Plan d’activités annuel de CANARIE

2025-2026 (EF26)

Le 19 mars 2025

canarie.ca | @canarie_inc

Table des matières

1. Aperçu

CANARIE a le plaisir de présenter son plan d'activités pour l'exercice 2025-2026 (EF26), première année de son nouveau mandat de 2025-2030. Le document que voici explique comment CANARIE prévoit atteindre les résultats prévus lors de l'exercice, les risques auxquels s'expose l'organisation et les mesures prises pour les atténuer.

1.1 Rôle de CANARIE

CANARIE et ses treize partenaires provinciaux et territoriaux forment le Réseau national de la recherche et de l'éducation (RNRE) du Canada, un réseau ultrarapide qui connecte les scientifiques, les enseignants et les innovateurs canadiens entre eux, et leur donne accès à leurs homologues, aux données et aux technologies du monde entier.

Afin de rendre le milieu canadien de la recherche et de l'éducation plus sûr, CANARIE finance, met en œuvre et soutient des initiatives en cybersécurité de concert avec ses partenaires du RNRE, le gouvernement, les établissements d'enseignement supérieur et le secteur privé. L'organisation dispense aussi des services de gestion des identités au milieu universitaire grâce à *eduroam* et à des services de gestion des identités et des accès.

Fondé en 1993, CANARIE est une société sans but lucratif principalement financée par le gouvernement du Canada.

1.2 Vision et principes directeurs pour le mandat de 2025-2030

La vision retenue par CANARIE pour son mandat de 2025-2030 est celle d'« Un Canada mieux protégé et plus novateur ».

En ce qui concerne le fonctionnement du réseau, la stratégie de CANARIE consistera à faire en sorte que son réseau évolue et grandisse d'une manière souple et rentable à long terme par le déploiement de fibres à la grandeur du pays. L'organisation disposera ainsi de la marge de manœuvre voulue pour ajouter des capacités au réseau et implanter sans délai des technologies transformatrices à un coût nettement plus abordable, face à l'expansion appréciable du trafic qu'on prévoit dans l'avenir. La location de services garantira la connectivité désirée en procurant la diversité nécessaire au réseau et en élargissant sa portée. CANARIE facilite aussi l'accès à son réseau en coordonnant l'évolution du Réseau national de la recherche et de l'éducation (RNRE) canadien et en procurant aux scientifiques du pays les services de gestion des identités et des accès qui leur permettent de recourir en toute sécurité aux jeux de données, aux infrastructures et aux outils disponibles dans le monde entier.

Sur le plan de la cybersécurité, CANARIE propose des outils et des services, et assure une coordination nationale qui aident le milieu canadien de la recherche et de l'éducation à mieux se protéger et à accroître sa résilience selon le principe de la cybersécurité collective. Dans cette optique, les activités de l'organisation gravitent autour de quatre axes : (1) évaluer et prioriser les risques courus par la communauté (grâce, par exemple, à l'Évaluation nationale de la cybersécurité, à l'analyse comparative des vulnérabilités; etc.); (2) rassembler, analyser et diffuser des informations exploitables sur les

menaces (avec, par exemple, le Fil de menaces, la surveillance du web clandestin, etc.); (3) synchroniser le triage des cyberincidents et y réagir plus rapidement (avec le projet pilote de SOC fédéré du CanSSOC, notamment); (4) regrouper et partager les ressources (modèles, cadres, contenu, etc. communs).

1.2 Nature des activités : EF26 (du 1er avril 2025 au 31 mars 2026)

Outre la gestion et l'évolution de son réseau et d'autres programmes, les principales activités que CANARIE prévoit pour l'EF26 et leurs résultats contribueront à étayer la vision d'« Un Canada mieux protégé et plus novateur ». En voici un aperçu.

- Continuer à rehausser le débit du réseau CANARIE pour le porter à 400 Gbps
- Achever la collecte de données sur le projet pilote de SOC fédéré du CanSSOC et soumettre une demande de financement à ISDE
- Poursuivre l'évolution et l'optimisation du programme Initiatives en cybersécurité (PIC) en accord avec les quatre axes stratégiques
- Adapter l'Évaluation nationale de la cybersécurité pour que ce service s'harmonise mieux avec les autres initiatives sectorielles d'évaluation et de priorisation des risques
- Collaborer avec la collectivité pour diffuser les résultats de l'atelier de visualisation et d'alignement stratégique en cybersécurité de mars 2025 de même que les constatations issues des projets d'analyse et de planification des investissements en cybersécurité
- Élargir le portefeuille des services d'identification en proposant le déploiement d'un service géré de gestion fédérée des identités
- Lancer le premier appel à projets du RNRE en vue de faciliter l'aménagement, l'agrandissement ou l'amélioration des infrastructures réseau et de sécurité, ainsi que de former et garder les éléments de talent
- Poursuivre la coordination avec l'Alliance de la recherche numérique du Canada (l'Alliance) afin de soutenir la stratégie du gouvernement canadien relative à l'infrastructure de recherche numérique

