

Banque de la défense, de la sécurité et de la résilience

Nouveau mandat de gestion du risque
pour les banques canadiennes





Rapport sommaire

Le modèle est connu. La mission, elle, ne l'est pas.

Le Canada et huit pays partenaires ont annoncé leur intention commune d'établir la BDSR en juillet 2026, à la suite de la négociation des statuts constitutifs de l'entente à Montréal. Selon les déclarations publiques, les activités débuteront dès 2027.^[1-3] L'analyse qui suit comporte des hypothèses au sujet du modèle opérationnel définitif.

La Banque de la défense, de la sécurité et de la résilience (la « BDSR ») vise à mobiliser des capitaux publics et privés pour soutenir les priorités en matière de défense, de sécurité et de résilience dans l'ensemble des pays membres. Les annonces publiques font état d'une institution multilatérale dirigée par le Canada, qui offrirait du financement à long terme et à faible coût ainsi que des garanties, compléterait les mécanismes nationaux et multilatéraux existants, notamment en s'harmonisant avec le Mécanisme multilatéral de défense (le « MMD »), et aiderait les gouvernements et les entreprises du secteur de la défense à combler leurs besoins de financement et à accroître leur capacité industrielle.^[4-8]

Il n'est pas nécessaire de concevoir de toutes pièces le mandat de gestion du risque. Les institutions multilatérales ont déjà recours aux garanties, au partage du risque, aux prêts intermédiés, au financement de projets et aux programmes de financement du commerce pour mobiliser les bilans

des banques commerciales. Elles disposent également d'approches bien établies en matière de contrôle diligent de l'intégrité, de lutte contre le blanchiment d'argent, le financement des activités terroristes et la fraude, ainsi que de surveillance de l'approvisionnement. La nouveauté réside dans la mission expressément axée sur la défense et dans l'importance stratégique des relations, des opérations et des données qui pourraient transiter par les banques participantes, ce qui crée un nouveau type de renseignements susceptibles de présenter un intérêt pour des acteurs hostiles, étatiques ou non étatiques.

Les banques commerciales canadiennes pourraient agir à titre de partenaires financiers, de banques transactionnelles, de banques spécialisées dans le commerce et les chaînes d'approvisionnement, d'intermédiaires sur les marchés financiers, de conseillers, de contrôleurs en matière de criminalité financière et de dépositaires de renseignements de valeur stratégique. Le rôle tenu déterminera les contreparties avec lesquelles la banque interagit, les données qu'elle traite, les renseignements auxquels elle a accès, les activités qu'elle peut perturber et les risques auxquels elle s'expose. Le périmètre de risque suit donc les flux financiers, les données et les relations et ne se limite pas au cadre juridique d'un prêt garanti par la BDSR.

Le nouveau risque le plus important tient à la valeur des informations bancaires courantes en tant que renseignements à utiliser. Les relations avec les fournisseurs, la propriété effective, les capacités de production, le calendrier des paiements, les flux commerciaux, les constatations découlant des contrôles diligents, les priorités gouvernementales et les dépendances à la technologie peuvent permettre à un adversaire de cartographier la base industrielle de défense, d'en repérer les points vulnérables, de contourner les sanctions, de recruter des personnes à l'interne, d'influencer les décisions ou de préparer des actions perturbatrices. Les banques pourraient être ciblées non seulement dans le but de voler de l'argent, mais aussi pour recueillir des renseignements, la cartographie de leurs activités, exercer une influence, compromettre leurs systèmes, retarder ou perturber leurs activités.



Les risques traditionnels existent toujours. La fraude, le blanchiment d'argent, le financement des activités terroristes, le contournement des sanctions et des contrôles à l'exportation, les cyberrisques, les risques liés aux tiers et les risques internes, ainsi que la résilience opérationnelle demeurent les principaux domaines de la gestion des risques. Les éléments qui changent sont leur contexte, leur interdépendance et leurs conséquences éventuelles. Un paiement bloqué, une demande refusée ou un incident d'accès aux données maîtrisé peut ne pas entraîner de perte comptabilisée, mais pourrait constituer un incident important lié à la criminalité financière, à la réglementation, à la réputation ou à la sécurité nationale.

La participation de la BDSR amènerait les institutions financières à interagir plus étroitement avec des secteurs, des contreparties et des activités liés à la défense, qui pourraient avoir une incidence différente sur leur tolérance au risque actuelle. Les institutions canadiennes pourraient ainsi devoir réévaluer délibérément la place de ces expositions dans leur tolérance au risque et les circonstances dans lesquelles elles peuvent être acceptées. Le défi qui en résulte est donc de déterminer comment évaluer, encadrer et contrôler les risques liés aux activités associées à la BDSR, à mesure que ceux-ci occupent une place plus délibérée dans le positionnement stratégique de l'institution en matière de risque.

