



Defence, security and resilience bank

New risk mandate for Canadian banks





Executive summary

The model is familiar. The mission is not.

Canada and eight partner countries announced their shared intention to establish the DSRB in July 2026, following negotiation of founding Articles of Agreement in Montreal. Public statements target operations as early as 2027. ^[1-3] The analysis that follows includes assumptions about the final operating model.

The proposed Defence, Security and Resilience Bank (DSRB) is intended to mobilize public and private capital for defence, security and resilience priorities across member countries. Public announcements describe a Canada-led multilateral institution that would provide long-term, low-cost financing and guarantees, complement existing national and multilateral tools, including alignment with the Multilateral Defence Mechanism (MDM), and help governments and defence-sector firms close financing gaps and expand industrial capacity. ^[4-8]

The risk mandate need not be invented from scratch. Multilateral institutions already use guarantees, risk-sharing, intermediated lending, project finance and trade-finance programmes to mobilize commercial-bank balance sheets. They also bring established approaches to integrity due

diligence, anti-money laundering, anti-terrorist financing and anti-fraud controls and procurement oversight. The novelty is the purpose-built defence mission and the strategic significance of the relationships, transactions and data that may flow through participating banks, ultimately creating a new class of information, valuable to state and non-state hostile actors.

Canadian commercial banks could participate as financing partners, transaction banks, trade and supply-chain banks, capital-markets intermediaries, advisors, financial-crime gatekeepers and custodians of strategically valuable information. The role assumed will determine which counterparties the bank touches, what it processes, what it knows, what it can disrupt and which risks it inherits. The risk perimeter therefore follows money, data and relationships, not merely the legal boundary of a DSRB-guaranteed loan.

The most important new risk is the intelligence value of ordinary banking information. Supplier relationships, beneficial ownership, production capacity, payment timing, trade flows, due-diligence findings, government priorities and technology



dependencies can help an adversary map a defence industrial base, identify pressure points, evade sanctions, recruit insiders, influence decisions or prepare for disruption. Banks may be targeted not only to steal money, but to learn, map, influence, compromise, delay or disrupt.

Traditional risks do not disappear. Fraud, money laundering, terrorist financing, sanctions and export-control evasion, cyber, third-party, insider risk and operational resilience remain core disciplines. What changes is their context, interdependence and potential consequence. A blocked payment, declined application or contained data-access event may not produce a booked loss, but could be a material financial-crime, regulatory, reputational or national-security incident.

The DSRB participation would bring financial institutions into closer contact with defence-related sectors, counterparties, and activities that may sit differently within existing risk appetites. For Canadian institutions, this may also require a deliberate reassessment of where those exposures fit within existing risk appetite and under what conditions they can be accepted. The resulting challenge is therefore to determine how DSRB-linked activities should be risk-assessed, governed and controlled as they become a more deliberate part of the institution's strategic risk posture.

The required response is a mission-specific overlay on existing frameworks, not a parallel compliance universe. Fraud, AML/ATF, sanctions, cyber, security, third party risk, data governance and operational resilience do not need to become one function. They do need one threat picture, a relationship-level view of the economic unit and supply chain, shared escalation triggers, clear decision rights, secure intelligence sharing and joint scenario testing. OSFI, FINTRAC, export-control, Controlled Goods and Cyber Centre frameworks provide much of the foundation; DSRB participation would require those foundations to operate together. ^[9,13,16,19]



Strategic choice, not only a product decision

Boards should define where and how the bank is prepared to participate, including sectors, roles, geographies, counterparties, data exposure and conditions for decline.



Role determines exposure

A lender, transaction bank, advisor and information custodian see different data, create different dependencies and require different controls.



Information becomes a protected asset

What the bank knows may be as important as what it moves. Strategic data requires classification, need-to-know access, monitoring and secure sharing.



Fraud becomes an intelligence signal

A fake supplier, payment diversion or unusual file access may indicate sanctions evasion, terrorist financing (TF), foreign influence, reconnaissance or supply-chain compromise.



Zero-dollar events can be material

Attempted transactions, exposed relationships, operational delay and reputational harm can trigger significant consequences even when no funds are transferred or lost.