2. Réalisations en 2024-2525

L'exercice 2024-2025 (FY25) est le cinquième et dernier exercice du mandat 2020-2025 de CANARIE. Les pages qui suivent donnent un aperçu de ce que l'organisation a réalisé jusqu'à présent, dans les trois champs d'activité admissibles, énoncés dans l'Accord de contribution qui la régissait durant ce mandat. S'y ajoutent des informations sur les projets en voie d'achèvement. Jusqu'à présent, CANARIE a accompli ce qui suit pendant l'EF25.

- L'organisation a déployé de l'équipement sur d'autres tronçons de son réseau afin d'en hausser le débit à 400 Gbps.
- Elle a renouvelé le droit inattaquable d'utiliser les fibres optiques sur la partie est de son réseau pour les vingt années qui viennent.
- Elle a continuer de déployer le service d'authentification du réseau sans fil *eduroam* en recourant à des fournisseurs de service ailleurs que dans les institutions comme dans les aérogares et les bibliothèques municipales.
- Elle a lancé la troisième mouture de son Évaluation nationale de la cybersécurité (ENC).
- Elle a poursuivi le projet pilote de SOC fédéré du CanSSOC.
- Elle a amélioré le service national « Fil de menaces » en y ajoutant la surveillance du web clandestin, en continuant d'élargir la participation de la communauté et en y intégrant le projet pilote de SOC fédéré du CanSSOC.
- Elle a lancé les projets d'analyse et de planification des investissements en cybersécurité afin (1) de mieux saisir la situation du secteur en la matière et (2) de cerner les éléments essentiels et les pratiques exemplaires qui permettront de sécuriser les organismes de recherche et d'enseignement au Canada.
- Elle a organisé l'assemblée générale de 2024 du RNRE afin de renforcer la collaboration entre les partenaires du RNRE canadien.
- Elle a organisé le Sommet de CANARIE de 2024 sur le thème des innovations transformatrices au service du bien.
- Elle a organisé le tout premier Forum SecuR&E canadien, une activité indépendante sur la cybersécurité destinée à la communauté.
- Elle a rédigé le mandat de CANARIE pour 2025-2030 en s'adaptant de manière à en faciliter l'application et en signalant ses différents aspects aux membres de la communauté.
- Elle a fait progresser les initiatives internationales en cybersécurité.

Projet à achever ou à lancer avant la fin de l'EF25

- Rassembler les membres de la communauté dans le cadre d'un atelier de visualisation et d'alignement stratégiques.

Le rapport annuel présentera les autres réalisations de l'EF25.

3. Activités prévues en 2025-2026

L'EFY26 constitue le premier exercice du nouveau mandat de 2025-2030 de CANARIE. Pour parvenir aux résultats escomptés, l'organisation entreprendra les activités énumérées ci-dessous en 2025-2026.

3.1 Exploitation du réseau

CANARIE entreprendra toutes les activités requises pour faciliter l'évolution de son réseau et la prestation des services qui s'y rattachent.

3.1.1 Programme Réseau

Au cours de l'EF26, le réseau CANARIE continuera de fonctionner et d'évoluer en tant qu'infrastructure scientifique essentielle à la recherche, à l'éducation et à l'innovation.

Activités durant l'EF26	Résultats à court et à moyen terme pour l'EF26
Exploiter le réseau En accroître la capacité, la redondance et la fiabilité Le rendre plus sûr En rehausser la surveillance par l'adoption de nouveaux outils Continuer à faciliter l'accès des utilisateurs aux outils d'aide Poursuivre l'automatisation des services Utiliser le système de détection des dénis de service distribués (DDoS) réservé au réseau CANARIE Échafauder des stratégies en vue d'améliorer l'efficacité, la fiabilité et la sûreté des activités sur le réseau grâce à l'intelligence artificielle (IA) Protéger le réseau et CANARIE en adoptant des mesures pour prévenir, détecter et combattre les cybermenaces et ainsi garantir l'intégrité, la	Déploiement de capacités supplémentaires sur le réseau en fonction de la croissance du trafic Meilleur accès aux services en nuage commerciaux Poursuite des travaux visant à rehausser le débit à 400 Gbps Remplacement des fibres sur le tronçon est du réseau Meilleur système de signalement, de surveillance et de quantification sur la sécurité du réseau Déploiement d'applications d'automatisation et poursuite de l'automatisation du réseau Plans visant à appliquer l'IA au fonctionnement du réseau Déploiement d'outils d'aide sur le portail des utilisateurs

confidentialité et la disponibilité des données et des systèmes Participer aux activités internationales de réseautique comme la connectivité dans la région polaire et le GNA-G (*Global Network Advancement Group*)	