La réponse requise consiste à ajouter aux cadres existants des mesures propres à la mission, plutôt qu'à créer un régime de conformité parallèle. La fraude, la lutte contre le blanchiment d'argent et le financement des activités terroristes (la « LBA/FAT »), les sanctions, les cyberrisques, la sécurité, les risques liés aux tiers, la gouvernance des données et la résilience opérationnelle n'ont pas à être regroupés en une seule fonction. Toutefois, ils doivent reposer sur une perception commune des menaces, une vision de l'unité économique et de la chaîne d'approvisionnement à l'échelle de chaque relation, des critères communs de signalement aux échelons supérieurs, des pouvoirs décisionnels clairement définis, un échange sécurisé de renseignements et des simulations conjointes de scénarios. Les cadres du BSIF, du CANAFE, des contrôles à l'exportation, du Programme des marchandises contrôlées et du Centre pour la cybersécurité fournissent une grande partie des éléments de base. La participation de la BDSR exigerait que ces différents cadres fonctionnent de manière conjointe. ^[9,13,16,19]



Un choix stratégique, pas seulement une décision liée aux produits

Les conseils d'administration devraient définir dans quels domaines et de quelle manière la banque est prête à participer, notamment en ce qui concerne les secteurs, les rôles, les régions, les contreparties, l'exposition aux données et les circonstances justifiant un refus.



Le rôle détermine l'exposition

Un prêteur, une banque transactionnelle, un conseiller et un dépositaire de renseignements ont accès à des données différentes, créent des dépendances différentes et nécessitent des contrôles différents.



Les renseignements deviennent un actif protégé

Les renseignements que la banque conserve pourraient avoir la même importance que ceux qu'elle transfère. Les données stratégiques doivent être classifiées et faire l'objet d'un accès fondé sur le principe du besoin de savoir, d'une surveillance et d'un partage sécurisé.



La fraude devient une source de renseignement

Un faux fournisseur, un détournement de paiement ou un accès inhabituel à des fichiers peut être le signe d'un contournement de sanctions, d'un financement des activités terroristes, d'une ingérence étrangère, d'une activité de reconnaissance ou d'une compromission de la chaîne d'approvisionnement.



Les incidents sans perte financière peuvent être importants

Les tentatives d'opérations, les relations compromises, les retards opérationnels et les atteintes à la réputation peuvent entraîner des conséquences importantes, même en l'absence de transfert ou de perte de fonds.



Les fonctions doivent converger

Le modèle opérationnel devrait relier les décisions relatives à la fraude, à la LBA/FAT, aux sanctions, aux cyberrisques, aux délits d'initiés et aux tiers ainsi qu'à la résilience, sans nécessiter le regroupement de ces fonctions sur le plan organisationnel.

01 La BDSR et ses véritables nouveautés

Un ensemble d'outils financiers multilatéraux connus dédiés aux missions expressément axées sur la défense, la sécurité et la résilience.

Proposition d'une institution multilatérale ayant pour mission la défense

La BDSR est conçue comme une institution financière internationale destinée aux alliés et partenaires participants. L'objectif annoncé consiste à mobiliser des capitaux à grande échelle, à réduire les coûts du financement et à accroître la capacité industrielle dans l'ensemble des pays membres. Les documents publics font état de prêts aux pays membres, de garanties susceptibles d'accroître l'accès à des capitaux privés abordables, ainsi que d'un soutien aux initiatives en matière de défense, de sécurité et de résilience dans l'ensemble des chaînes d'approvisionnement.^[1-4]

L'écosystème devrait s'étendre au-delà des entrepreneurs principaux. Il pourrait comprendre des fabricants du secteur de la défense, des entreprises des secteurs de l'aérospatiale et des technologies de pointe, des fournisseurs de services de cybersécurité et de télécommunications, des projets liés aux minéraux critiques et à la sécurité énergétique, des entreprises des secteurs du transport et des infrastructures essentielles, des entreprises à double usage, des PME, des sous-traitants

et des partenaires technologiques. Une banque canadienne pourrait donc être intégrée à un réseau transfrontalier de financement et de chaînes d'approvisionnement dont les activités commerciales ont une importance sur les plans géopolitique et de la sécurité nationale.

Le modèle est connu

Les institutions multilatérales existantes montrent comment le soutien public au crédit peut arriver à l'économie privée par l'intermédiaire des banques commerciales. Par exemple, les garanties de la Banque européenne d'investissement (« BEI ») peuvent couvrir une partie des pertes et favoriser l'octroi de prêts supplémentaires; les prêts intermédiés de la BEI sont déjà utilisés pour les banques commerciales afin de financer les chaînes d'approvisionnement de l'industrie européenne de la défense. Les programmes de financement du commerce de la Société financière internationale (« IFC ») et de la Banque européenne pour la reconstruction et le développement (« BERD ») ont recours à des garanties, au partage du risque, à des conventions-cadres et à des réseaux de banques partenaires pour accroître les capacités de financement du commerce.



