. CSP's experience offers a model for agile risk verification that should be a critical enabler of modernization across security organizations. These are skills that security organizations should elevate and institutionalize.

Authors

Oliver Jones: Oliver Jones is Vice President of Research and Development at Archipelago of Design, where his work focuses on design thinking and foresight practices in security education. As a contractor in the National Security Program at Canadian Forces College, he leads seminars on developing institutional strategy for complex problems with senior defence and security professionals. He has supported defence and security organizations in Canada and across NATO partner contexts through research and design facilitation. He holds a PhD in English from York University in Toronto, with research spanning war studies, systems thinking, and wargame design.

Karena Kyne: Karena Kyne has a background in Philosophy, International Relations, and Politics, and has supported Archipelago of Design in its work. Her academic experience is grounded in real-world security contexts. As an Adjunct Professor with the Joint Special Operations University in Tampa, she has facilitated workshops on context-specific challenges across NATO countries. She has also served as an Assistant Lecturer at universities in the UK and Canada.

Alexandre Picard: Alexandre holds a Bachelor's degree in Literature from the Université du Québec à Montréal, a Master of Business Administration (MBA) from HEC Montréal, and is a graduate of the Canadian Forces College's National Security Program (NSP 15). He joined Public Services and Procurement Canada (PSPC) in 2008, where he has held various leadership roles in corporate labour relations, values and ethics, corporate staffing, and ministerial services.

At PSPC, Alexandre serves in the Contract Security Program (CSP), the national authority for industrial security, which protects the Government of Canada when sharing sensitive and classified information with the private sector by delivering a suite of risk-based security services, including organizational security screening—assessing ownership, control and influence (OCI) and personnel security screening. In his current role, he leads the security screening of private sector entities, leads outreach, training, and client service delivery, and is actively engaged in modernizing the CSP.

References

Ackoff, R. L. *Redesigning the Future: A Systems Approach to Societal Problems*. Wiley-Interscience, 1974.

Lloyd, R. "Canada's 'As Is' Contract Security Program and the Aggregate Risk Profile of the Nation." Canadian Global Affairs Institute, 2024.

Rittel, Horst W. J., and Melvin M. Webber. "Dilemmas in a General Theory of Planning." *Policy Sciences* 4, no. 2 (1973), 155–169.

Sharpe, B. *Three Horizons: The Patterning of Hope.* Triarchy Press, 2013.

"Transforming the CSP Operating Model." PowerPoint slides. Public Services and Procurement Canada, 2023.