3.1.2 Programme Extension des infrastructures (PEI)

Durant l'EF26, CANARIE aidera les instituts de recherche du gouvernement à tirer parti du réseau de recherche dans le cadre de leurs projets de collaboration avec leurs partenaires du Canada et de l'étranger jusqu'à la cession définitive des connexions à Services partagés Canada (SPC), à la fin de l'EF28.

Activités durant l'EF26	Résultats à court et à moyen terme pour l'EF26
Maintenir la connexion à haute vitesse au réseau dans les installations de recherche du gouvernement Veiller à ce que les connexions répondent aux besoins des utilisateurs Préparer le transfert des connexions du PEI à SPC	Maintien des connexions existantes dans les installations de recherche du gouvernement qui satisfont aux exigences de rendement applicables au personnel scientifique de la fonction publique

3.1.3 Gestion des identités et des accès

Au cours de l'EF26, CANARIE procurera de robustes services de gestion des identités et des accès afin de sécuriser et de faciliter en permanence l'accès aux ressources et aux outils répartis grâce à son programme Fédération canadienne d'accès (FCA).

Activités durant l'EF26	Objectifs à court et à moyen terme pour l'EF26
Poursuivre la collaboration avec les participants de la Fédération canadienne d'accès (FCA) et les experts de l'industrie afin de planifier l'évolution de la FCA Augmenter le nombre de sites qui diffusent *eduroam* dans la communauté afin de multiplier les possibilités de téléapprentissage et l'usage créatif des espaces communs Élargir le portefeuille de services d'identification en déployant un service géré de gestion fédérée des identités Participer à l'évolution des services de gestion des identités avec la communauté internationale	Maintien du taux de participation élevé actuel à la FCA Hausse du nombre annuel de connexions à *eduroam* Hausse du nombre de projets visant à rehausser les capacités de la Fédération Hausse du nombre d'interfaces, d'applications et d'outils qui soutiennent les services de la FCA

3.1.4 Programme RNRE

Durant l'EF26, CANARIE continuera de faire évoluer le RNRE pour qu'il fonctionne de manière coordonnée et concoure à la réalisation des objectifs communs aux deux réseaux tout en respectant la diversité inhérente au modèle fédéré et en tirant parti de cet avantage.

Activités durant l'EF26	Objectifs à court et à moyen terme pour l'EF26
Accroître les capacités, la redondance, la fiabilité et la sécurité par l'entremise des réseaux des partenaires provinciaux et territoriaux du RNRE Connecter les installations de recherche et d'enseignement, y compris celles situées dans le Nord Renforcer la cybersécurité du RNRE Perfectionner les processus et rehausser les capacités du RNRE de même que soutenir et retenir les éléments talentueux	Préparation en vue du lancement d'un premier appel à projets qui permettra au RNRE d'aménager, d'agrandir ou d'améliorer le réseau et son infrastructure de sécurité ainsi que de perfectionner et de garder ses éléments de talent Développement et lancement de projets qui amélioreront les méthodes et les capacités du RNRE Analyse en prévision du lancement d'un deuxième appel à projets, au cours de l'EF27, en vue de raccorder les institutions autochtones qui ne sont pas encore connectées au RNRE

3.2 Cybersécurité

Pendant l'EF26, CANARIE aidera le milieu de la recherche et de l'éducation à renforcer sa cybersécurité de manière générale.