Cadre réglementaire canadien

Les lignes directrices du BSIF sur l'intégrité et la sécurité B-10, B-13 et E-21; le CANAFE, la LBA/FAT et la déclaration des cas de contournement des sanctions, les contrôles à l'exportation, les marchandises contrôlées et les lignes directrices sur la cyberrésilience couvrent déjà de nombreuses composantes de ces risques.^[13]

La mission est nouvelle

La BDSR n'est pas simplement un autre mécanisme de financement du développement. Elle est expressément conçue pour répondre à des objectifs en matière de défense, de sécurité et de résilience. Cette vocation modifie la valeur stratégique des activités et des renseignements sous-jacents. Une même garantie, un même prêt, un même paiement ou un même dossier de contrôle diligent peut s'inscrire dans une chaîne d'approvisionnement comprenant des marchandises contrôlées, des technologies à double usage, des priorités souveraines, des capacités de production sensibles et des dépendances opérationnelles critiques.

Ainsi, la question à se poser en matière de contrôle ne se limite plus à : « Cet événement pourrait-il entraîner une perte financière, causer un préjudice à un client ou donner lieu à un manquement réglementaire? » Un modèle tenant compte de la BDSR doit également déterminer si un événement pourrait révéler des relations sensibles avec des fournisseurs, permettre de cartographier les capacités du secteur de la défense, faciliter le financement des activités terroristes ou le contournement des sanctions et des contrôles à l'exportation, compromettre une chaîne d'approvisionnement essentielle, influencer une décision ou provoquer une perturbation stratégique.



À retenir pour les dirigeants

La BDSR n'oblige pas les banques à abandonner leurs cadres de gestion des risques existants. Elle les oblige plutôt à les appliquer dans une perspective de sécurité économique et de renseignement et à coordonner des contrôles qui sont souvent exercés séparément.

02 Rôles possibles des banques commerciales canadiennes

La participation devrait être définie en fonction du rôle exercé, des renseignements auxquels la banque a accès et des liens de dépendance créés et non en fonction d’une simple catégorie de produit.



Rôle possible	Exemple d'activités	Incidences distinctes sur les risques et les contrôles
Partenaire de financement	Prêts directs ou garantis, cofinancement, prêts consortiaux, facilités de crédit renouvelables, fonds de roulement et financement de projets.	Décisions en matière de crédit et d’admissibilité; contrôle diligent des emprunteurs et des promoteurs; clauses restrictives; surveillance de l’affectation et de l’utilisation finale du produit; concentration du portefeuille et concentration géopolitique.
Banque spécialisée dans le commerce et les chaînes d’approvisionnement	Lettres de crédit, garanties de bonne exécution et de paiement anticipé, financement des chaînes d’approvisionnement et financement des créances, des stocks et du matériel.	Visibilité sur les marchandises, les itinéraires, les factures, les utilisateurs finaux et les sous-traitants; exposition à la criminalité liée au commerce, au contournement des contrôles à l’exportation, à la substitution de fournisseurs et à la fraude documentaire.
Banque transactionnelle	Paiements, gestion de trésorerie, opérations de change, services de trésorerie, garanties, services d’entiercement et services d’agent.	Traitement de flux de grande valeur et urgents; détournement de paiements, exposition aux sanctions, dépendance opérationnelle et accès à des renseignements sur le calendrier d’approvisionnement et les cycles de production.
Intermédiaire sur les marchés financiers	Prise ferme d’obligations ou de prêts, distribution, titrisation, placements privés, couverture et accès aux investisseurs institutionnels.	Renseignements sur les opérations et informations à fournir; contreparties parmi les investisseurs et les membres des consortiums; conduite sur les marchés, barrières à l’information, risques de réputation et de concentration.
Conseiller et organisateur	Conseils financiers, structuration de projets, fusions et acquisitions, planification des capitaux, évaluation et soutien à l’exécution des opérations.	Accès précoce à des renseignements sur les gouvernements, la propriété, les technologies, les capacités et les renseignements liés aux décisions stratégiques; risques accrus de conflits, de délits d’initiés et d’influence.
Contrôleur en matière de criminalité financière	Connaissance du client et de l’entreprise, propriété effective, examen des sanctions et des renseignements défavorables, surveillance des opérations, contrôles antifraude et déclaration des opérations douteuses.	Décisions pouvant déterminer qui accède à l’écosystème, comment les expositions indirectes sont détectées et si les indicateurs liés aux mandataires, aux personnes sanctionnées, au FAT ou à l’ingérence étrangère sont signalés aux échelons supérieurs.
Dépositaire de renseignements et maillon de la résilience	Conservation des dossiers de contrôle diligent, des données sur les fournisseurs et les paiements, des contrats, des communications, des modèles, des identifiants d’accès et des renseignements sur les dépendances opérationnelles.	Vol de données stratégiques, recrutement de personnes à l’interne, compromission de tiers, fuite de données par l’IA et perturbation de services dont dépendent les intervenants du secteur de la défense.