Functions must converge

The operating model should connect fraud, AML/ATF, sanctions, cyber, insider, third-party and resilience decisions without forcing an organizational merger.



01 What the DSRB is - and what is genuinely new

A familiar multilateral-finance toolkit applied to a purpose-built defence, security and resilience mission.

A proposed multilateral institution with a defence mission

The DSRB is being designed as an international financial institution for participating allies and partners. The announced objective is to mobilize capital at scale, reduce financing costs and expand industrial capacity across member countries. Public materials describe loans to member countries, guarantees that can increase the availability of affordable private capital, and support for defence, security and resilience initiatives across supply chains. ^[1-4]

The likely ecosystem is broader than prime contractors. It may include defence manufacturers, aerospace and advanced-technology firms, cyber and telecommunications providers, critical-mineral and energy-security projects, transportation and critical infrastructure, dual-use companies, SMEs, subcontractors and technology partners. A Canadian

bank could therefore connect to a cross-border financing and supply-chain network whose commercial activity has geopolitical and national-security significance.

The model is familiar

Existing multilateral institutions demonstrate how public credit support can reach the private economy through commercial banks. For instance, the European Investment Bank (EIB) guarantees can cover a portion of losses and unlock additional lending; EIB intermediated lending is already being used with commercial banks to finance European defence-industry supply chains. IFC and EBRD trade-finance programmes use guarantees, risk sharing, master agreements and partner-bank networks to expand trade capacity.



Canadian regulatory foundation

OSFI Integrity and Security, B-10, B-13 and E-21; FINTRAC AML/ATF and sanctions-evasion reporting; export controls; Controlled Goods; and cyber-resilience guidance already address many component risks. ^[13]

The mission is new

The DSRB is not simply another development-finance channel. It is purpose-built around defence, security and resilience. That changes the strategic value of the underlying activities and information. The same guarantee, loan, payment or due-diligence file can sit within a supply chain involving controlled goods, dual-use technology, sovereign priorities, sensitive production capacity and urgent operational dependencies.

The resulting control question is wider than “Could this cause financial loss, customer harm or a regulatory breach?” A DSRB-informed model must also ask whether an event could expose sensitive supplier relationships, map defence-sector capacity, support terrorist financing or sanctions and export-control evasion, compromise a critical supply chain, influence a decision or create strategic disruption.



Executive takeaway

The DSRB does not require banks to abandon established risk frameworks. It requires them to apply those frameworks through an economic-security and intelligence lens, and to connect controls that are often operated separately.

02 Potential roles for Canadian commercial banks

Participation should be defined by the function performed, the information accessed and the dependency created - not by a single product label.