Activités durant l'EF26	Objectifs à court et à moyen terme pour l'EF26
Achever le projet pilote de SOC fédéré du CanSSOC, en évaluer l'impact et les retombées, en tirer des leçons et évaluer la possibilité de poursuivre ce service Élargir le service de renseignement sur les cybermenaces en intégrant notamment le Fil de menaces au projet pilote de SOC fédéré du CanSSOC afin de recueillir plus d'informations sur les menaces et d'adopter des mesures pour les combattre par anticipation Explorer une plateforme de partage de l'information en vue de faciliter l'échange sectoriel de modèles, de cadres et d'idées Élaborer des cadres, des politiques, des modèles et des outils de collaboration communs afin de donner plus de cohésion à la communauté et de l'harmoniser davantage Identifier des initiatives en cybersécurité qui profiteront à l'ensemble du secteur selon les données recueillies et leur analyse, et mettre ces initiatives à exécution Lancer des activités de marketing ciblées pour mieux faire connaître les initiatives en cybersécurité de CANARIE et augmenter la participation des organisations admissibles Inciter la communauté à se mobiliser davantage en complétant les méthodes de consultation actuelles avec des canaux informels, plus polyvalents, et accroître les capacités du secteur en cybersécurité Resserrer la collaboration avec les organismes de cybersécurité canadiens au bénéfice du secteur R-E et de l'économie Améliorer et élargir les initiatives les plus utiles en fonction des résultats des projets antérieurs	Déploiement et perfectionnement des initiatives dans les quatre axes stratégiques de la cybersécurité : évaluation des risques pour la communauté, renseignements sur les menaces, interventions et regroupement/partage des ressources Achèvement de la collecte de données sur le projet pilote de SOC fédéré du CanSSOC et remise d'une demande de financement à ISDE Élargissement du Fil de menaces du CanSSOC pour en faire un service national complet de renseignement sur les cybermenaces Organisation et direction éclairée d'événements qui inciteront la communauté à s'engager davantage et à harmoniser ses activités Adapter l'Évaluation nationale de la cybersécurité pour qu'elle s'accorde mieux avec les autres exercices sectoriels d'évaluation et de priorisation Établir un cadre solide pour faciliter la participation et la collaboration de la communauté, notamment en précisant le rôle et les responsabilités de chacun

3.3 Activités entreprises avec l'Alliance de la recherche numérique du Canada

Durant l'EF26, CANARIE collaborera avec l'Alliance de la recherche numérique du Canada (ARNC) afin d'aider le gouvernement canadien à mettre à exécution sa stratégie sur l'infrastructure de recherche numérique.

Activités durant l'EF26	Objectifs à court et à moyen terme pour l'EF26
Poursuivre l'intégration des outils et des services de CANARIE et de l'ARNC, y compris ceux en cybersécurité Continuer d'harmoniser les activités de gouvernance, de communication et de rayonnement Amorcer des discussions sur les façons d'appuyer la science au sein du gouvernement canadien, y compris les ministères et les organismes à vocation scientifique et les politiques scientifiques fédérales	Participation de l'ARNC et des sites d'hébergement à l'Évaluation nationale de la cybersécurité Planification d'approches communes en cybersécurité, y compris activités en cybersécurité de l'Alliance qui se greffent à l'approche du SOC fédéré du CanSSOC et en tirent avantage Alignement des deux organisations au niveau de la gouvernance en cybersécurité, notamment en confiant la présidence de leurs comités de cybersécurité respectifs à une seule et même personne Intégration de la gestion fédérée des identités aux services CIP de l'Alliance Participation de CANARIE aux mécanismes du projet pilote d'infonuagique

3.4 Activités appuyant l'équité, la diversité et l'inclusion

Au cours de l'EF26, CANARIE s'efforcera de faire progresser l'équité, la diversité et l'inclusion (EDI) à l'interne et dans les programmes que l'organisation a mis en place.

Activités durant l'EF26	Objectifs à court et à moyen terme pour l'EF26
Poursuivre les activités qui soutiennent les groupes mal représentés au Canada et ailleurs dans le monde	Préparatifs en vue du lancement d'un deuxième appel à projets durant l'EF27 afin de raccorder au RNRE les institutions autochtones qui ne le sont pas déjà

Dispenser au personnel de CANARIE de la formation sur les sujets qui feront progresser l'EDI Continuer à moderniser les politiques, les méthodes et les pratiques de CANARIE Poursuivre la stratégie et les activités de mobilisation des Autochtones Collaborer avec les membres de l'écosystème de l'IRN pour établir une politique commune sur l'EDI Continuer d'utiliser les plans EDI des institutions comme critère pour sélectionner les projets qui seront financés, quand la chose est appropriée	Participation au consortium chargé de poser un câble dans l'Arctique pour améliorer la connectivité dans le Nord Soutien des groupes d'entraide du personnel de CANARIE Prestation de formation supplémentaire aux employés, s'il y a lieu