La participation directe et indirecte compte

Une banque peut s’exposer à des activités liées à la BDSR sans être officiellement une contrepartie de celle-ci. Des clients existants peuvent devenir des fournisseurs admissibles; un emprunteur peut acquérir une entreprise du secteur de la défense ou à double usage; un client utilisant des services de paiement peut commencer à participer à un programme financé par la BDSR; un fournisseur tiers de services de contrôle diligent peut traiter des dossiers liés à la BDSR. La cartographie des expositions devrait donc distinguer la participation directe de l’exposition indirecte par l’intermédiaire des clients, des fournisseurs, des sous-traitants, des investisseurs, des prestataires et des fournisseurs de technologies.

Le périmètre de risque est déterminé par les flux financiers, les données et les relations et non le cadre juridique du prêt garanti.

En pratique, le choix des rôles devrait être pris en compte dans la tolérance au risque. Une banque pourrait être disposée à fournir des services de paiement, mais pas des services-conseils, à financer des infrastructures bien établies, mais pas des technologies émergentes à double usage, ou à participer à un prêt consorcial uniquement lorsque la BDSR ou une autre institution conserve certaines responsabilités précises en matière d’admissibilité, de surveillance et de partage des pertes. La participation n’est pas une décision binaire. Elle peut être modulée en fonction du produit, du secteur, de la région, de l’accès à l’information et du degré de maturité des contrôles.



03 Le nouveau risque : la valeur des activités bancaires en tant que renseignement à utiliser

Les banques peuvent être ciblées pour ce qu’elles savent, les liens qu’elles établissent, les opérations qu’elles traitent et les activités qu’elles peuvent perturber.

La participation à des activités liées à la BDSR crée une forme d’exposition aux renseignements stratégiques qui n’est pas entièrement prise en compte par les catégories traditionnelles de risques liés à la confidentialité, à la protection des renseignements personnels ou aux pertes découlant de cyberincidents. Les données générées dans le cadre des activités bancaires courantes peuvent révéler la façon dont un écosystème de défense est organisé et financé ainsi que ses liens de dépendance. Pris isolément, certains éléments de données peuvent sembler relever d’activités commerciales courantes, mais lorsqu’ils sont regroupés dans l’ensemble des clients, dans les données de paiement et des fournisseurs et sur une certaine période, ils peuvent constituer une source de renseignement.

<div>  Perception possible de la banque </div>	<div>  Valeur potentielle en tant que renseignement </div>
Relations avec les fournisseurs et les clients du secteur de la défense	Peuvent aider à cartographier la base industrielle du Canada et de ses alliés, à repérer les entreprises émergentes à double usage et à révéler les liens entre les entrepreneurs principaux, les PME et les sous-traitants.
Flux, montants et calendrier des paiements	Peuvent fournir des indications sur les activités d’approvisionnement, les cycles de production, les besoins urgents, les contraintes de trésorerie, les contreparties et les dépendances opérationnelles.
Dossiers de crédit et de contrôle diligent	Peuvent contenir des renseignements non accessibles au public sur la propriété, la direction, les revenus, les capacités, les prix, les contrats, les fournisseurs et les propriétaires effectifs, ainsi que des renseignements défavorables.
Financement du commerce et activités transfrontalières	Peuvent révéler les mouvements de marchandises, de services, d’outillage et de composants sensibles, les itinéraires de transbordement, les utilisateurs finaux et les goulots d’étranglement.
Renseignements sur les gouvernements et les opérations	Peuvent révéler les priorités des politiques, les fournisseurs privilégiés, les structures de financement, les approbations, le calendrier des projets et les positions de négociation.
Personnes et décideurs	Les directeurs de la relation avec les clients, les responsables du crédit, les conseillers et les dirigeants peuvent être la cible d’activités de piratage psychologique, de coercition, d’ingérence étrangère, de recrutement de personnes à l’interne ou de divulgation malveillante de renseignements personnels.
Dépendances liées aux tiers et aux technologies	Peuvent permettre de repérer des points d’entrée moins bien protégés, des comptes de service à accès privilégié, des fournisseurs de services de contrôle diligent, des plateformes infonuagiques, des API, des modèles et des points uniques de défaillance opérationnelle.

Exemples de risque lié aux renseignements stratégiques


Collecte de renseignements et espionnage

Cyberintrusions ciblées, vol d’identifiants, accès par des personnes à l’interne, compromission de tiers ou piratage psychologique visant à obtenir des fichiers, des communications ou des métadonnées.


Cartographie et regroupement

Regroupement de données sur la propriété, les fournisseurs, les paiements et leur calendrier afin de déterminer les capacités, les dépendances, les points vulnérables et les technologies émergentes.


Influence et infiltration

Recours à des sociétés-écrans, à des investisseurs dont l’identité est inaccessible, à des personnes recrutées à l’interne ou à des directeurs de la relation avec les clients manipulés afin de s’introduire dans l’écosystème ou d’influencer les décisions.


Contournement et détournement

Recours à des entités agissant pour le compte de tiers, à des structures de propriété complexes, à de faux utilisateurs finaux, au transbordement, à de fausses déclarations commerciales ou au détournement de paiements afin de transférer des fonds ou des capacités à des intervenants visés par des restrictions.