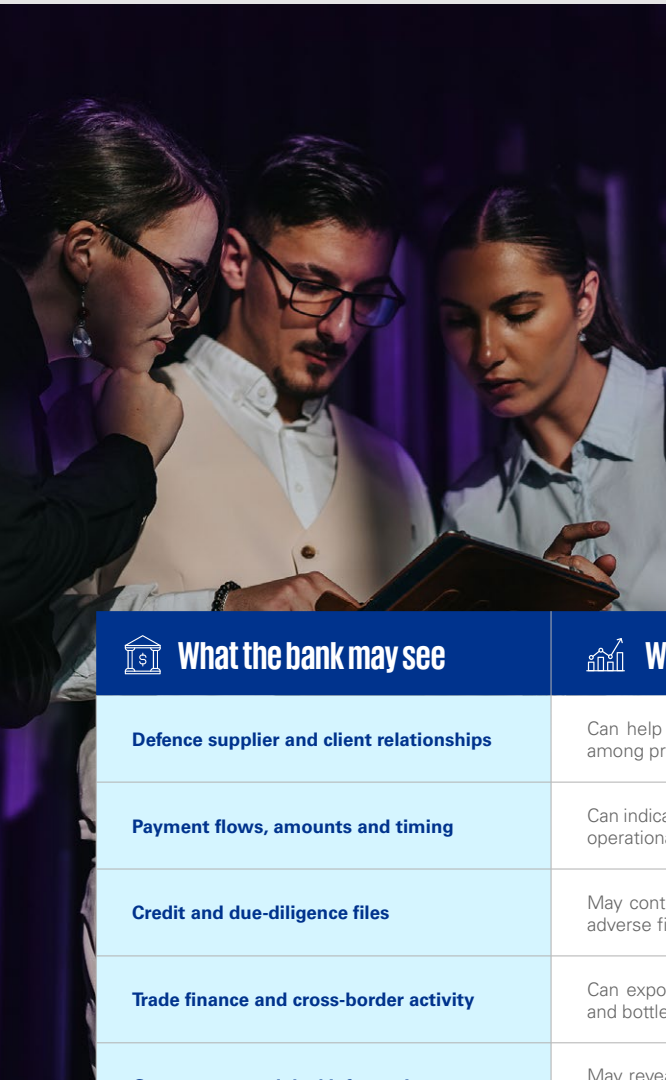
 Potential role	 Illustrative activities	 Distinct risk and control implications
Financing partner	Direct or guaranteed lending, co-financing, syndicated lending, revolving facilities, working capital and project finance.	Credit and eligibility decisions; borrower and sponsor due diligence; covenants; use-of-proceeds and end-use monitoring; portfolio and geopolitical concentration.
Trade and supply-chain bank	Letters of credit, performance and advance-payment guarantees, supply-chain finance, receivables, inventory and equipment finance.	Visibility into goods, routes, invoices, end users and subcontractors; exposure to trade-based crime, export-control evasion, supplier substitution and document fraud.
Transaction bank	Payments, cash management, foreign exchange, treasury, collateral, escrow and agency services.	Processing of high-value and time-sensitive flows; payment diversion, sanctions exposure, operational dependency and insight into procurement timing and production cycles.
Capital-markets intermediary	Bond or loan underwriting, distribution, securitization, private placements, hedging and institutional-investor access.	Disclosure and deal information; investor and syndicate counterparties; market conduct, information barriers, reputational and concentration risk.
Advisor and structurer	Financial advisory, project structuring, M&A, capital planning, valuation and transaction execution support.	Early access to government, ownership, technology, capacity and strategic-decision information; heightened conflict, insider and influence risk.
Financial-crime gatekeeper	KYC/KYB, beneficial ownership, sanctions and adverse-information review, transaction monitoring, fraud controls and suspicious-transaction reporting.	Decisions that may determine who enters the ecosystem, how indirect exposure is identified and whether proxy, sanctioned, TF or foreign-influence indicators are escalated.
Information custodian and resilience node	Custody of due-diligence files, supplier and payment data, contracts, communications, models, access credentials and operational dependencies.	Strategic-data theft, insider recruitment, third-party compromise, AI leakage and disruption of services that defence-sector participants rely on.

Direct and indirect participation both matter

A bank can acquire DSRB-related exposure without being a formal DSRB counterparty. Existing clients may become eligible suppliers; a borrower may acquire a defence or dual-use business; a payment client may begin serving a DSRB-funded programme; a third-party due-diligence provider may handle DSRB-connected files. Exposure mapping should therefore distinguish direct participation from indirect exposure through clients, suppliers, subcontractors, investors, vendors and technology providers.

The practical implication is that role selection should be part of risk appetite. A bank may be comfortable providing payment services but not advisory services; financing mature infrastructure but not emerging dual-use technology; or joining a syndicate only where the DSRB or another institution retains specified eligibility, monitoring and loss-sharing responsibilities. Participation is not binary. It can be calibrated by product, sector, geography, information access and control maturity.

The risk perimeter follows the money, data and relationships - not the legal boundary of the guaranteed loan.



03

The new risk: the intelligence value of banking activity

Banks may be targeted for what they know, what they connect, what they process and what they can disrupt.

Participation in DSRB-linked activity creates a form of strategic-information exposure that is not fully captured by traditional confidentiality, privacy or cyber-loss categories. Data generated in ordinary banking activity can reveal how a defence ecosystem is organized, financed and dependent. Individual data points may appear commercially routine; aggregated across clients, payments, suppliers and time, they can become an intelligence product.