4. Échéancier d'exécution des programmes

		Exercice 2025-2026			
Activités admissibles	**Initiatives**	**En cours**	**Lancement prévu ou *réel***	**Principaux jalons (antérieurs)**	**Achèvement prévu (antérieur)**
Exploitation du réseau					
Programme Réseau	Exploiter le réseau				
	En accroître les capacités, la redondance et la fiabilité - Jalon 6 : installer les fibres optiques sur le tronçon est - Jalon 7 : lancer le service 400 Gbps sur le tronçon est, rehausser le débit à 400 Gbps à l'ouest et au sud de Montréal - Jalon 8 : retirer le vieil équipement et procéder au nettoyage		***2020-04-01***	**2025-08-22** **2025-09-26** **2025-11-28**	**2025-11-28**
	Continuer d'améliorer les outils de surveillance et de quantification du réseau afin de le rendre plus sûr				
	Poursuivre le développement des services réseau virtuels - Jalon 1a : démonstration de la plateforme réseau virtuelle - Jalon 2 : inventaire dresssé sur la plateforme - Jalon 3 : démonstration de la configuration du réseau par la plateforme		***2023-04-01***	**2025-05-30** **2025-09-26** **2026-02-26**	**2030-03-31**
	Mise à niveau du système de détection des dénis de service distribués (DDoS) du réseau CANARIE - Jalon 1 : sélection d'un fournisseur pour le matériel et les services - Jalon 2 : mise en oeuvre du nouveau système DDoS - Jalon 3 : fin des réglages, en production		**2025-04-01**	**2025-08-29** **2025-11-28** **2026-02-27**	**2026-02-27**
	Surveiller la cybersécurité sur l'infrastructure, les services et le réseau de CANARIE; auto-surveillance de la cybersécurité sur le réseau des partenaires du RNRE				
	Exploiter le système de détection des attaques par déni de service distribué (DDoS) sur le réseau CANARIE et collaborer activement avec les partenaires du RNRE				
	Promouvoir et mettre en place un programme interne de perfectionnement en cybersécurité pour le personnel de CANARIE chargé de la sécurité et pour les analystes en sécurité du RNRE				
PEI	Procurer une connexion à haute vitesse aux installations de recherche du gouvernement - Jalon 1 : planifier le transfert des connexions de CANARIE à SPC		**2025-04-01**	**2025-06-27**	**2027-03-31**

Activités admissibles	Initiatives	En cours	Lancement prévu ou *réel*	Principaux jalons (antérieurs)	Achèvement prévu (antérieur)
Programme Gestion des identités et des accès	Promouvoir l'adoption de l'outil CAT (*Configuration Assistant Tool*) qui crée des profils eduroam pour accroître la sécurité de la communauté				
	Élaborer une documentation technique plus solide et des tutoriels pour simplifier le déploiement, la prestation et l'utilisation d'eduroam et des services de GIA				
	Promouvoir la technologie des services gérés qui facilite le déploiement d'eduroam pour augmenter le nombre de sites qui proposent ce service dans la communauté				
	Appliquer une technologie similaire à la gestion des identités et des accès - Jalon 1 : sélectionner une technologie de services gérés - Jalon 2 : tester le service dans plusieurs institutions - Jalon 3 : déployer la technologie dans d'autres institutions		**2024-08-07**	**2025-01-30** **2025-04-03** **2025-08-22**	**2025-09-26**
	Évaluer les besoins de la communauté en gestion des identités et des accès - Jalon 1: sélectionner un fournisseur après étude du marché - Jalon 2 : obtenir les résultats préliminaires - Jalon 3 : convertir les résultats en éléments d'une communauté de pratique GIA et adapter la prestation du programme de CANARIE en conséquence		**2025-03-04**	**2025-06-27** **2025-12-12** **2026-02-27**	**2026-03-27**
Programme RNRE	1er appel à projets - Jalon 1 : approuver la charte de l'appel - Jalon 2 : lancer l'appel aux partenaires du RNRE - Jalon 3 : sélectionner les projets		**2025-01-13**	**2025-01-30** **2025-04-03** **2025-10-08**	**2028-01-31**
	2e appel - raccorder les institutions qui ne le sont pas encore - Jalon 1 : approuver la charte de l'appel		**2025-07-01**	**2025-12-12**	**2029-01-31**