Prépositionnement et perturbation

Compromission préalable d’identifiants, de fournisseurs ou de processus afin de permettre à un intervenant de retarder le décaissement de fonds, d’interrompre la production, de divulguer des données ou de semer la confusion en situation de crise.


Attaques informationnelles et à la réputation

Divulgation sélective de renseignements, divulgation malveillante de renseignements personnels sur des dirigeants, amplification de controverses ou fausses allégations d’inconduite visant à décourager la participation ou à miner la confiance.

Les acteurs de la menace auront des motivations différentes

Les acteurs étatiques et ceux qui leur sont affiliés peuvent chercher à recueillir des renseignements, à obtenir un avantage stratégique ou à provoquer des perturbations. Les entités visées par des sanctions et des restrictions peuvent chercher à obtenir un accès, à dissimuler leurs activités et à contourner les mesures en place. Le crime organisé peut fournir des moyens facilitant ces activités, notamment des entreprises fictives, des sociétés prête-nom, des documents frauduleux et des services de transfert de fonds. Les cyberactivistes peuvent chercher à provoquer des perturbations, à divulguer des renseignements et à exercer des pressions sur le plan de la réputation. Les personnes à l'interne peuvent être recrutées, contraintes, négligentes ou compromises. Les acteurs non humains à l'interne – comptes de service, clés d'API, robots, scripts, modèles et flux des travaux automatisés – peuvent disposer d'un accès privilégié sans être assujettis aux contrôles comportementaux appliqués aux employés. Le Centre canadien pour la cybersécurité estime que des acteurs étatiques et non étatiques ciblent déjà les infrastructures essentielles et que les adversaires étatiques font preuve d'une audace croissante et mènent des activités de plus en plus perturbatrices.^[18]



Incidences pour la direction

Les renseignements stratégiques devraient être traités comme une catégorie d'actifs. Les banques devraient recenser les données liées à la BDSR, en attribuer la responsabilité à une fonction de l'entreprise, les classer selon leur degré de sensibilité stratégique, en limiter l'accès en fonction des besoins opérationnels, surveiller les identités humaines et les identités machines, contrôler l'utilisation de l'IA et définir les modalités d'échange sécurisé de renseignements entre les fonctions ainsi qu'avec les autorités.

04 Convergence des risques : de l'incident de criminalité financière au signal de sécurité nationale

Les risques fondamentaux sont interdépendants. Un même incident peut constituer à la fois un cas de fraude, un enjeu lié aux sanctions, un cyberincident et un signal de sécurité nationale.

Le risque réside dans la combinaison

Un fournisseur nouvellement constitué peut être un véhicule servant à commettre une fraude lors d'une demande, un prête-nom permettant de contourner des sanctions, un canal d'ingérence étrangère ou un moyen d'obtenir un accès d'apparence légitime à une chaîne d'approvisionnement stratégique. Une modification urgente liée au paiement peut correspondre à une fraude classique par compromission d'un courriel d'entreprise, à une tentative de détourner des fonds vers un acteur visé par des restrictions ou à une manœuvre délibérée visant à retarder la production. Un accès inhabituel à des dossiers de contrôle diligent peut constituer un incident lié à la protection des renseignements personnels, une utilisation abusive par une personne à l'interne ou une activité

de reconnaissance. La classification des cas devrait donc demeurer provisoire jusqu'à ce que les signaux aient été recoupés entre les différentes fonctions.

L'unité d'analyse doit également être élargie. Une analyse entité juridique par entité juridique ne suffit pas lorsque le contrôle et les avantages peuvent être répartis entre des sociétés mères, des coentreprises, des investisseurs, des sous-traitants, des utilisateurs finaux et des intermédiaires. Les banques doivent adopter une vision de l'unité économique et de la chaîne d'approvisionnement à l'échelle de chaque relation, appuyée par la résolution d'entités, la surveillance des changements et des renseignements contextuels.



Une première question différente

Cet incident pourrait-il révéler une relation sensible, permettre de cartographier des capacités, faciliter le FAT ou le contournement des sanctions et des contrôles à l'exportation, compromettre une chaîne d'approvisionnement essentielle, influencer une décision ou provoquer une perturbation stratégique, même si l'opération en cause semble peu importante sur le plan financier?



06 Un incident sans perte financière peut tout de même être important

Le registre des pertes ne reflète pas tous les risques.

Les renseignements que la banque conserve pourraient avoir la même importance que ceux qu'elle transfère.

Les analyses de rentabilité traditionnelles des investissements dans la lutte contre la fraude et la gestion du risque opérationnel reposent souvent sur les pertes financières comptabilisées ou prévues. Ce critère est nécessaire, mais insuffisant dans le cas des activités liées à la BDSR. Un contrôle peut réussir à empêcher des fonds de sortir de la banque tout en révélant une grave tentative de compromission, un mécanisme de financement des activités terroristes ou de contournement des sanctions, une exposition de données stratégiques, une préoccupation liée à une personne à l'interne ou une tentative visant à retarder un programme essentiel.