 What the bank may see	 Why it may have intelligence value
Defence supplier and client relationships	Can help map Canada's and allies' industrial base, identify emerging dual-use firms and reveal connections among prime contractors, SMEs and subcontractors.
Payment flows, amounts and timing	Can indicate procurement activity, production cycles, urgent requirements, cash constraints, counterparties and operational dependencies.
Credit and due-diligence files	May contain ownership, management, revenue, capacity, pricing, contracts, suppliers, beneficial owners and adverse findings not available publicly.
Trade finance and cross-border activity	Can expose movement of sensitive goods, services, tooling, components, transshipment routes, end users and bottlenecks.
Government and deal information	May reveal policy priorities, preferred suppliers, financing structures, approvals, project timing and negotiation positions.
People and decision makers	Relationship managers, credit officers, advisors and executives can be targets for social engineering, coercion, foreign influence, insider recruitment or doxing.
Third-party and technology dependencies	Can identify weaker entry points, privileged service accounts, due-diligence providers, cloud platforms, APIs, models and operational single points of failure.

How strategic-information risk manifests

Collection and espionage

Targeted cyber intrusion, credential theft, insider access, third-party compromise or social engineering used to obtain files, communications or metadata.

Mapping and aggregation

Combining ownership, supplier, payment and timing data to identify capacity, dependencies, pressure points and emerging technologies.

Influence and infiltration

Using front companies, opaque investors, recruited insiders or manipulated relationship managers to enter the ecosystem or shape decisions.

Evasion and diversion

Using proxy entities, complex ownership, false end users, transshipment, trade misrepresentation or payment redirection to move value or capability to restricted actors.

Pre-positioning and disruption

Compromising credentials, vendors or processes in advance so an actor can delay disbursement, interrupt production, leak data or create confusion during a crisis.

Narrative and reputational attack

Leaking selected information, doxing executives, amplifying controversy or falsely alleging misconduct to discourage participation or erode trust.

Threat actors will have different motives

Nation-state and state-aligned actors may seek intelligence, strategic advantage or disruption. Sanctioned and restricted entities may seek access, concealment and circumvention. Organized crime can provide enabling services such as synthetic businesses, shell companies, document fraud and money movement. Hacktivists may pursue disruption, leaks and reputational pressure. Human insiders can be recruited, coerced, careless or compromised. Non-human insiders - service accounts, API keys, bots, scripts, models and automated workflows - can hold privileged access without the behavioural controls applied to employees. Canada's Cyber Centre assesses that state and non-state actors are already targeting critical infrastructure and that state adversaries are increasingly bold and disruptive.^[18]



Management implication

Strategic information should be treated as an asset class. Banks should identify DSRB-linked data, assign business ownership, classify it by strategic sensitivity, restrict access by operational need, monitor human and machine identities, control AI use, and define how intelligence can be shared securely across functions and with authorities.



04 When Risks Converge: From Financial-Crime Event to National-Security Signal

The core risks are interdependent. A single event may be simultaneously a fraud case, a sanctions concern, a cyber incident and a national-security signal.

The risk is in the combination

A newly incorporated supplier may be an application-fraud vehicle, a sanctions proxy, a foreign-influence channel or an attempt to gain legitimate-looking access to a strategic supply chain. An urgent payment change may be conventional business email compromise, an effort to redirect funds to a restricted actor or a deliberate attempt to delay production. Unusual access to due-diligence files may be a privacy incident, insider misuse or reconnaissance. Case classification should therefore remain provisional until signals have been correlated across functions.



The unit of analysis also needs to widen. A legal-entity-by-legal-entity view is insufficient when control and benefit can sit across parent companies, joint ventures, investors, subcontractors, end users and intermediaries. Banks need a relationship-level view of the economic unit and the supply chain, supported by entity resolution, change monitoring and contextual intelligence.



A different first question

Could this event expose a sensitive relationship, map capacity, facilitate TF or sanctions and export-control evasion, compromise a critical supply chain, influence a decision or create strategic disruption - even if the immediate transaction appears financially immaterial?

05 How traditional risks evolve - and how mitigation must evolve

Existing controls remain necessary. They need broader context, better linkage and a mission-specific overlay.

The DSRB is unlikely to create an entirely new catalogue of banking risks. It changes the operating environment in which familiar risks emerge, the motives behind them and the consequences of control failure. The mitigation shift is from isolated transaction and product controls toward relationship, supply-chain, intelligence and resilience controls.