Activités admissibles	Initiatives	En cours	Lancement prévu ou *réel*	Principaux jalons (antérieurs)	Achèvement prévu (antérieur)
Cybersécurité	Continuer d'offrir le pare-feu DNS, le Fil de menaces, l'Évaluation nationale de la cybersécurité et l'analyse comparative des vulnérabilités aux organisations admissibles intéressées				
	Projet pilote du CanSSOC - Jalon 3 : achever la collecte des données - Jalon 4 : soumetttre une demande de financement à ISDE		***2023-09-03***	**2025-06-30** **2025-09-12**	**2026-08-28**
	Amélioration de la collecte de données pour l'évaluation de la plateforme de partage de l'information - Jalon 1 : choisir un fournisseur - Jalon 2 : finir les améliorations à temps pour lancer la 4e mouture des évaluations		**2025-04-01**	**2025-07-25** **2025-10-31**	**2026-03-31**
	Centre des opérations en sécurité partagé du CanSSOC				
	Évolution du Fil de menaces du CanSSOC - Jalon 1 : dupliquer le fil de menaces de McGill hébergé par CANARIE - Jalon 2 : terminer les améliorations et transférer les opérations quotidiennes de McGill à CANARIE		**2025-04-01**	**2025-09-26** **2026-02-20**	**2026-03-31**
Activités entreprises avec l'Alliance de recherche numérique du Canada					
Cybersécurité	Usage de l'Évaluation nationale de la cybersécurité (ENC) par l'Alliance et les sites d'hébergement - Jalon 1 : choisir l'administrateur responsable du questionnaire de l'ENC pour les sites d'hébergement - Jalon 2 : inscription à l'ENC		**2025-04-01**	**2025-07-31** **2025-09-30**	**2026-02-27**
	Alignement des deux organisations au niveau de la gouvernance de la cybersécurité, y compris présidence des deux comités de cybersécurité par la même personne				
	Poursuite du travail visant à intégrer la gestion fédérée des identités aux services CIP de l'Alliance				
Activités favorisant l'équité, la diversité et l'inclusion					
EDI	2e appel à projets du RNRE en vue de raccorder les institutions autochtones qui ne le sont pas déjà		Voir 2e appel du	Voir 2e appel du	Voir 2e appel du RNRE
	Poursuite des activités avec les consortiums qui posent un câble sous-marin dans l'Arctique pour rehausser la connectivité dans le Nord				
	Soutien constant des groupes d'entraide des employés de CANARIE				
	Formation supplémentaire pour le personnel				

5. Assertion et plan financier

Le gouvernement du Canada a débloqué 176 M$ pour financer les activités de CANARIE de 2026 à 2030. Grâce à ces fonds, CANARIE continuera d'investir de façon stratégique dans l'infrastructure et les services qu'il met à la disposition des chercheurs et des innovateurs du pays. Conformément à l'Accord de contribution, 29 600 000 $ iront au financement de ses activités durant l'EF26 et CANARIE s'engage à conserver, à investir, à administrer et à utiliser ces fonds comme le stipule l'Accord de contribution.

5.1 Revenus et dépenses

Le tableau qui suit résume les revenus et les dépenses prévus au titre des programmes de CANARIE pendant l'EF26.

	(en milliers $
Revenus	
Financement	
Gouvernement du Canada	29 600
Sous-total	**29 600**
Rentrées des programmes	
Droits d'utilisation	650
Intérêts	50
Sous-total	**700**
Revenus totaux	**30 300**
Dépenses	
Programmes	
Exploitation du réseau	
Infrastructure et services	15 517
RNRE	973
FCA	1 928
Sous-total	**18 418**
Cybersécurité	
Programmes et services	5 041
Projet pilote de SOC fédéré du CanSSOC	1 623
Sous-total	**6 664**
Sous-total (programmes)	**25 082**
Frais administratifs	5 218
Dépenses totales	**30 300**
Excédent	-

5.2 Financement

Tel qu'indiqué ci-dessus, CANARIE aura besoin de 29,6 M$ pour l'EF26.

5.3 Assertion

CANARIE affirme ne déroger à aucune des conditions de l'Accord de contribution actuellement en vigueur.

5.4 Recouvrement des coûts

Le tableau que voici indique les coûts que CANARIE devrait recouvrer au cours de l'EFY26.

	EF26 (en milliers $)
Espèces	
Droits d'utilisation du PEI – gouv. fédéral	100
Droits d'utilisation du PEI – autres établissements	6
Droits d'adhésion	544
Sous-total	**650**
Fonds de contrepartie	
RNRE	*0*
Sous-total	**0**
RECOUVREMENT TOTAL	**650**

Durant l'EF26, CANARIE continuera de percevoir des droits d'utilisation pour ses programmes et ses services comme suit.