Exemple d'incident	Pourquoi le registre des pertes peut n'indiquer aucune perte	Pourquoi l'incident peut néanmoins être important
Une demande présentée par un faux fournisseur est refusée avant l'octroi du financement	Aucune perte de crédit ni aucun remboursement au client.	L'entité peut être un prête-nom lié à des sanctions ou au FAT, un canal d'ingérence étrangère, une entreprise fictive cherchant à paraître légitime ou un moyen d'obtenir un accès à des fournisseurs et à des technologies.
Un détournement de paiement est bloqué	Aucune perte de fonds.	Une boîte de courriel ou une relation d'affaires légitime peut avoir été compromise; les instructions de paiement peuvent permettre de repérer un réseau visé par des restrictions; la tentative peut viser à retarder la production ou à mettre les contrôles à l'épreuve.
Un accès inhabituel est détecté avant qu'une exfiltration soit confirmée	Aucune perte liée aux données ne peut être quantifiée.	Le profil d'accès peut révéler le recrutement d'une personne à l'interne, une activité de reconnaissance, une cartographie de la propriété et des capacités ou la compromission d'identifiants de service donnant un accès continu.
Un incident touchant un tiers est rapidement maîtrisé	Aucune perte directe pour la banque et interruption limitée des activités.	Des fichiers sensibles peuvent avoir été consultés, une chaîne d'approvisionnement du secteur de la défense peut avoir été exposée et la banque peut devoir composer avec des conséquences liées à la notification, aux contrats, à la réglementation et à la confiance.
Une campagne cyberactiviste n'entraîne aucune perte liée aux paiements	Aucune perte liée à la fraude.	Des noms de clients, des renseignements sur des dirigeants ou certains documents peuvent être divulgués ou manipulés, entraînant la divulgation malveillante de renseignements personnels, des atteintes à la réputation, des risques pour la sécurité des employés et des pressions de la part des parties prenantes.

Les indicateurs pertinents du programme devraient donc relever d'autres éléments que les pertes financières liées à la fraude. Ils pourraient notamment comprendre la proportion des relations liées à la BDSR pour lesquelles la propriété finale, l'utilisateur final et les réseaux de sous-traitants ont été cartographiés; la couverture de la classification des données stratégiques; le nombre et l'ancienneté des identités humaines et machine disposant d'un accès privilégié; le délai nécessaire pour recouper les signaux provenant de différents domaines; le délai de signalement conjoint aux échelons supérieurs et de maîtrise des incidents; les divergences non résolues concernant la propriété ou l'utilisation finale; l'efficacité des notifications par les tiers; les résultats des simulations de scénarios et le risque résiduel accepté par les dirigeants.



Incidences sur le financement

Les modifications aux politiques ne suffiront pas à elles seules. Les banques pourraient devoir consacrer des ressources financières à des cycles de mise en œuvre portant sur la découverte et la classification des données, la résolution d'entités, la gestion intégrée des cas, le renforcement des contrôles des accès privilégiés, les typologies propres à la BDSR, les renseignements sur les menaces, la formation, les exercices de table et la production de rapports au conseil d'administration.

07 Décloisonnement : perception commune des menaces et pouvoirs décisionnels clairement définis

La convergence est une exigence du modèle opérationnel et non un exercice d'organigramme organisationnel.

Les événements liés à la BDSR relèveront rarement d'une seule fonction de contrôle. Une préoccupation soulevée lors de l'intégration d'un fournisseur peut concerner simultanément la fraude, la propriété effective, les sanctions, les contrôles à l'exportation, les activités de cyberreconnaissance, l'accès par des personnes à l'interne, les données détenues par des tiers et la réputation. Le renvoi successif d'un dossier entre des équipes cloisonnées entraîne des délais et une perte de contexte. L'objectif n'est pas de regrouper toutes les fonctions, mais de faire en sorte qu'elles s'appuient sur une vision commune des menaces et de la relation d'affaires dans le cadre de leurs activités.

La gouvernance peut s'appuyer sur les instances existantes

Les institutions n'ont pas nécessairement besoin de créer une nouvelle structure de gouvernance permanente. Un comité de direction chargé des risques déjà en place ou une instance existante de gouvernance de la criminalité financière peut voir son mandat élargi pour englober la BDSR et la sécurité économique, à condition de réunir les participants appropriés et de disposer des renseignements et des pouvoirs nécessaires ainsi que de mécanismes de signalement aux échelons supérieurs rapides. Le comité des risques du conseil d'administration devrait surveiller la tolérance au

risque, l'exposition au secteur de la défense et les objectifs de résilience; le chef de la gestion des risques devrait être responsable du cadre intégré de gestion des risques; le chef de la lutte contre le blanchiment d'argent devrait être responsable des obligations en matière de LBA/FAT, de sanctions et de criminalité financière; le chef de la sécurité de l'information ou le chef de la sécurité devrait protéger les renseignements stratégiques et gérer les cyberrisques et les risques liés aux personnes à l'interne; les dirigeants de l'entreprise devraient être responsables des décisions relatives aux clients et aux portefeuilles; et les fonctions liées aux affaires juridiques et à la conformité devraient interpréter les obligations relatives aux contrôles à l'exportation, à l'échange de données et à la gouvernance.