 Risk	 Traditional lens	 How it evolves in a DSRB ecosystem	 Mitigation shift
Fraud	Customer or bank loss through account takeover, scams, payment fraud, false applications and business email compromise.	Fraud can be a means of entering a defence ecosystem, misdirecting strategic funding, disrupting production, validating a compromised insider or collecting information.	Add DSRB-specific typologies for false eligibility, fake suppliers, synthetic businesses, duplicate financing, procurement manipulation, defence-client account takeover and relationship-manager social engineering. Route high-risk signals into joint investigations.
Money laundering and terrorist financing	Detect concealment and movement of illicit proceeds through clients, accounts and transactions.	Structures may conceal foreign influence, sanctioned interests, terrorist-financing links, strategic beneficiaries, end users or control of suppliers. Attempted access may matter even when funds do not move.	Move from entity-only KYC to an economic-unit and supply-chain view. Connect beneficial ownership, source/purpose, procurement, trade, geography, end-use and behavioural indicators. Define rapid STR and national-security escalation paths.
Sanctions and export controls	Screen named customers, counterparties, payments and jurisdictions against prescribed lists and rules.	Exposure may be indirect through owners, investors, joint ventures, subcontractors, front companies, dual-use goods, transshipment routes and false end users. Rules can change rapidly with geopolitics.	Use dynamic ownership and control analysis, indirect exposure mapping, event-driven rescreening, export-control expertise, product/end-use data, escalation for ambiguity and documented decision rights.
Trade-based financial crime and end-use	Identify false invoices, phantom shipments, over/under-invoicing and documentary discrepancies used to move value.	Defence procurement adds restricted goods, sensitive components, supplier substitution, misclassification, diversion, false certifications and end-use misrepresentation.	Link trade documents to KYC, contracts, invoices, shipping, goods classification, licences, payment data and expected purpose. Monitor route, counterparty, quantity and end-user changes.
Insider risk	Prevent theft, fraud, privacy breach and misuse by employees or contractors.	Sensitive roles may be recruited, coerced or manipulated for access, approvals, influence or intelligence. Non-human identities can perform insider-like actions.	Identify sensitive roles and data, enhance screening proportionate to role, enforce need-to-know access, monitor privileged human and machine identities, detect behavioural anomalies and secure transfers and exits.
Third-party and supply-chain risk	Manage service quality, outsourcing, data protection, continuity and compliance at vendors.	Vendors, correspondents, cloud platforms, due-diligence firms and subcontractors may become entry points into both the bank and defence ecosystem, with foreign-interference and concentration dimensions.	Apply an integrity and security lens, map subcontractors and fourth parties, require equivalent controls and rapid incident notification, test exit and substitution, and monitor geographic, ownership and government connections.



Control principle 1 - See the economic unit

The decisive questions are who ultimately controls and benefits, whether the end user and purpose are credible, how the subcontractor network changes over time, and whether funds and goods move consistently with that purpose.



06 A zero-dollar loss can still be a material incident

The loss ledger is not the risk ledger.

What the bank knows may be as important as what the bank moves.

Traditional fraud and operational-risk investment cases often begin with booked or forecast financial loss. That is necessary, but insufficient for DSRB-linked activity. A control can succeed in preventing funds from leaving the bank and still reveal a serious attempted compromise, a terrorist-financing or sanctions-evasion pathway, a strategic-data exposure, an insider concern or an effort to delay a critical programme.

 Illustrative event	 Why the loss ledger may show zero	 Why the event may still be material
Fake supplier application is declined before funding	No credit loss and no customer reimbursement.	The entity may be a sanctions or TF proxy, a foreign-influence channel, a synthetic business seeking legitimacy or an attempt to gain access to suppliers and technology.
Payment diversion is blocked	No funds are lost.	A legitimate mailbox or relationship may be compromised; the payment instructions may identify a restricted network; the attempt may be intended to delay production or test controls.
Unusual access is detected before confirmed exfiltration	No quantified data-loss amount.	The access pattern may reveal insider recruitment, reconnaissance, mapping of ownership and capacity, or compromised service credentials with persistent reach.
Third-party incident is contained quickly	No direct bank loss and limited outage.	Sensitive files may have been viewed, a defence supply chain may be exposed, and the bank may face notification, contractual, regulatory and trust consequences.
Hacktivist campaign causes no payment loss	No fraud loss.	Client names, executive information or selected documents may be leaked or manipulated, creating doxing, reputation, employee-safety and stakeholder pressure.