- Dans le cadre de son Programme d'extension des infrastructures (PEI) patrimonial, CANARIE absorbe le coût de la connexion des laboratoires fédéraux ou autres au RNRE. La somme recouvrée pour raccorder les établissements fédéraux au réseau correspond à un montant fixe, versé annuellement par Services partagés Canada en compensation du coût annuel d'une telle connexion. Pour les autres établissements, non fédéraux, qui bénéficient du PEI, le montant inscrit au budget correspond au recouvrement total des dépenses prévues.
- Les droits d'adhésion correspondent aux fonds recouvrés dans le cadre du programme FCA et d'autres initiatives du programme Réseau.
- Le coût des projets financés dans le cadre du programme RNRE sera divisé entre CANARIE et d'autres sources de financement (provinces, partenaires du RNRE, etc.). La contribution de CANARIE sera établie un projet à la fois et l'organisation s'assurera qu'on atteigne les objectifs de recouvrement. C'est pourquoi on accordera la priorité aux projets pour lesquels on aura

réuni d’autres fonds. Puisque le premier appel à projets du RNRE ne sera lancé qu’au cours de l’EF27, aucun fonds de contrepartie n’est prévu pour l’EF26.

5.5 Politique et stratégie d’investissement

CANARIE continuera d’investir et de gérer les fonds qui lui sont avancés selon les politiques, les normes et les procédures que suivrait avec prudence une personne chargée de prendre des décisions sur l’investissement de biens qui ne lui appartiennent pas. CANARIE administrera les fonds d’après les modalités de l’Accord de contribution, plus précisément les lignes directrices de son annexe E. L’objectif est double : a) procurer à CANARIE les fonds nécessaires au moment où il en a besoin pour couvrir ses dépenses et b) optimiser les revenus de placement selon la stratégie et la politique pertinentes adoptées par l’organisme. Les décisions relatives aux placements seront prises dans l’optique de préserver les capitaux, de manière à disposer de fonds suffisants pour couvrir les dépenses à venir.

La politique et la stratégie d’investissement précisent la nature des transactions autorisées, les risques maximaux concernant les opérations de toute sorte, y compris ceux relatifs aux opérations de crédit auxquelles doit faire face l’organisme, ainsi que le pouvoir décisionnel des représentants de CANARIE autorisés à effectuer diverses opérations. La politique et la stratégie d’investissement sont revues chaque année. Le Comité de la vérification comptable et des placements les a examinées en octobre 2024. La politique en matière de placements est régie par les exigences de l’Accord de contribution.

6. Stratégie de surveillance du rendement et stratégie d'évaluation et d'atténuation des risques

6.1 Surveillance du rendement

CANARIE recueille des données sur tous ses programmes et services et sur son réseau à l'interne. Des mesures externes du rendement sont aussi glanées dans la collectivité, par le biais de sondages et de rapports, de même qu'avec le concours des réseaux régionaux. CANARIE œuvre avec le ministre pour que ces informations soient intégrées à une stratégie générale de gestion du rendement. Par ailleurs, les données sur le rendement se rapportant à chaque activité admissible sont exposées dans le rapport que CANARIE produit annuellement.

6.2 Risques relatifs à l'exécution des programmes

Étant donné la diversité et la complexité de l'écosystème dans lequel il opère, CANARIE doit absolument gérer les risques pour parvenir aux résultats escomptés, énoncés dans l'Accord de contribution. La direction de l'organisme signale les risques et son conseil d'administration les surveille.

Les risques sont classés d'après la probabilité qu'ils se concrétisent et la gravité de leurs conséquences. La façon dont ils sont traités varie selon ces deux paramètres, comme l'indique le tableau ci-dessous.

		Probabilité		
		Faible	**Moyenne**	**Élevée**
Impact	**Faible**	Courir le risque	Courir le risque en le surveillant	Surveiller et gérer le risque
	Modéré	Courir le risque en le surveillant	Élaborer des mesures pour atténuer le risque	Dresser un plan pour atténuer le risque
	Élevé	Identifier des mesures d'atténuation et suivre la situation régulièrement	Élaborer des mesures d'atténuation et suivre la situation régulièrement	Dresser un plan d'atténuation et suivre la situation régulièrement