Test de conception

La banque est-elle en mesure d'établir des liens entre un faux fournisseur, une modification de dernière minute liée au paiement, un accès inhabituel par un directeur de la relation avec les clients et un sous-traitant visé par des restrictions, puis de prendre une décision défendable en quelques heures plutôt qu'en quelques jours?

08 Questions à l'intention des dirigeants

La réflexion devrait commencer avant même la première opération.

01 Quel rôle la banque entend-elle jouer dans l'écosystème de la BDSR et quel périmètre de risque découle de ce choix?

Dans quels secteurs, rôles, relations avec les contreparties, chaînes d'approvisionnement et régions la participation demeure-t-elle conforme aux objectifs stratégiques et à la tolérance au risque et dans quels cas des activités par ailleurs attrayantes devraient-elles être restreintes ou refusées?

02 La banque comprend-elle l'ensemble de son exposition liée à la BDSR, au-delà de chaque opération considérée individuellement?

Peut-elle repérer les concentrations et les dépendances touchant les clients, les propriétaires effectifs, les fournisseurs, les sous-traitants, les produits, les paiements, les données, les fournisseurs de technologies et les régions, y compris les expositions indirectes découlant de l'ensemble de la chaîne d'approvisionnement?

03 Quels renseignements stratégiques la banque pourrait-elle acquérir, générer ou permettre à des tiers d'en déduire du fait de sa participation, et dans quelles circonstances leur exposition, leur altération ou leur perte deviendraient-elles importantes?

Les contrôles relatifs à l'accès, à la traçabilité, à la conservation et au partage des données ainsi qu'aux modèles et à l'IA tiennent-ils compte non seulement des exigences traditionnelles en matière de confidentialité, mais aussi de la valeur en tant que renseignement des données sur la propriété, les capacités, les dépendances, les flux commerciaux et d'autres renseignements à l'échelle de chaque relation?

04 La banque est-elle en mesure de reconnaître les situations où des indicateurs de risque connus prennent une importance différente dans un contexte de défense, de sécurité et de résilience?

Les signaux liés à la fraude, à la LBA/FAT, aux sanctions, aux cyberrisques, aux personnes à l'interne et aux tiers sont-ils suffisamment recoupés pour distinguer les inconduites courantes du contournement des sanctions, de l'ingérence étrangère, des activités liées à des acteurs étatiques, de la compromission de la chaîne d'approvisionnement, de la coercition ou d'un repositionnement en vue de provoquer des perturbations?

05 Quels incidents devraient être considérés comme importants même lorsque le registre des pertes n'indique aucune perte?

Les tentatives d'opérations, les paiements bloqués, les demandes refusées, les relations exposées, les renseignements compromis et les incidents d'accès maîtrisés sont-ils évalués en fonction de leurs conséquences réglementaires, réputationnelles et opérationnelles ainsi que de leurs conséquences sur le plan du renseignement et de la sécurité nationale? Peuvent-ils donner lieu à un signalement aux échelons supérieurs en l'absence de perte financière comptabilisée?

06 Les pouvoirs décisionnels sont-ils adaptés aux situations où les éléments probants peuvent demeurer incomplets alors que les conséquences sont asymétriques?

Qui peut accepter le risque résiduel, restreindre ou suspendre une activité, la refuser ou y mettre fin? Quels seuils déterminent le signalement aux échelons supérieurs? Quels protocoles juridiques, d'échange de renseignements et de gestion de crise s'appliquent lorsque convergent des enjeux de criminalité financière, de sécurité nationale, de contrôles à l'exportation ou d'ingérence étrangère?

07 Les cadres existants de gestion des risques et de contrôle peuvent-ils fonctionner comme un système cohérent en ce qui concerne une même relation, une même menace et une même chaîne d'approvisionnement?

Les fonctions responsables de la fraude, de la LBA/FAT et des sanctions, des cyberrisques, des risques liés aux personnes à l'interne et aux tiers, de la résilience opérationnelle, des affaires juridiques et des activités commerciales partagent-elles une vision commune des menaces, des critères communs de signalement aux échelons supérieurs et les mécanismes d'intervention nécessaires pour agir de façon concertée, sans créer une structure de conformité parallèle?

Conclusion

La question stratégique qui se pose aux institutions financières canadiennes n'est pas seulement de savoir si elles peuvent financer des initiatives en matière de défense, de sécurité et de résilience. Elles doivent également déterminer si elles peuvent exercer leurs activités en toute sécurité dans un environnement où la criminalité financière, le financement des activités terroristes, les sanctions et les contrôles à l'exportation, la fraude, les cybermenaces, l'ingérence étrangère et les enjeux de sécurité nationale convergent de plus en plus.