Relevant programme metrics should therefore include more than fraud dollars. Examples include the proportion of DSRB-linked relationships with ultimate ownership, end user and subcontractor networks mapped; coverage of strategic-data classification; the number and age of privileged human and machine identities; time to correlate cross-domain signals; time to joint escalation and containment; unresolved ownership or end-use discrepancies; third-party notification performance; scenario-test results; and residual risk accepted by executives.



Funding implication

Policy changes alone will not be enough. Banks may need funded implementation cycles for data discovery and classification, entity resolution, integrated case management, privileged-access uplift, DSRB-specific typologies, threat intelligence, training, tabletop exercises and board reporting.



07 Breaking down silos: one threat picture, clear decision rights

Convergence is an operating-model requirement, not an org-chart exercise.

DSRB-linked events will rarely fit neatly within one control function. A supplier onboarding concern can involve fraud, beneficial ownership, sanctions, export controls, cyber reconnaissance, insider access, third-party data and reputation at the same time. Sequential referrals between isolated teams create delay and lose context. The objective is not to merge every function, but to make them operate from a common view of the threat and the relationship.

Governance can build on existing forums

Institutions may not need a new permanent governance structure. An existing Executive Risk Committee or financial-crime governance forum can be expanded with a DSRB and economic-security mandate, provided it has the right participants, information, authority and escalation speed. The Board Risk Committee should oversee risk appetite, defence-sector exposure and resilience objectives; the CRO

should own the integrated risk framework; the CAMLO should own AML/ATF, sanctions and financial-crime obligations; the CISO/CSO should protect strategic information and address cyber and insider risk; business leaders should own client and portfolio decisions; and Legal and Compliance should interpret export-control, data-sharing and governance obligations.



Design test

Can the bank connect a fake supplier, a last-minute payment change, unusual access by a relationship manager and a restricted subcontractor - and make a defensible decision within hours rather than days?

08 Guiding questions for executives

The agenda should start before the first transaction.

01

What role does the bank intend to play in the DSRB ecosystem, and what risk perimeter follows from that choice?

Across sectors, roles, counterparties, supply chains, geographies, where does participation remain within strategic and risk appetite – and where should otherwise attractive activity be constrained or declined?

02

Does the bank understand its full DSRB-linked exposure beyond the individual transaction?

Can it see concentrations and dependencies across clients, beneficial owners, suppliers, subcontractors, products, payments, data, technology providers and geographies – including indirect exposure through the wider supply chain?

03

What strategic information could the bank acquire, generate or enable others to infer through participation, and what would make its exposure, alteration or loss material?

Are controls over access, lineage, retention, sharing, models and AI calibrated not only to conventional confidentiality requirements, but also to the intelligence value of ownership, capacity, dependencies, trade flows and other relationship-level information?

04

Can the bank recognize when familiar risk indicators acquire a different significance in a defence, security and resilience context?

Do fraud, AML/ATF, sanctions, cyber, insider and third-party signals connect sufficiently to distinguish ordinary misconduct from sanctions evasion, foreign interference, state-aligned activity, supply-chain compromise, coercion or pre-positioning to disruption?

05

Which events should be treated as material even when the loss ledger remains zero?

Are attempted transactions, blocked payments, declined applications, exposed relationships, compromised information and contained access events assessed for their regulatory, reputational, operational, intelligence and national-security consequences – and can they trigger escalation without a booked financial loss?

06

Are decision rights commensurate with situations in which evidence may remain incomplete while consequences are asymmetric?

Who can accept residual risk, restrict activity, pause, decline or exit; what thresholds govern escalation; and what legal, information-sharing and crisis protocols apply when financial-crime, national-security, export control or foreign-interference concerns converge?

07

Can existing risk and control frameworks operate as a coherent system around the same relationship, threat, supply chain?