Plus de précisions dans le tableau qui suit

Risque	Description	Prob.	Impact	Risque	Mesures d'atténuation et plan d'action
Nouveau libellé de l'Accord de contribution	Le libellé de l'Accord de contribution a changé et CANARIE devra s'y adapter.	E	M	EM	• Collaborer avec ISDE pour satisfaire les exigences du ministère
Risque associé aux fournisseurs	La chaîne d'approvisionnement pourrait poser des risques sur le plan de la cybersécurité.	M	E	ME	• Ajouter des exigences sur la gestion des risques liés à la cybersécurité au processus d'approvisionnement • Examiner le libellé des exigences sous l'angle juridique • Élaborer un code de conduite pour les fournisseurs avec le service des finances pour adapter les pratiques d'approvisionnement • Étudier les risques soulevés par le recours à une source d'approvisionnement unique
Intrusion IT dans l'organisme ou cybercriminalité	Une intrusion dans la dorsale de CANARIE pourrait exposer les données de recherche, ouvrir une porte qui mettrait les institutions raccordées au réseau en danger et ternir la réputation de l'organisme	M	E	ME	• Continuer d'investir dans les technologies de l'information • Appliquer des correctifs et améliorer les pratiques • Détecter les attaques par déni de service distribué (DDoS) • Dispenser une formation en sécurité au personnel et surveiller la sécurité • Acheter une assurance en cybersécurité • Dresser des plans d'intervention • Premier exercice sur maquette tenu en mars 2023 • Exercice sur maquette interne terminé en novembre 2024. Plans de maintien des activités et d'intervention actualisés d'après les résultats de l'exercice • Exercice sur maquette avec les partenaires du RMRE réalisé en juillet 2024 • Faire régulièrement le point sur la sécurité aux rencontres mensuelles du personnel
Intrusion dans le réseau CANARIE	Une intrusion dans la dorsale du réseau CANARIE pourrait exposer des données de recherche, ouvrir une porte qui mettrait en danger les institutions raccordées au réseau et ternir la réputation de CANARIE	M	E	ME	• Investir dans la sécurité (p. ex., SIEM) • Détecter les attaques par déni de service distribué (DDoS) • Appliquer les normes MANRS en protection des réseaux

Risque	Description	Prob.	Impact	Risque	Mesures d'atténuation et plan d'action
Intrusion dans le RNRE	Une intrusion dans le réseau d'un des partenaires du RNRE pourrait affecter le réseau CANARIE et ternir la réputation du RNRE ainsi que celle de CANARIE, par contrecoup	M	E	ME	• Investir conjointement dans la sécurité (p. ex., SIEM). • Les partenaires du RNRE ont engagé des analystes en sécurité qui collaborent à l'échelon national. • Adopter le cadre de cybersécurité • Instaurer le bulletin de note en sécurité du RNRE • Faciliter l'inclusion du RNRE au centre des opérations en sécurité (SOC) • Appliquer les normes de sécurité MANRS à la majeure partie du RNRE • Exercice sur maquette effectué à l'assemblée générale du RNRE en octobre 2024
Risque d'un conflit économique entre le Canada et les É.-U. (guerre tarifaire)	Si le gouvernement des É.-U. applique des tarifs douaniers à de nombreux produits canadiens et que le gouvernement fédéral adopte des mesures de rétorsion, CANARIE pourrait avoir du mal à se procurer du matériel des fournisseurs américains ou à renouveler des contrats, ce qui entraverait ses opérations.	M	E	ME	• Risque impossible à atténuer • Mémoire sur l'analyse de la situation
Projet pilote de SOC fédéré du CanSSOC	Risque que le modèle fédéré et que la difficulté inhérente à amener les intervenants à s'aligner engendre une participation insuffisante au projet, ce qui réduirait la masse de données disponible pour l'analyse	F	E	FE	• Groupe de travail des ressources humaines • Groupe de travail des dirigeants en sécurité de l'information • Supervision par la direction • Principes directeurs sur la participation des partenaires du RNRE adoptés • Charte du projet pilote endossé par la Commission consultative en cybersécurité • Nombreuses séances d'information sur le contenu et la nature des ententes de partage de l'information à l'intention des institutions participantes • Poursuite des activités avec les institutions susceptibles de participer au projet pour leur faciliter la tâche et les encourager à aller de l'avant

Risque	Description	Prob.	Impact	Risque	Mesures d'atténuation et plan d'action
					• 13 institutions dans cinq provinces ont ratifié l'entente en vue de participer au projet
Activités communes avec l'Alliance	Exigences de l'Accord de contribution dépendant de la capacité de l'Alliance à soutenir les activités communes	F	F	FF	• Collaborer avec ISDE, l'Alliance et la collectivité pour soutenir la nouvelle organisation • Poursuite des rencontres avec l'Alliance. Resserrement des liens avec le président et d'autres membres importants du personnel de l'Alliance