Alors que la sécurité économique devient une priorité croissante pour le Canada et ses alliés, les banques participantes pourraient devenir plus que de simples intermédiaires financiers. Elles pourraient devenir des composantes essentielles de l'infrastructure de résilience collective. Les institutions les mieux placées pour soutenir la BDSR seront celles qui reconnaîtront rapidement deux réalités : les activités bancaires courantes peuvent avoir une valeur stratégique en tant que renseignement et une défaillance des contrôles peut être importante même lorsque le registre des pertes n'indique aucune perte.

La BDSR ne transforme pas les formes de criminalité connues. Elle leur donne des conséquences stratégiques. Les dirigeants doivent donc s'appuyer sur les éléments de base existants, y ajouter des mesures propres à la mission de défense, financer leur mise en œuvre et veiller à ce que les fonctions chargées de gérer différents risques puissent avoir une vision commune des menaces et agir en visant la même menace.

Communiquez avec nous



Éric Lachapelle, M.Sc, CPA, CAMS, CRCP, CFA
 Associé, Services-conseils, leader régional, Services financiers et conformité réglementaire, et leader national, Crimes financiers
 Montréal
 KPMG Canada



Marilyn Abate, CPA, CA, CPA (Illinois), CBV, CFF, CFE
 Associée, Juricomptabilité et Services-conseils – Gestion des risques
 Toronto
 KPMG Canada



Joseph Nammour, CPA
 Directeur principal, Centre national d'excellence en crimes financiers
 Montréal
 KPMG Canada



Jaimin Patel, CFE
 Directeur principal, Juricomptabilité – Enquête, intégrité et règlement de différends
 Toronto
 KPMG Canada



Ryan Pedwell
 Premier directeur et chef de cabinet, Centre national d'excellence en crimes financiers
 Toronto
 KPMG Canada

Notes de recherche et sources

Les politiques définitives de la BDSR et les exigences relatives à la participation demeurent assujetties à la ratification et à la finalisation de leur conception.

- [1] Premier ministre du Canada - Déclaration sur la Banque de la défense, de la sécurité et de la résilience, 7 juillet 2026.
- [2] Ministère des Finances Canada - Le Canada accueille des partenaires pour faire progresser l'établissement de la Banque de la défense, de la sécurité et de la résilience, 23 mars 2026.
- [3] Ministère des Finances Canada - Le Canada se réjouit des progrès réalisés vers l'établissement de la Banque de la défense, de la sécurité et de la résilience, 29 avril 2026.
- [4] Premier ministre du Canada - Huit pays s'engagent à soutenir les efforts dirigés par le Canada pour mettre en place la Banque de la défense, de la sécurité et de la résilience, 7 juillet 2026.
- [5] Mark Carney, Luc Frieden - Financial Times - Credible deterrence requires a new Nato bank, 24 juin 2026 (en anglais).
- [6] Joint statement from member countries of the Multilateral Defence Mechanism, 6 juillet 2026 (en anglais).
- [7] Déclaration commune du premier ministre du Canada, Mark Carney, et du premier ministre du Royaume-Uni, Keir Starmer, sur le financement de la défense.
- [8] PM call with Prime Minister Carney of Canada: 22 juillet 2026 (en anglais).
- [9] Global Risk Institute – Security as a systemic Financial Risk: What defence, security and resilience Bank means for financial leaders, mai 2026 (en anglais).
- [10] Banque européenne d'investissement - Garanties et prêts intermédiés de la BEI dans le secteur de la défense par l'intermédiaire de la Deutsche Bank, 11 juin 2025 (en anglais).
- [11] Société financière internationale - Global Trade Finance Program (en anglais).
- [12] Banque européenne pour la reconstruction et le développement - Trade Facilitation Program (en anglais).
- [13] Bureau du surintendant des institutions financières - Ligne directrice, Intégrité et sécurité.
- [14] Bureau du surintendant des institutions financières - Ligne directrice B-10, Gestion des risques liés aux tiers.
- [15] Bureau du surintendant des institutions financières - Ligne directrice B-13, Gestion du risque lié aux technologies et du cyberrisque et ressources sur les tests de cyberrésilience fondés sur le renseignement.
- [16] Bureau du surintendant des institutions financières - Ligne directrice E-21, Gestion du risque opérationnel et résilience opérationnelle.
- [17] CANAFE - Déclaration d'opérations douteuses; les exigences liées à la propriété effective; indicateurs de financement d'activités terroristes; bulletin sur le contournement des sanctions.
- [18] Centre canadien pour la cybersécurité - Évaluation des cybermenaces nationales 2025-2026.
- [19] Services publics et Approvisionnement Canada - Exigences du Programme des marchandises contrôlées et évaluations de sécurité.



L'information publiée dans le présent document est de nature générale. Elle ne vise pas à tenir compte des circonstances de quelque personne ou entité particulière. Bien que nous fassions tous les efforts nécessaires pour assurer l'exactitude de cette information et pour vous la communiquer rapidement, rien ne garantit qu'elle sera exacte à la date à laquelle vous la recevrez ni qu'elle continuera d'être exacte à l'avenir. Vous ne devriez pas y donner suite à moins d'avoir d'abord obtenu un avis professionnel se fondant sur un examen approfondi des faits et de leur contexte.