Do fraud, AML/ATF sanctions, cyber, insider, third-party, operational resilience, legal and business functions share the threat picture, escalation triggers and response mechanisms required to act together – without creating a parallel compliance architecture?

Conclusion

The strategic question for Canadian financial institutions is not only whether they can finance defence, security and resilience initiatives. It is whether they can operate safely in an environment where financial crime, terrorist financing, sanctions and export controls, fraud, cyber threats, foreign influence and national security increasingly converge.

As economic security becomes a higher priority for Canada and its allies, participating banks may become more than financial intermediaries. They may become critical components of collective resilience infrastructure. The institutions best positioned to support the DSRB will be those that recognize two propositions early: familiar banking activity can carry strategic intelligence value, and a control failure can be material even when the loss ledger shows zero.

The DSRB does not make familiar crimes unfamiliar. It makes them strategically consequential. The executive task is therefore to use the foundations that already exist, add a defence-mission overlay, fund the required implementation, and ensure that functions designed to manage different risks can see and act on the same threat.

Contact us



Éric Lachapelle, M.Sc, CPA, CAMS, CRCP, CFA
 Partner, Advisory Services,
 Regional Financial Services and
 Regulatory Compliance and
 National Financial Crimes Leader
 Montréal
 KPMG Canada



Marilyn Abate, CPA, CA, CPA (Illinois), CBV, CFF, CFE
 Partner, Forensics and Risk
 Consulting
 Toronto
 KPMG Canada



Joseph Nammour, CPA
 Senior Manager, National Financial
 Crimes Centre of Excellence
 Montreal
 KPMG Canada



Jaimin Patel, CFE
 Senior Manager, Forensic Investigation,
 Integrity & Disputes Services
 Toronto
 KPMG Canada



Ryan Pedwell
 Director and Chief of Staff, National
 Financial Crimes Centre of Excellence
 Toronto
 KPMG Canada

Research and source notes

Final DSRB policies and participation requirements remain subject to ratification and design.

- [1] Prime Minister of Canada - Declaration on the Defence, Security and Resilience Bank, 7 July 2026.
- [2] Department of Finance Canada - Canada hosts partners to advance establishment of the DSRB, 23 March 2026.
- [3] Department of Finance Canada - Canada welcomes progress towards establishment of the DSRB and hosting its headquarters, 29 April 2026.
- [4] Prime Minister of Canada - Eight countries commit to supporting the Canada-led DSRB, 7 July 2026.
- [5] Mark Carney, Luc Frieden - Financial Times - Credible deterrence requires a new Nato bank, 24, June 2026.
- [6] Joint statement from member countries of the Multilateral Defence Mechanism, 6 July, 2026.
- [7] Joint statement from the Prime Minister of Canada, Mark Carney, and the Prime Minister of the United Kingdom, Keir Starmer, on defence financing
- [8] PM call with Prime Minister Carney of Canada: 22 July 2026
- [9] Global Risk Institute – Security as a systemic Financial Risk: What defence, security and resilience Bank means for financial leaders, May 2026.
- [10] European Investment Bank - Guarantees; and EIB defence-industry intermediated financing with Deutsche Bank, 11 June 2025.
- [11] International Finance Corporation - Global Trade Finance Program
- [12] European Bank for Reconstruction and Development - Trade Facilitation Programme.
- [13] Office of the Superintendent of Financial Institutions - Integrity and Security Guideline.
- [14] Office of the Superintendent of Financial Institutions - Guideline B-10, Third-Party Risk Management.
- [15] Office of the Superintendent of Financial Institutions - Guideline B-13, Technology and Cyber Risk Management; and intelligence-led cyber-resilience testing resources.
- [16] Office of the Superintendent of Financial Institutions - Guideline E-21, Operational Risk Management and Resilience.
- [17] FINTRAC - Reporting suspicious transactions; beneficial ownership requirements; terrorist activity financing indicators; sanctions-evasion bulletin.
- [18] Canadian Centre for Cyber Security - National CyberThreat Assessment 2025-2026.
- [19] Public Services and Procurement Canada - Controlled Goods Program requirements and security assessments.



The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavour to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

© 2026 KPMG LLP, an Ontario limited liability partnership and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved. The KPMG name and logo are trademarks used under license by the independent member firms of the KPMG global organization.